University of Piraeus
School of Information and Communication Technologies
Department of Digital Systems

Postgraduate Program of Studies
MSc Digital Systems Security

MSc Dissertation

Examining compliance requirements under the EU's Digital Operational Resilience Act (DORA) for the Financial Sector

Maria-Fani Skiadioti
A.M.: MTE2320

Supervisor Professor: Stefanos Gritzalis

Piraeus
February 2025

Abstract

The current dissertation strives to critically examine the regulatory requirements under Regulation (EU) 2022/2554 of the European Parliament on digital operational resilience for the financial sector (DORA) that is framed by and aims to set out uniform requirements for the security of networks and information systems of entities operating in the financial sector including ICT third-party service providers. In that direction, the European Supervisory Authorities (ESAs), namely the European Banking Authority (EBA), the European Insurance and Occupational Pensions Authority (EIOPSA), and the European Security and Markets Authority (ESMA), in consultation with the European Union Agency on Cybersecurity (ENISA), are in the process of developing common draft regulatory technical standards to both ensure the harmonization of ICT risk management tools, methods, processes and policies and provide a simplified ICT risk management framework for certain financial entities. Further on this, in Article 2(h) of Commission Delegated Regulation (EU) 2024/1774 supplementing DORA regarding the general elements of said security policies, procedures, protocols, and tools, the financial entities should ensure that they consider "leading practices and, where applicable, standards as defined in Article 2, point (1), of Regulation (EU) No 1025/2012" [1].

Under that prism, this dissertation will look into these requirements and also address the collaborative relevance of existing standards and frameworks namely the ISO/IEC standards regarding the management of risks, ensuring business continuity and protection of information assets and the Threat Intelligence-Based Ethical Red Teaming (TIBER)-EU framework developed by the European Central Bank (ECB) to test and improve the cyber resilience of financial infrastructures and institutions in an effort to consolidate the key points of this pivotal regulatory framework mostly based on a qualitative review of regulatory texts and technical standards and expert reviews. Ultimately, the core elements of our review will constitute an aggregated checklist tool for high-level monitoring based on tests performed to assess the level of compliance with controls linked to identified risks.

The current essay will thus be organized as follows. Initially, an introduction to the background leading to DORA and current outlook of the supervisory priorities' landscape will set the foundation for delving into the requirements of the regulatory framework. The second chapter will be dedicated to the literature review, an overview of the DORA legislative framework and its main pillars and policy mandates, a respective high-level overview of other standards and frameworks that will be discussed and the objectives of the essay. The focus of the third chapter will be a more thorough navigation through DORA's requirements going through the regulatory technical standards per area of interest and, subsequently, a comparative and/or collaborative analysis with the standards and framework discussed in the second chapter. The fourth chapter will include the assumptions for the development of a checklist incorporating the qualitative analysis of the previous chapters. Finally, the fifth and last chapter will entail conclusions based on the analysis of the previous chapters and possible areas of extension and interest based on future updates post application of the provisions of DORA starting January 17, 2025.

Table of Content

1. Introduction

1.1 Background

Effective governance structure and strong risk culture are critical elements of an organization making sound decisions as they, collaboratively with other factors, play a pivotal role in ensuring safety and soundness and, in the case of organizations operating in the banking sector, the stability of the financial system they operate in. In the recent past, we have witnessed that a failure of a single entity, can lead to spillover effects on the whole sector and, even on the overall economy, through , for instance, interbank lending as in liquidity shortages due to wariness, loss of confidence in the banking system as a whole triggering deposit withdrawal, credit crunches as in the remaining players tightening lending standards post the collapse of a major player, with consequences in the operation of businesses and employment, decline in asset prices and so on.

The collapse of Credit Suisse in 2023 constitutes a recent significant event in the financial world that was, among a broader context, partly driven by idiosyncratic issues some of which related to poor governance eroding investor confidence. The emergency takeover by UBS prevented a total collapse but also led to concentration of financial risk in a single entity arising questions about the future of competition and overall stability of the Swiss banking sector among others, and, as a result, prompted increasing regulatory scrutiny globally regarding the resilience of the financial sector.

Even before that though, new goals, risks and challenges had emerged for the banking sector in the form of financial technologies (fintech) and technology outsourcing. All this was stimulated by thin profit margins of banking services, transformation of traditional business models of financial market participants to adapt to a changing market landscape a significant aspect of which being the creation of financial ecosystems where banks and other entities collaboratively offer a range of services, the increase of bank penetration as in the digitalization of financial services making them more accessible to a broader audience, the loss of the monopoly in the provision of traditional services to the provision of alternative payment systems by tech

companies and startups (e.g. digital wallets, P2P payment systems, Digital-Only Banks, Cryptocurrencies and De-Fi) and subsequent diversification of the financial market, the imposition of quasi-state control functions of banks by regulators bringing about increased responsibilities for enhanced compliance and state-mandated controls such as AML (anti-money laundering) regulations and the, as a result of all the aforementioned, bank's desire for partnerships to keep pace with the rapid technological advancements [2].

A growing segment of technology outsourcing in the banking sector involves cloud computing whose use by financial institutions was reinforced by the normalization of flexible working and is linked with both benefits and risks.

In terms of benefits, the use of cloud services can lead to enhanced security and operational resilience as cloud service providers, benefitting from economies of scale as opposed to individual clients, can make larger investments in digital security and automated systems to detect and remedy issues quickly and, major cloud platforms are capable of supporting requirements, allowing clients to manage cyber risk using best practices, standards, data encryption and activity logging. Further, the computing resources available through the cloud can facilitate the deployment, by both financial institutions and their regulators, of stronger data analytics tools thus improving compliance monitoring, risk management, and supervisory analysis. What is more, the distributed nature of cloud technologies can provide greater operational efficiency as, cloud providers, can distribute data centers geographically to avert disruptions to a single point.

Finally, another potential benefit of said services is reduced costs. Through their use, financial institutions can decrease their technology infrastructure expenses by eliminating the need for significant capital investments in proprietary data centers thus increasing their agility when developing new products and services testing various scenarios, software tools and alternative configurations without delay, leveraging the cloud's scalability. However, the aforementioned benefits also come with novel risks arising from the unique technical features of cloud computing that depends on multi-tenancy as in multiple clients sharing the same pool of computing resources and having

access to the same computing environment as financial institutions, leaving room for potential unauthorized access to their data.

1.2 Core regulatory guidelines leading to DORA

In response to this increasing trend of financial institutions outsourcing technology functions to cloud and other TSPs, regulators of said institutions have issued principles-based regulations and guidance addressing outsourcing [3] to overcome uncertainty regarding supervisory expectations in the area. In 2019, EBA issued a final report on its guidelines on outsourcing arrangements, updating the Committee of European Banking Supervisors (CEBS) guidelines on outsourcing issued in 2006, which applied exclusively to credit institutions and also integrating its recommendations on outsourcing to cloud service providers issued in 2017, in the direction of establishing a more harmonized framework for all financial institutions. The guidelines apply to all financial institutions within the EU including credit institutions, investment firms, and payment and electronic money institutions and give emphasis on outsourcing of critical and important functions, particularly when the service provider is located outside the EU. The key points of these guidelines as they have been identified consist of the following:

- ✓ Outsourcing should not be permitted in the case where it undermines the conditions of the financial institution's authorization either by removing or modifying them. The responsibility of the institution's management body can never be outsourced, nor can outsourcing lower the institution's obligation to comply with regulatory requirements (including social and environmental responsibilities)

- ✓ The management body should ensure that sufficient resources are available to appropriately support and ensure the performance of its responsibilities, overseeing the risks and managing the outsourcing arrangements included. It should also set strategies and policies regarding the business model, risk appetite and risk management framework. Responsibilities for documentation,

management and monitoring of all outsourcing arrangements should be clearly defined.

The outsourcing policy should also differentiate between outsourcing of critical or important functions and other outsourcing arrangements, outsourcing to service providers that are authorized by a competent authority and those that are not, intragroup outsourcing arrangements, outsourcing arrangements within the same institutional protection scheme and outsourcing to entities outside the group and outsourcing to service providers located within a Member State and third countries.

- ✓ An emphasis is therefore given on effective internal governance arrangements as institutions need to manage contractual relationships including evaluating and monitoring the ability of the service provider to abide to the conditions included in the outsourcing agreement, ensuring compliance with all legal and regulatory requirements and conduct documentation, and monitoring of all outsourcing arrangements. On that note, business continuity and data protection should be appropriately considered as the institutions to which these guidelines apply fall within the scope of application of Regulation (EU) 2016/679. Contracts must therefore include provisions for data security, audit rights, and the possibility of sub-outsourcing. Further, concentration risks should be taken into account, especially in the case of critical or important functions involved in outsourcing arrangements with cloud providers, as a potential failure of service may lead to disruptions in the provision of services across multiple institutions.

- ✓ The guidelines also provide points that should be considered when assessing which functions are critical or important such as functions directly connected to the provision of core banking activities, the potential impact of disruption to the outsourced function and the services provided to clients, the size and complexity of the affected area e.tc.

- ✓ Institutions must additionally ensure that they have full access to all information related to the outsourced functions including the right to audit the outsourcing provider and potential subcontractors and outsourcing agreements should also

include clauses in order for competent authorities to have similar access and audit rights.

- ✓ Emphasis is also given on risk management functions specific to outsourcing in the context of an institution-wide risk management framework across all business lines and internal units, cyber risks included. Requirements are subjected to the principle of proportionality in regard to the institution's size, scope, nature and complexity of operations and include identification, assessment, monitoring and management of all risks, including those stemming from arrangements with TPs as well as the conduction of thorough risk assessments prior to entering into an outsourcing agreement.

- ✓ Regarding cloud services, special emphasis is given on their performance and quality in terms of ensuring confidentiality, integrity and availability of data and systems and processes involved in processing, transferring, or storing said data as well as appropriate traceability mechanisms aimed at keeping records of technical and business operations being in place to detect malicious attempts. Further, given that cloud service providers often operate a geographically dispersed computing infrastructure, the security, privacy and processing of data require particular attention.

- ✓ Exit plans from outsourcing agreements regarding critical or important functions such as migrating to another service provider or transitioning the outsourced functions back in-house should be in place and documented [4].

On 12 January 2016, the revised Payment Services Directive (PSD2) **(**Directive (EU) 2015/2366) regulating payment services and payment service providers entered into force and EU Member States were given until 13 January 2018 to transpose it into national law. The Directive aimed at more integrated and efficient European payments market as well as enhanced security of payments and consumer protection and was supplemented by RTS on strong customer authentication (Article 97) and common and secure open standards of communication, as well as guidelines on incident reporting (Article 96) (including incident reporting templates (initial, intermediate and

final reporting) and incident classification guidelines) as well as and guidelines on security measures for operational and security risks.

Regarding ICT Risk Assessments, EBA issued relevant guidelines in 2017 framed by an Annex containing a taxonomy of ICT risks mapped into five broad categories (a. ICT availability and continuity risk, b. ICT security risk, c. ICT change risk, d. ICT data integrity risk and e. ICT outsourcing risk) and supporting documents regarding current practices and policy options that were considered for the conduction of the guidelines, aiming at promoting common procedures across the financial institutions of jurisdiction that were put to application starting January 2018. The general provisions of the guidelines on the part of the financial institutions involved the requirement of an ICT strategy consistent with the business strategy in place, suitable for planning and implementing important and complex ICT changes and that are adequately documented and supported. Special emphasis was given on internal governance as in a robust and transparent organizational structure with clear responsibilities on ICT, including the management body and its committees and effective communication between key responsible persons for ICT and the management body ensuring that important ICT-related information or issues are adequately reported, discussed and decided upon at management body level and that the latter is informed and in the position to address ICT related risks.

Further, financial institutions were to be assessed on whether, the risk appetite and Internal Capital Adequacy Assessment Process (ICAAP) entailing the assessment of risks to capital, cover ICT risk as part of the broader operational risk category and that this risk is within the scope of institution-wide risk management and internal control frameworks. Material ICT risks and critical ICT systems and services supporting core activities should be hence identified when reviewing the entity's risk profile. Controls that should be considered whilst addressing material ICT risks were mapped into the five main risk categories described in the guidelines' Annex.

For all the above, an appropriate framework was asked to be in place for identifying, understanding, measuring, and mitigating ICT availability and continuity risks with defined roles and responsibilities that encompasses dependencies between business processes and supporting systems, recovery objectives for said systems,

appropriate contingency planning, business resilience and continuity control environment policies and standards and operational controls. This framework should also test said ICT availability and continuity solutions against a range of realistic scenarios including cyberattacks, fail-over tests and tests of back-ups for critical software and data, with the tests involved entailing planning and documentation and their results contributing to strengthening effectiveness of the solutions they address [5]. In conformity with these guidelines, financial institutions updated their operational risk taxonomies to incorporate risks directly or indirectly related to ICT risks, established independent functions dedicated to those risks and developed a framework serving the aforementioned purposes and assessing their cyber maturity. Cyber risks had to be quantified and their key points revolving around threat management, identity and access management, architectures and infrastructures among others had to be covered along with a BCM framework and strategy plan.

Following these guidelines, in September 2020, the European Commission released a proposed regulation on digital operational resilience for the financial sector aiming to establish a complete and comprehensive framework on digital operational resilience. On December 2022, the regulation was formally adopted by the European Parliament and the Council of the European Union (Regulation (EU) 2022/2554), entering into force in January 2023. Since then, competent authorities were tasked to develop Regulatory Technical Standards (RTS) detailing its practical application and by January 2025 financial institutions must ensure their compliance with the regulation, including implementing necessary ICT risk management frameworks, governance measures, and incident reporting mechanisms and demonstrate it via reporting on their ICT risks. Finally, on March 2024, the supplementing Regulation (EU) 2024/1774 followed that builds on DORA framework. In the next section, we will briefly go through the latest updates in that area.

1.3 Current regulatory landscape

At this point, we have established that cyber risk and data security constitute key drivers of banks' operational risk and are rapidly advancing on the priority list of regulators of financial institutions. According to ECB's SSM supervisory priorities for

2024-2026 reflecting the annually reviewed ECB Banking Supervision's medium-term strategy for the next three years, the European banking sector faces several challenges and, aside from resilience to immediate macro-financial, geopolitical shocks and issues of timely and effective remediation actions, enhanced vigilance is also required in regard to risks stemming from new business practices and technologies in the context of digital transformation and remaining competitive. Supervisory investigations have indicated that some banks have not allocated adequate resources to their digital transformation strategy (business strategy and risk management) whilst resilience and continuity of critical services -even in the event of severe operational disruptions- are challenged by growing cyber threats and increased operational reliance on third-party service providers. Banks will be therefore asked to demonstrate their ability to respond and recover amidst adversity by boosting their progress in digital transformation and strengthening and adjusting their operational resilience frameworks and improve their IT security/cyber risk management.

The aforementioned areas are therefore areas of focus and supervisory priorities. Deficiencies in digital transformation strategies will be addressed via reviews of the impact of digital transformation on the banks' business model/strategy, targeted OSIs (on-site inspections) on digital transformation and publications of supervisory expectations and best practices regarding digital transformation strategies. Regarding deficiencies in operational resilience frameworks (IT outsourcing and IT security/cyber risks) and amidst an increased complexity of supply chains triggered by increasing reliance on third parties, an emphasis will be given in outsourcing risk arrangements as in enhanced third-party management both in terms of understanding of inter-dependencies that can potentially lead to concentration risks and in terms of efficiency through sound asset and vendor management.

On that note, ECB Banking Supervision has established an annual collection of supervised institutions' outsourcing registers and will continue to carry out targeted reviews of outsourcing arrangements and cyber resilience, targeted OSIs and also concluded a System-wide cyber resilience stress test in January 2024 among 109 banks directly supervised by the ECB that focused on the banking sector's response and recovery capabilities from a severe but plausible cybersecurity incident whose results will be included in ECB's 2024 SREP (Supervisory Review and Evaluation Process)

[6]. Banks were asked to demonstrate their ability to activate crisis response plans, communicate with all external stakeholders, analyze affected areas and implementing mitigation measures to enable operation until full recovery of IT systems. Said ability was assessed based on activation of recovery plans including restoring backed-up data and aligning with critical third parties on the incidence response, ensuring the resilience of affected areas and reviewing response and recovery plans [7].

As businesses necessarily continue to evolve, this evolution affecting all lines of operation, and, even more so, given the increased regulatory scrutiny in order for existing and emerging risks to be properly addressed, weaknesses across the traditional three lines of defense (3LOD) risk management model (Business Operational Management, Risk Management and Compliance, Internal Audit) are gradually exposed. DORA pertains to all as its requirements will need to be met and assured by financial institutions and service providers across the industry.

From all the above, it is evident that DORA is a pivotal framework that will urge entities of the financial sector to understand how their practices regarding ICT and operational resilience, third party risk management and cyber impact on the resilience of critical functions, have a sound and well-documented ICT risk management framework and encourage them to develop new capabilities in the area such as scenario testing, much like they manage their other risks. The importance of such an initiative justifies the incentive behind the conduction of the current essay as new developments on the subject unfold, technical standards are finalized and entities within the scope of DORA should put substantial effort into improving their ability to assess and enhance their operational resilience related capabilities.

2. Literature Review & Objectives

2.1 General overview of the DORA Framework: Main Pillars & Policy Mandates

The focus of this chapter will be to explore the imperative of DORA top-down, looking into what this framework brings to the table in the direction of enhanced security and resilience through examination of regulatory texts. We will first discuss the main pillars of the framework and policy mandates that have been developed by the competent authorities then proceed to a brief mention of its provisions per area and, finally, outline the objectives of the current essay.

As priorly discussed, the main objective of DORA is to harmonize rules framing operational resilience for the financial sector applying to 20 different types of financial entities and ICT third-party service providers as stated in its Article 2. DORA is lex specialis to the Network Information Security (NIS) Directive and to Article 11 and Chapters III, IV and VI of the Critical Entity Resilience (CER) Directive.

The main pillars of DORA according to EIOPA briefly constitute of:

a. **ICT risk management** (Chapter II of Regulation (EU) 2022/2554) as in principles and requirements on the ICT risk management framework. Financial entities' management bodies are urged to take accountability and assume and distribute responsibilities for the management of ICT risks, reviewing and approving policies involving the use of ICT TTPs, for setting and approving a digital operational resilience strategy. DORA assumes and extends requirements outlined in previous ESAs guidelines' efforts (such as EIOPA's "Guidelines on information and communication technology security and governance"), conferring on them a binding nature and placing the level to which they are put through under regulatory scrutiny.

b. **ICT third party risk management** (Chapter IV.I of Regulation (EU) 2022/2554) framing monitoring of ICT third-party providers, key contractual provisions and ROI (register of information) on said providers.

c. **Oversight framework for critical ICT TPPs** (Chapter IV.II of Regulation (EU) 2022/2554) involving the designation of a Lead Overseer appointed from one of the ESAs to coordinate and execute oversight tasks and obligations of critical ICT TTPs and financial entities as well as enforcement of corrective measures and sanctions.

d. **Digital operational resilience testing** (Chapter V of Regulation (EU) 2022/2554). DORA establishes resilience testing requirements of -at least- annual frequency, covering testing of ICT tools and systems and advanced testing based on TLPT.

e. **ICT – related incident management, classification, and reporting** (Chapter III of Regulation (EU) 2022/2554) to competent authorities and notification of stakeholders.

f. **Information sharing arrangements** (Chapter VI of Regulation (EU) 2022/2554) on cyber threat information and intelligence.

The operationalization of the DORA framework mandated the joint preparation through the Joint Committee (JC) of a set of products (guidelines and Regulatory Technical Standards) by the ESAs, the most current versions of which are depicted in the following table per DORA Pillar as summarized above [8]. Additionally, on 25 June 2024, three relevant Commission Delegated Regulations (CDRs) were published in the Official Journal of the EU: CDR (EU) 2024/1772 on RTS specifying the criteria for the classification of ICT-related incidents and cyber threats, CDR (EU) 2024/1773 on RTS specifying the detailed content of the policy regarding contractual arrangements framing ICT services supporting critical or important functions provided by ICT third-party service providers and CDR (EU) 2024/1774 on RTS specifying ICT risk management tools, methods, processes and policies and the simplified ICT risk

management framework. These products will be discussed in more detail in the following chapter. The table below provides a mapping of regulatory products per DORA Pillar:

Pillar	Products	Article(s).Section(s)
a. ICT risk management	a1) Draft RTS on ICT Risk Management Framework and on simplified ICT Risk Management Framework	15,16
	a2) Joint Guidelines on the estimation of aggregated annual costs and losses caused by major ICT-related incidents	11.1
b. ICT third-party risk management	b1) Draft RTS to specify the policy on ICT services supporting critical or important functions	28.10
	b2) Draft ITS on Register of Information & illustrative excel template	28.9
	b3) JC 2024-53_Final report DORA RTS on subcontracting	30.5
c. Oversight framework for critical ICT TPPs	c1) Joint Guidelines on oversight cooperation	32.7
	c2) Joint Regulatory Technical Standards on the harmonization of conditions enabling the conduct of the oversight activities	41
d. Digital operational resilience testing	d1) Joint Regulatory Technical Standards specifying elements related to threat led penetration tests	26.1
e. ICT related incident management classification and reporting	**e1) Draft RTS on classification of major incidents and significant cyber threats**	18.3
	e2) Joint Technical Standards on major incident reporting	20.a,.b
Other	Joint Regulatory Technical Standards on the criteria for determining the composition of the joint examination team	

*products denoted in bold refer to mandates with impact on reporting

Table 1 – Regulatory Products Per DORA Pillar

2.2 General overview of relevant standards and frameworks

In order to deliver the mandates of DORA, "the ESAs have duly considered existing European and international standards on ICT risk management, such as EBA Guidelines on ICT and security risk management (2019), EIOPA Guidelines on ICT security and governance (2020), NIS2 Directive and the NIST cybersecurity framework components, as well as ISO-IEC 27000 family standards, 2020 FSB CIRR toolkit, the G7 Fundamental Elements of Cyber security in the financial sector, CPMI-IOSCO Guidance on cyber resilience for financial market infrastructures, and the BCBS

principles for operational resilience and sound management of operational risk, effective risk data aggregation and risk reporting". Further to that, common industry terms are used as defined in ISO standards for understanding and implementation purposes [9]. Therefore, identifying elements across standards closely linked to DORA mandates provides useful insight on what those bring to the table in comparison for FEs.

For the purposes of the comparative analysis that will follow in the next chapter, in this section, we will proceed to identify the relevant existing standards to the main pillars of DORA that will form the basis for the current essay's objectives. The following Table briefly illustrates the frameworks in close relevance to DORA's main Pillars.

DORA Pillars	Frameworks				
	ISO/IEC 27001	ISO/IEC 22301	ISO/IEC 31000	ISO/IEC 27036	TIBER-EU
a. ICT risk management	✓	✓	✓	✓	
b. ICT third-party risk management	✓	✓	✓	✓	
c. Oversight framework for critical ICT TPPs					
d. Digital operational resilience testing	✓	✓	✓	✓	✓
e. ICT related incident management classification and reporting	✓	✓	✓	✓	✓
f. Information sharing arrangements	✓	✓	✓	✓	

Table 2 – Relevant Frameworks Per DORA Pillar

At this point, we will proceed with a general overview of said standards whose key points will be discussed directly or indirectly in more detail in the context of DORA.

- ✓ **ISO/IEC 27001** is the leading international standard for managing information security by providing a framework of policies and procedures (methods, processes, tools) framing the implementation, maintenance, and continual improvement of an information security management system (ISMS) that takes as input information security requirements and outputs information security outcomes that address them as well as requirements for the assessment and treatment of information security risks tailored to the needs of the organization. The requirements set out are generic in nature to accommodate applicability across all types of organizations. Its key components consist of a list of

information security controls, and areas of scope and context, roles and responsibilities, risk management, monitoring of risk, performance and compliance and documenting, communication and awareness, supplier relationships, internal audit, management of incidents and continual improvement.

- ✓ **ISO/IEC 22301** is the international standard for business continuity management (BCM) and provides a framework for the identification of threats to the organization and building the capability for effective incidence response. Its key components consist of the areas of business impact analysis, risk assessment, business continuity strategies and incidence response and recovery planning.

- ✓ **ISO/IEC 31000** provides guidelines in the direction of managing risks and integrating risk management processes (risk assessment, risk treatment, monitoring and review, effective communication, and consultation) into the organizational processes, complimenting ISO/IEC 27001.

- ✓ **ISO/IEC 27036** covers guidelines regarding the management of information security in supplier relationships, ensuring that the security of information is maintained throughout the supply chain and its key components concern supplier risk management and security controls in contracts and monitoring and reviewing supplier performance and the level of protection of shared information.

- ✓ **TIBER-EU** is an initiative of the ECB in the direction of developing a framework for Threat Intelligence-based Ethical Red Teaming aimed at enhancing cybersecurity resilience of the financial sector in the EU. Intelligence-led red team tests mimic the tactics, techniques and procedures of real-life threat actors and involve the use of a variety of techniques to simulate an attack on an entity's critical functions (CFs) and underlying systems (i.e., its people, processes and technologies), assisting an entity in assessing its protection, detection and response capabilities [10]. On May 2018, the ECB provided a framework document detailing the key phases involved in the

TIBER-EU test along with several supporting documents for its implementation. This Framework is directly linked to DORA as the targeted RTS for threat led penetration tests is based on its mandatory principles that are also within the scope of the DORA mandates.

2.3 Objectives

In this section, we will proceed to outline the three primary objectives of the current essay:

1. **Addressing DORA requirements in conjunction with regulatory guidelines and technical standards as they have been developed in their most recent versions and their complementary CDRs:** Following the public consultations of proposed draft RTSs, most technical standards framing the main DORA Pillars have been set out, along with templates where applicable. In the next chapter, we will navigate this material that provides a more thorough understanding on DORA mandates.

2. **Performing a comparative analysis with relevant standards:** Provided how dynamic the ICT risk environment is and that FEs, as part of their ICT security policies, procedures, protocols, and tools, are expected to develop and implement an ICT asset management policy, capacity and performance management procedures, and policies and procedures for ICT operations that ensure: the monitoring of the status of ICT assets throughout their lifecycles, the optimization of ICT systems' operation and performance meets the established business and information security objectives and that said are operating and managed effectively day-to-day, the importance for ICT security policies developed by FEs to be based on leading practices and standards was outlined in supporting DORA documentation [1]. It is therefore evident that identifying intercept points between DORA's mandates and relevant standards and frameworks will complement the previous objective.

3. Leveraging the first two objectives, the third objective will address **the development of a checklist on DORA's requirements in the form of an Excel tool.**

3. ESAs' Technical Standards & comparative analysis of DORA requirements and other security enhancing standards

3.1 Analysis of DORA Provisions and regulatory products per Pillar

3.1.1 ICT Risk Management

The commitment of the ESAs towards strengthening ICT risk management frameworks within FEs is exemplified by providing guidelines through RTS providing further specifications to harmonize ICT risk management tools, methods, processes, and policies across FEs, aiming to ensure a consistent and effective implementation of robust ICT risk management frameworks throughout the sector. In this subsection, we will proceed to look into these guidelines and how they complement DORA mandates.

Article 5 of DORA focuses on Governance and Organization establishing requirements for FEs to implement effective ICT risk management and specific responsibilities for the management body in relation to Article 6 that requires FEs to establish and maintain a comprehensive ICT risk management framework that ensures their ability to withstand, respond to, and recover from ICT-related disruptions including ICT security policies and protocols, methods to attain ICT strategies and business objectives, measures for identifying and assessing risks and the aspect of continuous improvement through monitoring in close relevance to most clauses of ISO/IEC 27001 regarding Leadership, Planning, Operation, Performance Evaluation and Improvement. Articles 8 to 10 are concerned with the aspects of Identification, Protection-Prevention and Detection and Articles 11 and 12 address business continuity aspects of Response and Recovery and Backup policies and procedures and Recovery procedures and methods including checks and reconciliations to ensure maintenance data integrity and consistency, all indicative of the high level of preparedness required. Article 13 focuses on impact assessment of ICT-related incidents and ICT-related disruptive incident reviews in conjunction with the ICT risk assessment process, business continuity plans and ICT response and recovery plans under the prism of

monitoring the effectiveness of the latter and mapping evolution of the FEs' ICT risk over time. Finally, Article 14 is concerned with communication strategies and policies and Article 15 with the required specifications of the components comprising the aspects discussed on all the previous Article that shall all be part of a risk management framework. FEs are to consider articles 6 to 14 of DORA together with the RTS developed for that purpose and discussed in the following subsection and consider the integration of outlined policies and procedures in their ICT risk management framework.

3.1.1.1 Draft RTS on ICT risk management framework and on simplified ICT risk management framework

Under its Article 15 , DORA tasks the ESAs to develop RTS in the direction of "further harmonization of ICT risk management tools, methods, processes and policies, and under Article 16 (3), to develop a simplified ICT risk management framework for certain FEs, taking into account the size and the overall risk profile of the FE, and the nature, scale and complexity of its services, activities and operations, while duly taking into consideration any specific feature arising from the distinct nature of activities across different financial services sectors" [11]. The general principles provided by the relevant RTS are technology-neutral and sector agnostic. At this point, we will proceed to identify the key elements contained in the relevant RTS based on our judgement and this will be the process followed across all RTS given the density and cross-references (that will be as high-level as possible) of the contained information. The summary of contents of the RTS is depicted in the following figure:

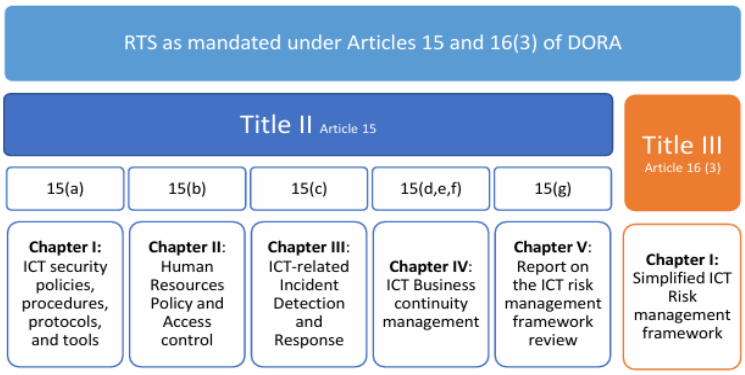

Figure 1 – Contents of RTS on ICT risk management framework and on simplified ICT risk management framework [9]

In paragraph 26, a summary of specific elements required per area is outlined in a table, indicating which areas require only policies or only procedures, which require specific elements of both (outlined under both only policies and only procedures), and 4 areas are outlined under policies and procedures without specifying which elements should go in policies and which in procedures, as it was acknowledged that some elements are more principles and fit for policies and other are more elements of practical / technical implementation and thus more fit for procedures. As such the required leeway is provided for FEs to choose those elements for the areas in which both policies and procedures are needed. It is also highlighted that these areas are not exhaustive as per what policies and procedures in their ICT risk management framework should be developed and implemented.

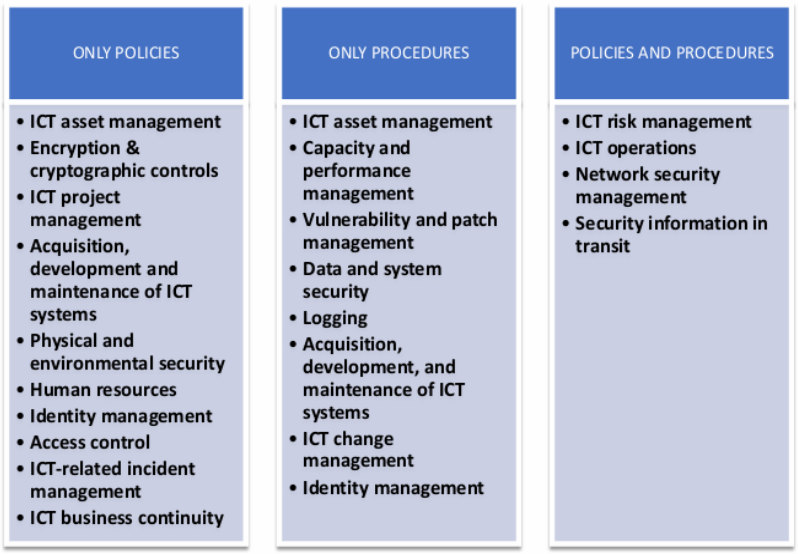

Figure 2 – Overview of policies and procedures [9]

As per what was outlined in Figure 1, Chapter I of the RTS is focused on "the mandate established in Article 15 (a) of DORA, which requires specifying further elements to be included in the ICT security policies, procedures, protocols and tools referred to in Article 9(2) of DORA". Schematically, the components addressed, as in constituting the key elements of the ICT risk management framework, are depicted as such:

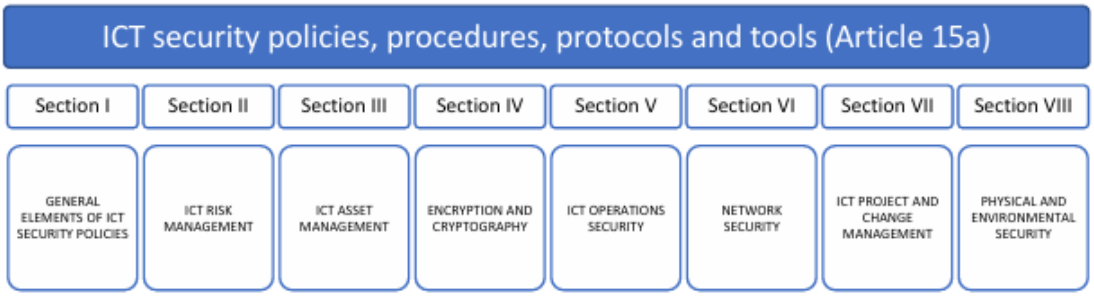

Figure 3 – Article 15(a) components [9]

The simplified version of the above based on proportionality as per Article 16 (3) is the following:

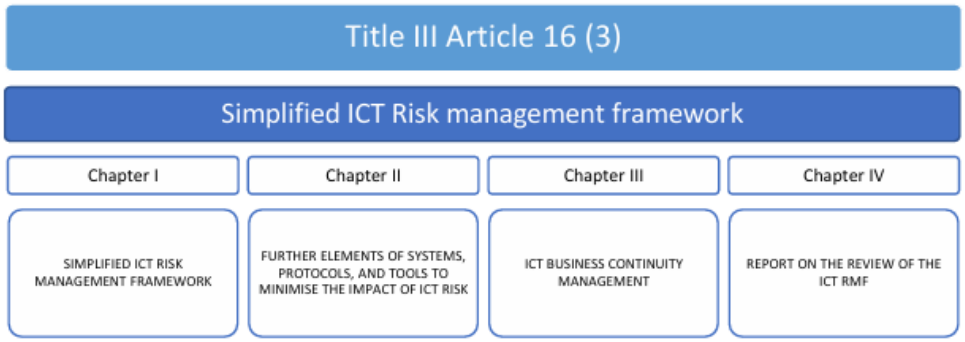

Figure 4 – Article 16(3) components [9]

It is noted that provisions on Governance have been omitted post public consultation and the need for provision of additional guidance in the future will be assessed. We will proceed to briefly go through the provisions for the Sections II-VIII as per Article 15(a) so as to have a clearer picture of the requirements for the next objectives of the current essay.

✓ Section II: ICT RISK MANAGEMENT

Its purpose is to outline the minimum requirements applicable to FEs regarding the development and documentation of their ICT risk management policies and procedures. FEs are required to:

i. establish an ICT risk management policy that includes the necessary measures and procedures for effectively managing ICT risk with clear

definitions for the approved risk tolerance levels for each type of risk identified so as to proactively address and mitigate ICT risk, safeguard data, and maintain the overall security and resilience of their operations.

ii. establish a process and a methodology to conduct their ICT risk assessment that identifies vulnerabilities and threats that affect or may affect business functions, ICT systems, and supporting ICT assets also comprising quantitative or qualitative indicators to measure the impact and likelihood of occurrence of these vulnerabilities and threats.

iii. have a comprehensive and systematic approach to treating ICT risk identified through the ICT risk assessment so that they can mitigate and manage ICT risk in line with their risk tolerance levels contributing to their overall resilience and security of their ICT systems and operations. They should also have a structured approach to identify, accept, document and review residual risks, the latter being integrated within the general risk management process, as well as identify responsibilities regarding their acceptance.

iv. monitor changes occurring within their ICT environment (internal and external vulnerabilities) and their ICT risk to ensure they have an up-to date understanding of their risk landscape through tracking and assessing the various risks associated with their ICT systems, applications, and infrastructure as well as its alignment with changes in the business strategy and digital operational resilience strategy to ensure that it remains relevant.

✓ Section III: ICT ASSET MANAGEMENT

FEs are required to:

i. correctly identify, classify and adequately document, among others, ICT assets and information assets. On that note, Article 4 requires the establishment of a policy for the management of ICT assets, complementing the elements included in Article 8(6) of DORA with respect to the inventory

of the ICT assets and information assets. The feedback from public consultation indicated that stakeholders considered important to keep record of the end date of the provider's support or the date of the extended support of ICT assets.

ii. place special focus on those ICT assets or systems necessary for business operation, considering their criticality and potential impact in case of the loss of their confidentiality, integrity and availability and define and implement a procedure to perform a criticality assessment of the information and ICT assets.

✓ Section IV: ENCRYPTION AND CRYPTOGRAPHY

FEs are also required to:

i. establish a comprehensive policy on encryption and cryptographic controls, incorporating key elements to effectively manage these security measures (taking into consideration data classification and ICT risk assessment results) and encryption of internal network connections and traffic with external parties, considering data criticality and classification.

ii. strive to identify and adopt the most effective practices for their specific circumstances while having a forward-looking perspective, taking into consideration leading practices, reliable techniques, and the classification of involved ICT assets. If they cannot adhere to leading practices or standards, they should implement and keep records of mitigation and monitoring measures to maintain resilience against cyber threats. This also applies in the cases where updating or changing cryptographic technology is not feasible.

iii. establish and document a cryptographic key management policy as an integral part of the overall encryption policy which should establish guidelines for the correct use, protection, and lifecycle management of cryptographic keys, ensuring their secure generation, storage, distribution, and disposal.

✓ Section V: ICT OPERATIONS SECURITY

This section is involved with five areas: (i) policies and procedures for ICT operations, (ii) capacity and performance management, (iii) vulnerability and patch management, (iv) data and system security and (v) logging. Within the respective areas, FEs are required to:

i. cover key elements such as installation, maintenance, configuration, and deinstallation of ICT assets, as well as controls and monitoring of ICT systems, error handling, and recovery procedures in order to minimize disruptions to business operations, detect and respond to security incidents promptly, and ensure the continuity and security of their services. Additional requirements apply for cases where testing is conducted in production environments.

ii. identify the capacity requirements of their ICT systems and implement resource optimization and monitoring procedures with special attention to be given to systems with long or complex procurement processes or those that are resource intensive.

iii. establish procedures to detect vulnerabilities and update relevant information resources accordingly. Regular automated vulnerability scanning and assessments, typically using specialized software tools, of ICT assets are required so as to cover the widest range of assets possible in an automated way based on their classification and overall risk profile, and at least on a weekly basis for those ICT assets supporting critical or important functions. Further, ICT third-party service providers should handle any vulnerabilities and report them to the FEs. The tracking of ICT third-party libraries (including tracking patches and updates), disclosure of vulnerability-related information, and deployment of patches are also vital and patch deployment prioritization should be made based on vulnerability criticality and risk profiles, while monitoring and verifying remediation. “FEs should also record detected vulnerabilities, evaluate software and hardware patches and updates, test and deploy them in a controlled

environment, and establish emergency procedures and deadlines for installation".

iv. ensure "the security of networks against intrusions and data misuse, and preserve the availability, authenticity, integrity and confidentiality of data is the data and system security. To this end, FEs should implement the various security measures outlined in Article 15 of DORA".

v. identify events to be logged, set retention periods, and secure log data for effective monitoring and investigation of ICT security incidents, protect logging systems from data tampering. Clock synchronization aids incident response and forensic analysis. "The level of detail in logs should align with their purpose and the usage of the ICT asset producing the log".

✓ Section VI: NETWORK SECURITY

FEs are required to:

i. develop policies, procedures, protocols, and tools to ensure the security of networks including segregation and segmentation of ICT systems and networks based on their criticality, classification, and risk profile. The mapping and visualization of networks provide an overview for effective management.

ii. take measures to mitigate unauthorized risks, design networks in accordance with security requirements and industry leading practices, secure network traffic between internal networks and external connections, regularly review connection filters and network architecture, limit potential attack vectors, ensure that security requirements are met for services provided either by an ICT intra group service provider or by ICT third-party service providers.

iii. develop policies, procedures, protocols, and tools to protect data transfer regarding securing information in transit and take measures to prevent data leakage and secure information transfer with external parties, taking into account the results of the approved data classification and the ICT risk

assessment processes. FEs should also comply with data protection laws for the transfer of personal data.

✓ Section VII: ICT PROJECT AND CHANGE MANAGEMENT

FEs are required to:

i. have an appropriate ICT project and change management framework in place.

ii. design a policy on the acquisition, development and maintenance of ICT systems, focused fundamentally on the testing of these systems and on the security implications that can be derived from these processes.

iii. test and approve changes and focus on governance of such changes and on the procedures for making urgent changes or reversing changes made if necessary.

iv. have specific provisions for Central Counterparties (CCPs) and Central Securities Depositories (CSDs). These provisions mirror those found in existing delegated regulations under the European Market Infrastructure Regulation (EMIR) and Central Securities Depositories Regulation (CSDR) and CCPs and CSDs should test their ICT systems both prior to their use and after significant changes, and include the minimal list of external stakeholders they should involve in such tests, if they consider such involvement appropriate.

✓ Section VIII: PHYSICAL AND ENVIRONMENTAL SECURITY

The implementation of a relevant policy, aimed at specifying its elements with respect to securing premises, data centers, sensitive designated areas and hardware equipment inclusive of measures such as the protection of ICT assets against unauthorized access, attacks, accidents and from environmental threats and hazards, and the proper maintenance of these assets is required. With respect to bespoke hazards and measures, financial entities are encouraged to use international standards, such as

ISO 27002 as further guidance. Further, a need for a clear desk policy for papers and a clear screen policy for information processing facilities is established.

Proceeding with Chapter II of the RTS, it is concerned with human resources policy and access control set out under Article 15(b) of DORA closely linked to Article 9(4)(c) that mandates the implementation of policies that "limit the physical or logical access to information assets and ICT assets to what is required for legitimate and approved functions and activities only, and establish to that end a set of controls that address access rights and ensure a sound administration thereof". The Chapter comprises three areas: Human resources policy ("requirements on contracts, covering the pre-employment phase, on communication and awareness, the employment period and on requirements to be considered after the termination of the contractual relationship", taking into consideration controls and measures identified in the ISO/IEC 27001 and ISO/IEC 27002 standards), Identity management ("elements to be included by FEs as part of their controls on access management rights, in the policies and procedures to ensure the unique identification of natural persons and systems accessing the financial entities' information. Provisions related to the management of user accounts and linked identities are also included") and Access control (elements to be included by FEs in their access control policy addressing topics of governance, authentication methods, strategy, access rights and physical access.

Chapter III covers the aspect of ICT-related incident detection and response which will be looked into in the next subsections as there is a dedicated RTS on incident management, classification, and reporting. Chapter IV is focused on ICT business continuity management following the mandates of Articles 11, 24, 25 and 26 of DORA. Article 11(4) "establishes the need to maintain and periodically test ICT business continuity plans, notably with regard to critical or important functions outsourced or contracted through arrangements with ICT third-party service providers" and Article 11(5) the obligation to conduct a business impact analysis (BIA). Finally, Chapter V focuses on Article 6(5) of DORA establishing the obligation to document and review the ICT risk management framework, ensuring of its continuous improvement. Article 27 of the RTS elaborates on the content that is expected from such report, covering the minimum elements that should be included in it [9].

3.1.1.2 Joint Guidelines on estimation of aggregated annual costs and losses caused by major ICT-related incidents

Article 11(11) of DORA mandates that ESAs develop "common guidelines on the estimation of aggregated annual costs and losses caused by major ICT-related incidents" in the direction of harmonizing the estimation by FEs of their aggregated annual costs and losses caused by major information and communication technology (ICT)-related incidents according to Article 11(10) DORA, which are then to be submitted by financial entities, other than microenterprises, to their CA upon its request (non-major incidents are out of scope of the Guidelines). We will proceed to outline very briefly two points addressed in the relevant RTS relevant to the reporting:

i. The ESAs have decided to allow financial entities to choose which reference year they intend to use for reporting purposes (calendar or accounting) with future annual reports being consistent on that aspect. If the FE wants to change that decision, this should be notified to the CA that has a 2-month period to object.

ii. The Guidelines specify a common template for the submission of the aggregated annual costs and losses for major ICT-related incidents (irrespective of the reason, all incidents that have been reported as major according to DORA) that fall within the reference year for which the CA requested the estimation or that had been submitted in previous reference years and had a quantifiable financial impact on the FE in the relevant reference year as well as financial recoveries (in 1000s units). The derivation of gross costs and losses (costs or losses that the FE paid or booked) and recoveries will be the result of the estimation of costs and losses of each major ICT-related incident individually as well as the financial recoveries and as such it will also be reported (per incident). In their estimation, FEs should also include accounting provisions that are reflected in their financial statements such as the profit and loss account of the relevant reference year. Where accurate data is not available, FEs should

base their estimation on other available data and information to the extent possible [12].

3.1.2 ICT Third-Party Risk Management

Chapter V of the DORA Regulation addresses the management of ICT-related third-party risks. Article 28(1) underlines the general principles based on which FEs are to manage this risk as an integral component of ICT risk within their ICT risk management framework. The first principle concerns full responsibility and accountability of FEs on contractual arrangements for the use of ICT services to run their business operations and their compliance with all obligations under the DORA Regulation and applicable financial services law. The second revolves around the notion of proportionality that should be taken into account for the management of ICT third-party risk, both in regard to the nature, scale, complexity and importance of ICT-related dependencies and the criticality or importance of the respective service, process or function concluded with ICT third-party service providers, and its potential impact on the continuity and availability of financial services and activities, at individual and at group level.

- ***ICT third-party risk strategy & ROI***

FEs, other than those exempted as of Article 16(1) of the Regulation and other than microenterprises, shall adopt, and regularly review, a strategy on ICT third-party risk, taking into account the multi-vendor strategy referred to in Article 6(9) (where applicable) and that strategy being inclusive of a policy on the use of ICT services supporting critical or important functions provided by ICT third-party service providers that shall be applicable on an individual basis and, where relevant, on a sub-consolidated and consolidated basis and regularly reviewed along with the identified risks stemming from contractual arrangements based on the assessment of the overall risk profile of the entity and the scale and complexity of its business services.

Moreover, as part of their ICT risk management framework, FEs shall maintain and update at entity level, and at sub-consolidated and consolidated levels, a register of information in relation to all contractual arrangements on the use of ICT services provided by ICT third-party service providers. Said arrangements shall be appropriately documented, distinguishing between those that cover ICT services supporting critical or important functions and those that do not, and FEs shall report at least yearly to the competent authorities on the number of new arrangements on the use of ICT services, the categories of ICT third-party service providers, the type of contractual arrangements and the ICT services and functions which are being provided and have, upon request, the full register of information available along with any information deemed necessary under the prism of effective supervision [11]. In the next subsection, we will proceed to look into the draft Technical Standards framing the composition of return on information templates and aiming to ensure a minimum level of harmonized content, promote continuous screening of dependencies and enhance supervisory efficiency.

- ***Contractual Agreements & effective management and auditing of services***

Further on contractual agreements, the DORA Regulation specifies that, before entering into one, FEs shall assess and take into consideration several criteria such as:

- ✓ whether the ICT services concerned cover a critical/important function.
- ✓ whether supervisory conditions are met.
- ✓ identify and assess a priori all -relevant to the arrangement- risks including whether it would lead to an elevated risk concentration. This particular point is covered in Article 29 of the DORA Regulation where it is stated that it should be taken into consideration whether the ICT third-party provider is not easily substitutable and whether multiple critical services are linked to the same provider or closely connected ICT third-party service providers and that these considerations should be assessed in conjunction with weighing costs and benefits of alternative solutions such as the use of alternative providers and how they align to business needs and objectives set out in the digital resilience strategy of FEs.

- ✓ involvement of due diligence on prospective providers to verify their capability, reliability, and resilience, ensuring the provider's suitability throughout the selection and assessment phases included.
- ✓ identification of conflicts of interest that might arise.
- ✓ compliance of ICT third-party service providers with appropriate information security standards. When contractual arrangements concern critical or important functions, FEs shall take due consideration of the use, by ICT third- party service providers, of the most up-to-date and highest quality information security standards prior to concluding the arrangements [11].

Additional topics covered in this Chapter closely follow EBA Guidelines on outsourcing arrangements (EBA/GL/2019/02) (whose main points were briefly discussed in 1.2 of the current essay) and concern the exercise of access, inspection and audit rights over the ICT third-party service provider, termination rights and circumstances under which termination may occur and exit strategies, with an emphasis given to the auditing of services (especially those that entail high technical complexity) as a product of a risk-based approach, with a pre-determined frequency and adherence to commonly accepted audit standards in line with any supervisory instruction on the use and incorporation of such audit standards [11]. Along with ROI templates, a relevant regulatory product that we will also look into in the next subsections will be the Joint RTS on subcontracting ICT services supporting critical or important functions that specifies, among others, the elements that an FE needs to determine and assess when subcontracting ICT services supporting critical or important functions as mandated by Regulation (EU) 2022/2554 and under the prism of a cost-benefit analysis [11].

3.1.2.1 RTS on Register of Information (ROI)

Article 28(9) of DORA mandated ESAs to develop draft implementing technical standards in the direction of establishing the standard templates for the purposes of the ROI, including information that is common to all contractual arrangements on the use of ICT services [13]. Following this, a relevant Consultation Paper (CP) set the foundation for templates aiming to enable FEs to capture minimum

and necessary information concerning the contractual arrangements and the assessment of the related risks stemming from them for FEs and the ICT supply chain with a focus on material subcontractors, identify unambiguously and consistently the ICT third-party service providers and the FEs by using the Legal Entity Identifier (LEI) code thus enabling efficient aggregation of all relevant information, identify all functions supported by the ICT services provided by ICT third-party service providers whilst distinguishing critical ones and, in the case of groups, capture internal (exclusively) within the group and external contracts.

ROI is thus composed as a set of open tables, all linked to each other by using different specific keys in order to form a relational structure and the proposed templates were to be maintained and updated initially: i. at an entity level (concern the financial entity maintaining ROI) and ii. at sub-consolidated and consolidated level entailing the same templates as those maintained at entity level plus additional templates used to link the registers of information of the various entities in scope of the group and to ensure uniqueness of entries (no double counting).

Post public consultation feedback however, one set of templates was instead set out, encompassing all the information. On that note, to enable the operability of the ROI at entity, sub-consolidated and consolidated level across all the FEs that are part of the same group, FEs should ensure the uniformity, correctness and consistency of all the data in the ROI (unicity and consistency across the scope of consolidation of the different keys e.g. the contractual arrangement reference numbers, the function identifier and the unique identifiers of the financial entities and ICT third-party service providers (i.e. 'LEI')) [13]. Apart from the templates containing the FE maintaining the ROI at entity level, list of entities within the scope of ROI & list of branches (RT.01.01 & RT.01.02 & RT. 01.03) and the template containing meanings and definitions of the closed set of indicators used in the ROI (e.g. specification of the meaning of "high", "medium", "low" options regarding the impact of discontinuation of the ICT services) (RT.99.01), all ROI templates are linked to one another by using relational keys. These are Contractual Arrangement Reference Number, LEI of Entity making use of the ICT Services, ICT Service Provider Identifier, Function Identifier and Type of ICT Services (Annex III). Annex III includes a table of identifiers per Type of ICT services (e.g. S06 refers to Data analysis as in provision of services related to the support for data analysis

(digital data service)). Figure 1 depicts the set of templates and how they are linked via the relational keys. Table 3 summarizes the content of each template.

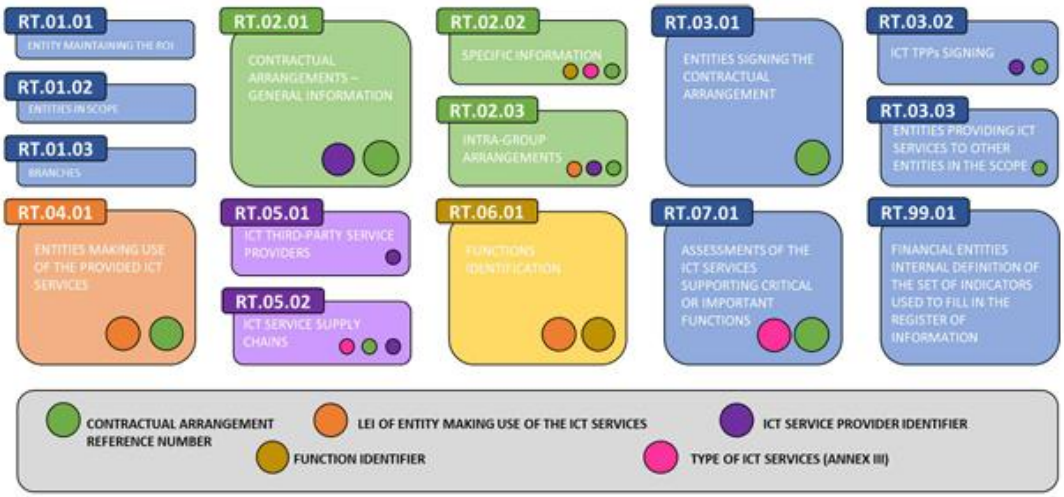

Figure 5 – ROI templates [13]

Templates maintained (as per Final Report)
RT.01.01 - Financial Entity maintaining the register of information
Identification of the financial entity maintaining the register of information at entity level
RT.01.02: List of entities within the scope of the register of information
List of all the FEs belonging to the group. In case the financial entity responsible for maintaining and updating the register of information does not belong to a group, only this financial entity shall be reported in this template
RT.01.03: List of branches
List of all branches of the FE, identified in RT.01.02
RT.02.01 - Contractual Arrangements – General Information
List of all contractual arrangements between the financial entity and its direct ICT third-party service providers. For each contractual arrangement, the financial entity shall assign a unique 'contractual arrangement reference number' to identify unambiguously the contractual arrangement itself
RT.02.02 - Contractual Arrangements – Specific Information
Provision of details in relation to each contractual arrangement listed in RT.02.01 with regard to: (i) the ICT services included in the scope of the arrangement, (ii) the functions of the financial entities supported by those ICT services, (iii) other important information in relation to the specific ICT services provided (e.g. notice period, law governing the arrangement, etc.)
RT.02.03 - List of intra-group contractual arrangements
Identification of the links between intra-group contractual arrangements and contractual arrangements with ICT third-party service provider which are not part of the group using the **'contractual reference numbers'** when part of the ICT service supply chain
RT.03.01 - Entities signing the Contractual Arrangements for receiving ICT service(s) or on behalf of the entities making use of the ICT service(s)
Information on the entities signing the contractual arrangements with the direct ICT third-party service providers on behalf of the entities making use of the ICT services. Within the scope of sub-consolidation and consolidation, the financial entity making use of the ICT services provided is not necessarily the entity signing the contractual arrangement with the ICT third-party service providers

RT.03.02 - ICT third-party service providers signing the Contractual arrangements for providing ICT service(s)
Identification of all the ICT third-party service providers referred to in template RT.05.01 signing the contractual arrangements referred to in template RT.02.01 for providing the ICT service
RT.03.03 - ICT third-party service providers signing the Contractual arrangements for providing ICT service(s) to other entities within the scope of consolidation
Identification of all the entities referred to in template RT.01.02, signing the contractual arrangements referred to in template RT.02.01 for providing ICT services to other entities in the scope of consolidation
RT.04.01 - Entities making use of the ICT services
List of all entities making use of the ICT services provided by the ICT third-party service providers. The entities making use of the ICT services shall be either the FEs in scope or the ICT intra-group service providers. In case the ROI is maintained and updated at entity level, the entity signing the contractual arrangement and the entity making use of the ICT services are the financial entity maintaining the register
RT.05.01- ICT third-party service providers
List and general information for the identification of: (i) the direct ICT third-party service providers, (ii) the ICT intra-group service providers, (iii) all subcontractors included in template RT.05.02 on ICT service supply chains, (iv) identifying the ultimate parent undertaking of the ICT third-party service providers listed in points (i) to (iii)
RT.05.02 - ICT service supply chains
Identification and linking of the ICT third-party service providers that are part of one ICT service supply chain. FEs shall identify and rank the ICT third-party service providers for each ICT service included in the scope of each contractual arrangement and link the ICT service providers (including intragroup service providers) as well as subcontractors supporting a critical or important function or material parts thereof (rank 1 - Direct ICT third-party service providers, rank 2 - Subcontractors of direct ICT third-party service providers, rank 3 -Subcontractors of rank 2 subcontractors etc.). All ICT third-party service providers belonging to the same ICT service supply chain share the same **'contractual arrangement reference number'** as referred to in template RT.02.01 and the same type of ICT services
RT.06.01 - Functions identification
Identification and provision of information on the functions of the FE, including a unique identifier, the **'function identifier'** for each combination of licensed activity and function
RT.07.01 - Assessments of the ICT services
Information in relation to the assessment on the ICT services performed by the FE (e.g. substitutability, date of last audit, etc.)
RT.99.01 - Definitions from Entities making use of the ICT Services
Entity-internal explanations, meanings and definitions of the closed set of indicators used in the ROI

Table 3 – Content Per ROI template

Regarding ICT service supply chains, the notion of 'rank' is indicative of the position of an ICT third-party service provider in the ICT service supply chain. The rank assigned to each ICT third-party service provider is any natural number higher or equal to '1'. The lower the natural number assigned to the rank, the closer the arrangement is to the financial entity [13]. A schematic depiction of this is the following:

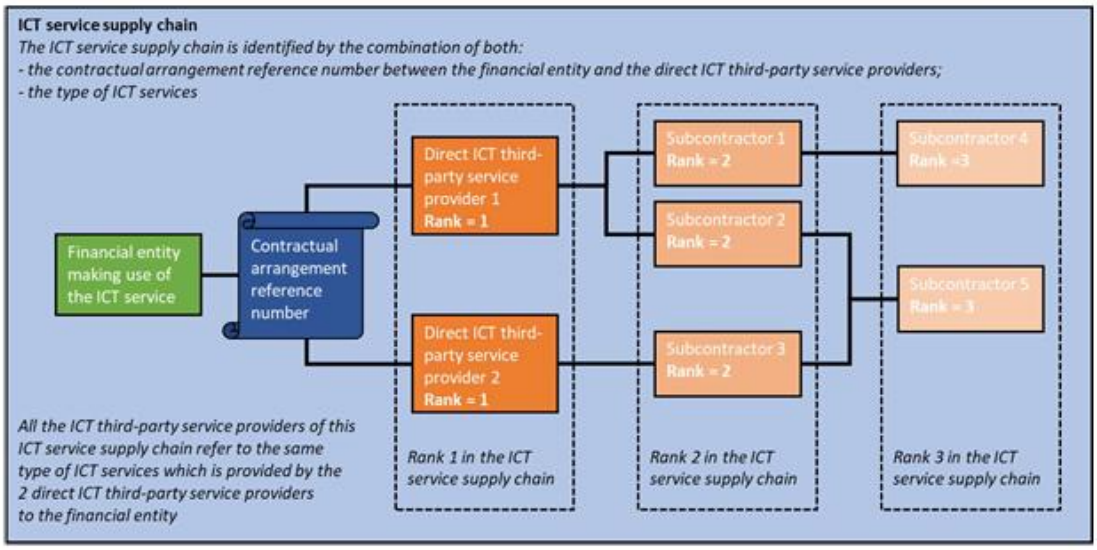

Figure 6 – ICT service supply chain illustration [13]

3.1.2.2 Joint RTS on subcontracting ICT services supporting critical or important functions

As per Article 30(5) of DORA, ESAs were mandated to "develop draft regulatory standards to specify elements which a FE needs to determine and assess when subcontracting ICT services supporting critical or important functions" [11]. The legal requirements for compliance set out in the key principles for the management of ICT third-party risk in Section I of Chapter V constitute the baseline scenario of an impact assessment whilst the developed RTS strives to address areas that require further specification.

The first part of the RTS was dedicated to the specification of elements set out in Article 30(2) regarding contractual provisions. The second part was dedicated to impact assessment and, more specifically, to addressing the issues of monitoring of the subcontracting chain, proportionality and definition of ICT services and critical and important functions. Regarding the former, three potential approaches were considered: Option A that involved monitoring ICT risk across the entire subcontracting chain, with particular focus on subcontractors that directly underpin critical or important functions, Option B that involved limiting the monitoring to a select number of subcontractors and

Option C that involved the delegation of monitoring responsibility entirely on the direct ICT third party providers. Option C was ruled out as it does not align with the DORA framework. Option B was also ruled out for ensuring only partial alignment with DORA as, although simplifying oversight, it could potentially lead to the dilution of the FE's control over the full chain and, consequently, to increased risk exposure along the chain. Option A was thus retained as it ensures end-to-end accountability (independently of the rank of subcontractors) across the entire chain, maintaining compliance with regulatory mandates and full responsibility for addressing any risks effectively. Further, as the requirements of this Option capture subcontractors for the use of ICT services supporting critical or important functions (following an ex-ante risk assessment and the identification of subcontracting of ICT services supporting critical or important function as per Article 3), respective burdens for non-critical services are avoided as they are not subjected to such rigorous oversight.

Finally, the RTS addresses the matter of costs related to the monitoring process of the subcontracting chain, which will differ depending on the business model and complexity of the subcontracting chain. Given that for certain FEs (e.g. credit institutions), sectoral legislation already establishes a quite detailed set of requirements for outsourcing and, on that note, existing procedures are in place, the additional costs were expected to be very low. Further, standardized contractual requirements towards ICT third-party service providers were deemed to strengthen the negotiation position of FEs when negotiating contracts with ICT third-party service providers [14].

3.1.3 Digital Operational Resilience Testing

Taking into account the proportionality principle set out in Article 4 of DORA, Article 24 is dedicated to the aspect of digital operational resilience testing aiming to "assess preparedness for handling ICT-related incidents, of identifying weaknesses, deficiencies and gaps in digital operational resilience, and of promptly implementing corrective measures". FEs other than microenterprises, are to "establish, maintain and review a sound and comprehensive digital operational resilience testing programme as an integral part of the ICT risk-management framework" that includes "a range of assessments, tests, methodologies, practices and tools".

- ***Risk-based testing, requirements for testers, policies, procedures & scope***

The conduction of testing is to follow a risk-based approach considering the evolving landscape of ICT risk, entity specific risks, criticality of information assets and services and any other factor falling into this scope and deemed appropriate and to be performed by independent parties, whether internal or external. Where tests are undertaken by an internal tester, sufficient resources shall be dedicated and avoidance of conflicts of interest shall be ensured throughout the design and execution phases of the test. Article 26(8) states that testers are to be contracted following the requirements outlined in Article 27 and that, in the case FEs use internal testers for the purposes of undertaking TLPT, external testers shall be contracted every three tests. Article 3 of DORA defines TLPT as "a framework that mimics the tactics, techniques and procedures of real- life threat actors perceived as posing a genuine cyber threat, that delivers a controlled, bespoke, intelligence-led (red team) test of the financial entity's critical live production systems".

Credit institutions that are classified as significant in accordance with Article 6(4) of Regulation (EU) No 1024/2013 (said significance based on size, importance for the economy of the Union or any participating Member State and cross-border activities), shall only use external testers the requirements for which are covered in Article 27(1). Regarding contracts with external testers, "FEs shall ensure that they require a sound management of the TLPT results and that any data processing thereof, including any generation, store, aggregation, draft, report, communication or destruction, do not create risks to the FE". The respective requirements for internal testers are covered in Article 27(2) among which, aside from having verified from a competent authority that dedicated resources are sufficient and conflicts of interest avoided during the design and execution phases of the test, the provision of threat intelligence is to be conducted by an external to the entity provider.

Further, procedures and policies are to be established in the direction of prioritizing, classifying and remedying all emerging issues throughout the performance of the tests framed by internal validation methodologies to "ascertain that all identified

weaknesses, deficiencies or gaps are fully addressed". Appropriate tests (vulnerability assessments and scans, open-source analyses, network security assessments, gap analyses, physical security reviews, questionnaires and scanning software solutions, source code reviews where feasible, scenario-based tests, compatibility testing, performance testing, end-to-end testing and penetration testing) are to be conducted "on all ICT systems and applications supporting critical or important functions". These tests along with testing tools are briefly discussed in Article 25.

Article 26 of the DORA Regulation is dedicated to advanced testing of ICT tools, systems and processes based on TLPT. FEs, other than those exempted as of Article 16(1) of the Regulation and other than microenterprises are to carry out at least every 3 years advanced testing by means of TLPT, the frequency of which, based on risk profile and operational circumstances, may be deemed by the competent authority inadequate or that it should be reduced. Identification of "all relevant underlying ICT systems, processes and technologies supporting critical or important functions and ICT services, including those supporting the critical or important functions which have been outsourced or contracted to ICT third-party service providers" and assessment of "which critical or important functions need to be covered by the TLPT" are crucial as they will determine its scope. TLPT is to cover several or all critical functions of the entity and be performed on live production systems supporting them.

- ***Outsourcing and pooled TLPT, RM controls & mutual attestation of conformity to requirements (results, remediation plans and documentation)***

Regarding outsourcing, the participation of the ICT third-party service providers is to be ensured and full responsibility for compliance to be maintained by the entity. In the case the TLPT exercise may potentially impact the quality or security of services provided to customers that are entities outside the scope of the Regulation or the confidentiality of the data related to such services, an agreement in writing between the FE and the provider that the ICT third-party service provider "directly enters into contractual arrangements with an external tester, for the purpose of conducting, under the direction of one designated FE, a pooled TLPT involving several FEs (pooled testing) to which the ICT third-party service provider provides ICT

services" may take place. The pooled testing is to "cover the relevant range of ICT services supporting critical or important functions contracted to the respective ICT third-party service provider by the FEs and be considered TLPT carried out by the FEs participating in the pooled testing". It follows that complexity as imposed by the types of ICT services involved will require calibration of the number of the FEs involved in the process.

FEs, with the cooperation of ICT third-party service providers and other parties involved, including the testers (but excluding the CAs), are to apply effective risk management controls for risk mitigation of "any potential impact on data, damage to assets, and disruption to critical or important functions, services or operations at the financial entity itself, its counterparts or to the financial sector" and, following the end of the testing and agreement upon reports and remediation plans, shall provide to the relevant authority with a summary of findings, remediation plans and documentation supporting the conduction of TLPT in accordance with the requirements, which then Authorities shall confirm with an attestation and this attestation, along with findings and remediation plans, shall be in line notified to the relevant CA by the FE [11]. More on this we will follow in the following subsection in conjunction with the relevant points of the TIBER-EU framework.

3.1.3.1 Joint RTS specifying elements related to threat led penetration tests

Further on what was outlined in the previous subsection, under its Article 26(11), DORA tasks the ESAs to develop an RTS "in accordance with the TIBER-EU framework", in the direction of providing further specifications on "the criteria used for identifying FEs required to perform TLPT, the requirements and standards governing the use of internal testers, the requirements in relation to scope, testing methodology and approach for each phase of the testing, results, closure and remediation stages and the type of supervisory and other relevant cooperation needed for the implementation of TLPT and for the facilitation of mutual recognition". As such, an RTS has been developed in the direction of addressing certain aspects of advanced testing of ICT tools, systems and processes based on TLPT and sector/entity agnostic requirements, in accordance with the TIBER-EU framework, a European framework for threat

intelligence-based ethical red-teaming [15] designed for use at entities that are part of the core financial infrastructure, whether at national or at European level. Its implementation is a multi-stakeholder process that requires the involvement of the following parties to work under a spirit of trust and cooperation: the **entity** responsible for managing the end-to-end test and ensuring that all risk management controls are in place to facilitate a controlled test; the **authorities**, who oversee the test and ensure it is conducted in accordance with the requirements of the TIBER-EU framework; and **external TI and RT providers**, who conduct the test. Overall, it is the respective entity that bears the first and final responsibility for conducting the test.

Intelligence-led red team tests mimic the tactics, techniques and procedures (TTPs) of real-life threat actors and involve the use of a variety of techniques to simulate an attack on an entity's critical functions (CFs) and underlying systems (i.e. its people, processes and technologies), enabling the entity's assessment of its protection, detection and response capabilities. The TIBER-EU framework sets out a mandatory three-phase process for an end-to end test:

- ✓ The *preparation phase* representing the formal launch of the test where the teams responsible for managing the test, the scope of the test and the TI and RT providers who are to carry out the test are established. The determined scope of the test is attested by the entity's board and validated by the CA.

- ✓ The *testing phase* (including threat intelligence and red teaming), during which the TI provider prepares a Targeted Threat Intelligence Report (TTI Report) on the entity, comprising attack scenarios for the test and useful information on the entity which will be used by the RT provider to carry out an intelligence-led red team test of specified critical live production systems, people and processes that underpin the entity's CFs.

  The purpose of the targeted threat intelligence process is to use specific targeted threat intelligence and reconnaissance related to the entity, taking into consideration the real-life actors within the threat landscape, to help develop attack scenarios. The scenarios are based on available evidence of real-world

threat actors, combined with Open-source intelligence (OSINT) data on the entity as well as some knowledge of the CFs that form the scope and target of the red team test. In order for intelligence gathering to be as efficient as possible given the time and resource constraints, and to ensure the intelligence is relevant to the scope and the entity's business, the TI provider should seek from the entity and be provided with: a business and technical overview of each CF-supporting system in scope, the current threat assessment and/or threat register, examples of recent attacks. In cases where the entity has an internal threat intelligence capability or function, the TI provider should liaise with it and gather relevant information. Finally, in cases where the national jurisdiction has produced a Generic Threat Landscape report (GTL), this should also be leveraged by the TI provider as a basis for producing the TTI Report. On July 2020, the ECB issued relevant guidance for the conduction of the TTI Report among a long list of accompanying documents per responsible party withing the scope of the Framework.

In regards to the execution of the test, should obstacles occur, the RT provider should develop alternative ways to reach the test objective or flag. For instance, during the testing phase, the RT provider may be unable to progress to the next stage owing to time constraints or because the entity has been successful in protecting itself. In such scenarios, the RT provider, with agreement from the White Team (WT) (small number of entity's staff members knowing about the conduction of the test) and TTM, may be given a leg-up, where the entity essentially gives the RT provider access to its system, internal network, etc. to continue with the test and focus on the next flag/target. In this event, the leg-up should be duly logged ensuring that maximum benefit is derived by all stakeholders from a time-limited test.

Communication and process trail throughout are essential. The TTM should be updated at least once a week by the RT provider, while the WT should be kept informed of progress on an ongoing basis and at each stage so that it has the opportunity to discuss with the RT provider and TTM what actions can and cannot be taken next. This also provides a chance for escalation procedures to be invoked where necessary. The WT can halt the test at any time if it considers

it necessary to do so. All of the RT provider's actions should be logged for replay with the target entity's security or response capability, the Blue Team (BT), as evidence for the Red Team Test Report, and for future reference.

- ✓ The *closure phase* (including remediation planning and result sharing), where the RT provider is required to prepare a draft Red Team Test Report, which will include details of the approach taken to the testing, along with the findings and observations from the test and advice on areas for improvement in terms of technical controls, policies and procedures, and education and awareness, where necessary for the main stakeholders' awareness. Post discussion of the issues uncovered during the test, the entity, based on the findings, will agree on and finalize a Remediation Plan, in close consultation with the competent authority, the process of the test will be reviewed and discussed, and the key findings from the test will be shared with other relevant stakeholders.

As per what was also mentioned in the previous subsection, given the criticality of the live production systems, people and processes involved in the tests, there are inherent elements of risk involved in the tests and hence a high emphasis is given on establishing robust risk management controls throughout the entire process of the test to ensure it is conducted in a controlled manner.

To ensure a controlled and safe test, the roles and responsibilities of all stakeholders must be clearly established and understood. However, equally critical is its conduction without the prior knowledge of the entity (except for the WT) in order to gain a true picture of the entity's protection, detection and response capabilities. In addition, to ensure that the test is conducted to the highest standards, the external TI and RT providers must meet specified requirements and ideally be accredited and certified by appropriate bodies. Further, it is the responsibility of all stakeholders involved to ensure that they conduct tests within the remit of all laws and regulations, and that appropriate risk management controls (e.g. contracts) are in place to enforce this, as activities performed to fully replicate a real-life attack may involve e.g. gathering data on employees and customers of the entity or use data gathered in the

threat intelligence phase to create email, telephone and in-person ruses as part of a scenario [10].

The TIBER-EU Framework's Annex outlines mandatory and optional requirements during each phase as well as a Responsibility Assignment Matrix within the scope of the TIBER-EU test and a list of accompanying documents per responsible party covering guidelines, plans and reports which provide additional and specific guidance for its implementation.

Having outlined some core aspects of the TIBER-EU Framework, at this point, we need to clarify as per the developed RTS that the DORA mandate does not cover the entirety of the Framework. The main differences, excluding those related to the CAs and their assignment, comprise the following:

- ✓ DORA allowing for, in terms of testing, taking advantage of internal resources at corporate level, under certain conditions aiming at safeguarding the quality of the tests.

- ✓ Under the TIBER-EU, Purple Teaming (collaborative testing activity that involves both the RT (the testers) and the BT (the staff from the attacked FE) is strongly encouraged but not mandatory whereas under DORA, Purple Teaming is mandatory in the closure phase.

The relevant RTS also includes the proportionality principle in terms of the identification of FEs required to perform TLPT that are systemically important and mature from an ICT perspective and is to be understood as a set out of the minimum requirements for conducting TLPTs under DORA.

➢ *Participants and Testing Process*

The TLPT participants as per the RTS are:

- ✓ The TLPT cyber team (or TCT): the staff within the TLPT authority where all operative TLPT-related matters are addressed.

- ✓ The Control Team: TIBER-EU's White Team, namely the team that manages the TLPT from the side of the FE undergoing the exercise. This includes all aspects from procurement of the external providers, the risk assessment the operational management of the day-to-day testing activities, risk management, etc. The Control Team lead should have the necessary mandate within the FE to guide all the aspects of the test, without compromising its secrecy.

- ✓ The Blue Team: Comprising those employees that are defending the FE against simulated or real cyber threat while not knowing that they are tested.

- ✓ The TIP: Mimics a hacker information gathering activity by using multiple reliable sources.

- ✓ The Testers: DORA concept of 'testers' is broader than that of 'Red Team' under the TIBER-EU framework as DORA permits the use of both internal and external testers as long as they adhere compliance with all requirements.

The testing process also comprises, as in the case of TIBER-EU, three phases: preparation, testing and closure, all very close with what was described under the TIBER-EU.

The *preparation phase* is much similar to the respective phase under the TIBER-EU.

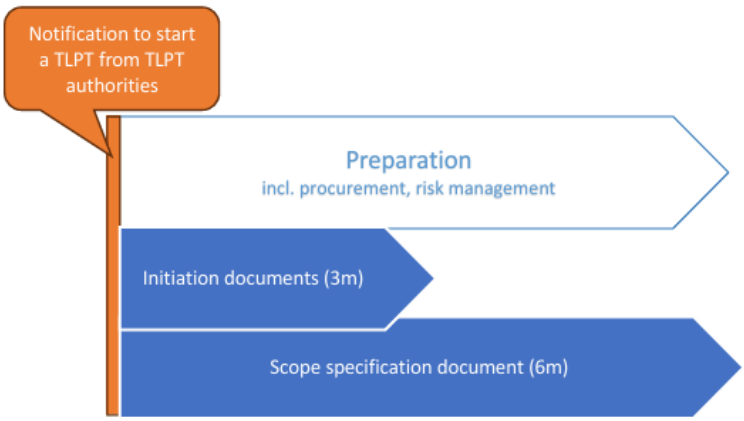

Figure 7 – Preparation phase [15]

The *testing phase* is broken down into a threat intelligence part, namely the production of the scenarios, which are to be tested during the red teaming part of the testing phase, the test plan and the active red team testing. The duration of the latter has to be a minimum of 12 weeks to mimic stealthy threat actors. The exact duration of each test is subjected to fine tuning in agreement with the TLPT authorities and in consideration of the specific characteristics of each TLPT.

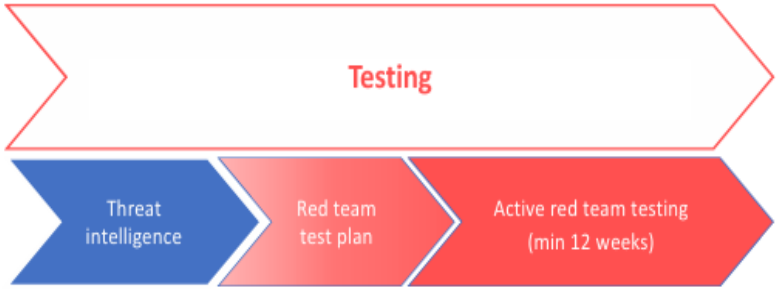

Figure 8 – Testing phase [15]

Finally, the *closure phase* is the phase where "the TLPT is revealed to the BT and the RT and BT reports are drafted. BT and RT come together to replay relevant defensive and offensive actions carried out during the test, a purple teaming exercise will also take place then, and ultimately a test summary report and remediation plan will be prepared by the financial entity and shared with the TLPT authority" [15].

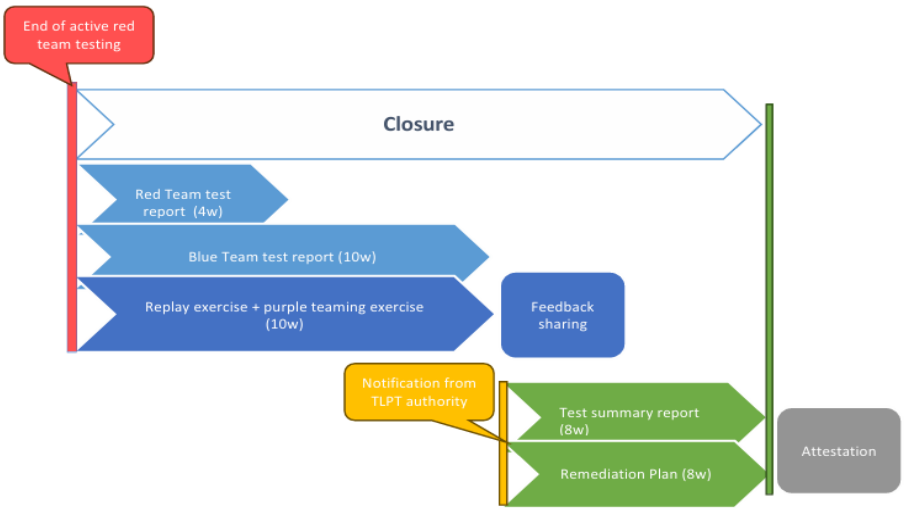

Figure 9 – Closure phase [15]

Additionally, the RTS covers requirements on the use of internal testers and approaches on cooperation, among which the cases of joint and pooled TLPTs and, in Chapter III, requirements regarding test scope, testing methodology and results of TLPT are set out. In the Annexes of the RTS specifications on the content of relevant documents of each phase of the testing process are outlined (project charter, scope specification document, targeted threat intelligence report, red team test plan, red team test report, blue team test report, report summarizing the relevant findings of the TLPT, attestation of the TLPT).

3.1.4 ICT – related incident management, classification, and reporting

Article 18(3) of DORA mandates the ESAs to develop through the Joint Committee and in consultation with the ECB and ENISA, common draft regulatory technical standards further specifying:

i. the classification criteria set out in Article 18(1) of DORA, along with materiality thresholds for the determination of major ICT-related incidents or, as applicable, major operational or security payment-related incidents, that are subject to the reporting obligation laid down in Article 19(1) of DORA.

ii. the criteria to be applied by CAs for assessing what is outlined in i.

iii. the criteria to classify cyber threats as significant, including high materiality thresholds for their determination.

3.1.4.1 RTS on criteria for the classification of ICT-related incidents, materiality thresholds for major incidents and significant cyber threats

The relevant RTS outlines an overview for the classification criteria and thresholds for the determination of major incidents under DORA. Post public consultation, the ESAs opted for treating the classification criterion "Critical Services Affected" as a mandatory condition for classifying an incident as major. All other criteria ("Clients, financial counterparts and transactions", "Data losses", "Reputational Impact", "Duration and Service Downtime", "Geographical Spread" and "Economic Impact") were treated equally. As such, if the mandatory condition holds and either one of the following conditions is met:

- ✓ any malicious unauthorized access to network and information systems as part of the 'Data loss' criterion is identified; Or

- ✓ the materiality thresholds of any other two criteria are triggered

then the incident is classified as **major**. The following Figures depict this classification rule and an overview of criteria details and their thresholds:

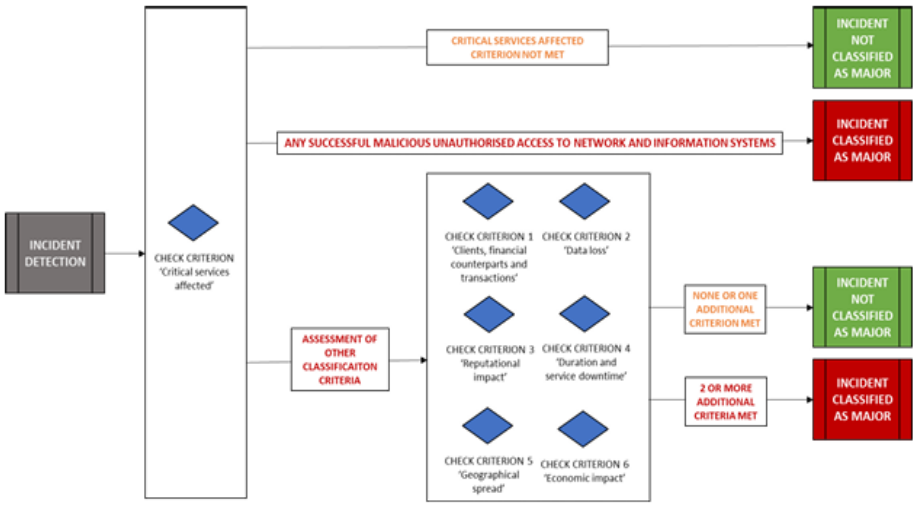

Figure 10 – Classification rule for major ICT-related incidents [16]

Major ICT-related Incident or security or operational payment-related incident
if critical services are affected and (i) any malicious unauthorised access to network and information systems identified, which may result to data losses or (ii) the thresholds of two additional criteria from the below are met

	Mandatory condition	Additional classification criteria					
	Critical services affected	**Clients, financial counterparts and transactions**	**Data losses**	**Reputational Impact**	**Duration and Service Downtime**	**Geographical Spread**	**Economic Impact**
Materiality threshold	**The incident has had any impact on critical services**	Any of: a) **>10% of all clients** using the affected service; b) **>100 000 clients** using the **affected** service; c) **>30% of all financial counterparts** used by the FE; d) **>10%** of the daily average number of **transactions**; e) **>10%** of the daily average amount of **transactions;** f) any **identified impact on clients or financial counterpart** identified by the FE as relevant.	**Any impact on the availability, authenticity, integrity or confidentiality of data**, which has or will have an **adverse impact** on the implementation of the **business objectives** of the FE or on **meeting regulatory requirements**	Any **reputational impact set out in Article 2 a) to d) (overview below)**	a) **incident duration** is **longer than 24 hours**; or b) **service downtime** is **longer than 2 hours for** ICT services that support critical or important functions	**Any impact** of the incident identified in the territories of **at least two Member States**	Costs and losses incurred by the FE **exceed** or are likely to exceed **€100 000** (can be based on estimates where actuals cannot be determined)
Criteria Detail	Assess if the incident : a) affects ICT services or Network and information systems that support **critical or important functions of the FE; or** b) affects financial services that require authorisation, registration or are otherwise supervised by competent authorities; or c) represents a successful, malicious and unauthorised access to the network and information systems of the financial entity.	**1. all affected clients unable to make use of the service** provided by the FE during the incident or that were **adversely impacted by the incident.** These include also third parties explicitly covered by the contractual agreement between the FE and the client as beneficiaries of the affected service. **2.** all affected **financial counterparts with contractual arrangements with the FE.** **3. relevant clients and financial counterparts** whose impact will affect the business objectives of the FE or market efficiency. **4.** all **affected transactions** with monetary amount, with one leg in the EU. (FEs can use **estimates** from comparable reference periods where actuals not available)	1. **availability** of data – data on demand rendered temporarily or permanently inaccessible or unusable; 2. **authenticity** of data – compromised trustworthiness of the source of data; 3. **integrity** of data – data inaccurate or incomplete due to non-authorised modification 4. **confidentiality** of data – data being accessed by or disclosed to unauthorised party or system.	**Reputational impact evidenced by any of the below:** a) **incident reflected in the media**; or b) received **repetitive complaints**; or c) inability **to meet regulatory requirements**; or d) **likely loss of clients or financial counterparts** with a material impact on FE's business. **Level of visibility** of the incident to be taken into account.	**1. Duration** measured from the moment an incident occurs or is detected, until it is resolved. (estimate if not yet known) **2. Service downtime** measured from the moment service fully/ partially unavailable/ delayed to clients, financial counterparts or other internal or external users, until activities are restored to the same level before the incident.	**Assess significant** impact of the incident in **other EU Member States** on: a) **clients or financial counterparts;** b) **branches** of the FE or **other group financial entities;** (c) **Financial market infrastructures or third party providers** that may affect other FEs.	**Types of direct and indirect incurred costs** a) expropriated funds or financial assets liability, including theft; b) replacement or relocation costs; c) staff costs; d) contract non-compliance fees; e) customer redress and compensation costs; f) forgone revenues; g) communication costs; h) advisory costs. (based on available data at time of reporting)
Triggered Yes/No							

Figure 11 – Classification rule for major ICT-related incidents [16]

The relevant Articles of the RTS provide further details on how each criterion is to be assessed. The classification and subsequent assessment against materiality thresholds provides the basis for the reporting framework of the major ICT-related incidents, helping FEs to identify which incidents are major and therefore need to be reported to the CAs, and which are out of scope. FEs shall carry out similar but simplified assessment to identify significant cyber threats.

The baseline scenario (minimum harmonization) is the situation when the current definitions and taxonomy is kept, without further changes or further harmonization. This includes:

- ✓ ENISA taxonomy, NIS 2.
- ✓ PSD2 payment-related major incidents.
- ✓ the text of the Regulation 2022/2554 (entering into force on17 January 2025), but without RTS enhancements specifying the criteria for classification of major ICT-related incidents and cyber threats.

The Directive (EU) 2022/2555 or Network and Information Security (NIS 2) Directive entered into force on 17 January 2023, and constitutes an expansion of NIS Directive. NIS1, and subsequently NIS2, are considered the horizontal framework for cybersecurity in the EU and serve as a baseline standard for a minimum harmonization of all sectoral legislation in this field. Directive (EU) 2015/2366 on Payment Services in the Internal Market (PSD2) required payment service providers (PSPs) to establish a framework to maintain effective incident management procedures, detection and classification of major operational or security incidents included [16]. The main differences between NIS2 and DORA comprise their scope (NIS2 Directive applies to operators of essential services in several sectors whereas DORA is sector specific) and their enforcement mechanisms as Regulations do not require national transposition whereas Directives must be transposed into national law with potential variations in implementation across member states.

3.1.4.2 Final report on the content of the notification and reports for major incidents and significant cyber threats

According to Article 19(1) of DORA FEs “shall report major ICT-related incidents to the relevant competent authority”. Further, Article 19(4) of DORA, in turn, specifies that FEs “may, on voluntary basis, notify significant cyber threats to the relevant competent authorities when they deem the threat to be of relevance to the financial system, service users or clients” [17].

As per Article 19(4) of DORA, FEs, provided the occurrence of an ICT-related incident or cyber threat classified as major or significant shall submit to the relevant CA:

i. an *initial notification*;

ii. an *intermediate report* after the initial notification, as soon as the status of the original incident has changed significantly or the handling of the major ICT-related incident has changed based on new information available, followed, as appropriate, by updated notifications every time a relevant status update is available, as well as upon a specific request of the competent authority;

iii. a *final report*, when the root cause analysis has been completed, regardless of whether mitigation measures have already been implemented, and when the actual impact figures are available to replace estimates [11].

The relevant RTS provides guidance on populating the standard form for reporting the aforementioned notifications, their submission through the use of secure electronic channels set out by their CA, the provision of aggregated information for recurring incidents, which do not individually meet the criteria for a major ICT related incident but do so cumulatively in accordance with Article 8(2) of DORA and the reclassification process in cases where, after further assessment of the incident, the FE reaches the conclusion that the incident previously reported as major at no time fulfilled the classification criteria and thresholds in accordance with Article 18(4) of DORA.

Further the RTS specifies, where FEs intend to outsource the incident reporting obligation in accordance with Article 19(5) of DORA, including where such outsourcing will be part of a general and/or long-term outsourcing arrangement, they shall inform their CA prior to the first notification or reporting under such an arrangement and the latest as soon as the outsourcing arrangement has been concluded. FEs shall provide the details of the third-party that will submit the incident notifications or reports on their behalf and shall also inform their CA in the case where such

outsourcing no longer takes place or has been cancelled. A third-party provider as such may aggregate the information about a major ICT-related incident impacting multiple FEs in one single notification or report, and submit it to the competent authority for all impacted FEs provided the conditions set out in Article 7 of the RTS. Finally, Annex I of the RTS contains reporting templates for major incidents, Annex II glossary and instructions for reporting of major incidents, Annex III contains the templates for notification of significant cyber threats and Annex IV the respective glossary and instructions for this set of templates [17].

3.2 Comparative analysis with existing frameworks

Having established a deeper understanding on the scope of DORA and its requirements, in this section, we will proceed to map them in conjunction with the main clauses of the relevant standards outlined in section 2 of the current essay. The comparison between DORA mandates and the TIBER-EU framework, the main points of which have already been discussed in the previous subsections given its high relevance with the RTS on TLPT, has already been covered.

The following Tables provide a brief summary of the main points of each standard per ISO 27001 clause and a brief mapping of DORA requirements to said clauses based on our judgment from the materials' review in the previous section (Regulation and supplementing RTS). The purpose of this comparison framework was to depict which general clauses the Regulation addresses and at what level.

Based on our judgment, DORA Regulation mandates cover a superset of what is outlined in the reviewed standards in the sense that it strives to be as specific as possible in its guidance given its vast scope across FEs' operations. As such, and in an effort of harmonization across entities, it is evident that the content and structure of the standards that are more generic and sector agnostic in nature has been taken into account in conjunction with previous Regulations underpinning relevant FEs' activities and processes. Considering the increasing challenges faced by the financial sector amidst a highly dynamic cybersecurity landscape, the high level of resilience and its supervision is to be ensured and the DORA Regulation is the embodiment of that and

a showcase of the fact that cyber resilience has emerged as a high priority area in the sector and as a result subjected to proportionate of its importance regulatory scrutiny.

ISO 27001 Clause	ISO 27001 (ISMS)	ISO 22301 (BCMS)
4. Context of the Organization	Places an emphasis in understanding internal and external issues, defining the organization's and ISMS' scope within the context of the organization (overall objectives, operations, legal & regulatory obligations etc.) and its processes.	Places an emphasis on understanding the organizational context in the direction of resilience planning, understanding of the context of BCMS and documenting its relevant processes.
5. Leadership	Focuses on leadership commitment in the direction of setting ISMS objectives, and integrating the ISMS into strategic planning for reaching overall organizational objectives. Further, top management should establish, maintain, and communicate the information security policy and assign roles, responsibilities and authorities within the scope of the ISMS.	Top management's responsibility to drive BCM integration and strategy alignment, to ensure that it reaches its intended outcome and to assign roles in that context.
6. Planning	Risk assessment and treatment based on information security risk.	Focuses on identifying risks and opportunities, setting business continuity objectives, and planning actions to achieve them
7. Support	Emphasizes on resource availability, competency, awareness, and documented information.	Covers the resources, competence, awareness, communication, and documented information necessary to support the BCMS.
8. Operation	Focuses on operational control to implement risk mitigation and ISMS processes.	Details processes for the implementation of business continuity plans and controls, including conducting a Business Impact Analysis (BIA) and Risk Assessment. It emphasizes preparedness and testing of continuity strategies.
9. Performance Evaluation	Focuses on performance measurement, audits, and reviews	Focuses on BCM monitoring, measurement, and evaluation of effectiveness.
10. Improvement	Focuses on continuous ISMS improvement and corrective actions	Focuses on continuous improvement of BCM processes.

Table 4 – ISO 27001 & ISO 22301

ISO 27001 Clause	ISO 31000 (Risk Management)	ISO 27036 (Supplier Security)
4. Context of the Organization	Defines a risk management framework and external context.	Covers supplier-related context and external dependencies.
5. Leadership	Mandates top-level endorsement of a risk management framework (embedding of risk management into organizational processes and tailoring for organizational needs, allocation of resources etc.) and emphasis is given on roles and stakeholder engagement.	No specific Leadership section. Focuses on governance, policies and responsibilities for managing supplier relationships and ensuring alignment with organizational information security objectives.
6. Planning	Provision of a framework for risk identification, analysis, and mitigation (overall details on the systematic application of risk management).	Planning to manage supplier risks, including due diligence. Discussion of strategies for identifying and assessing supplier-related information security risks and provision of guidance on defining security requirements for suppliers based on organizational risk tolerance.
7. Support	Communication and resource allocation to support risk activities.	No specific Support Section.
8. Operation	Implementation of risk management.	Offers guidance on monitoring supplier compliance with agreed security measures and addresses the handling of incidents related to supplier relationships.
9. Performance Evaluation	Covers the evaluation effectiveness of risk controls.	Focuses on continuous review of supplier performance.
10. Improvement	Focus on improving risk frameworks through feedback.	Focuses on improvement of supplier management practices based on learnings.

Table 5 – ISO 31000 & ISO 27036

ISO 27001 Clause	DORA (Digital Operational Resilience)
4. Context of the Organization	Focuses on thorough understanding of operational resilience needs and environment under a multi-stakeholder, multi-faceted prism covering all the areas of the ISO frameworks and encompasses a proportionality principle based on specific criteria that is taken into account horizontally across all areas and requirements (as such, DORA RTS guidelines are technology and sector agnostic emphasizing on area coverage based on proportionality and CA judgement where appropriate). Specific references are given for regulatory obligations, linking them to specific areas of interest (e.g. TLPT) and extensive documentation (Risk management Framework, Business Continuity Plan, ROI for documenting contractual agreements, incident reporting (with additional requirements when it is outsourced plus guidelines in the case of reporting on behalf of multiple FEs, TLPT reporting, estimation of aggregated annual costs and losses caused by major ICT-related incidents etc.).
5. Leadership	Strong top-management responsibility for IT resilience and emphasis on FE's responsibility across all areas of mandates (pertaining to risk management, business continuity and supplier relationships covered by the outlined ISO standards among others) with specifications and reporting guidelines where appropriate. Great emphasis is given on roles and responsibilities within the organization and when third parties are involved and also responsibilities in relevance to communication with CAs.
6. Planning	Enforces risk management aligned with risk tolerance, business continuity and specific regulatory requirements for the methodology of conducting risk assessments among others (triggers for classification of incidents, multi-phased TLPT processes with emphasis on identification, risk scenario planning, response, documentation, communication, logging, reviewing and CA involvement). For several mandates, specific timeframes and periodicity are set.
7. Support	Emphasizes on all the aspects covered by the four outlined ISO standards for resilience initiatives. Specific requirements are set for all stakeholders involved.
8. Operation	Implementation and monitoring of ICT risk mitigation controls with provision of guidelines across several supporting materials with reference to ISO 27002 controls.
9. Performance Evaluation	Special emphasis on audits and reviews for digital resilience compliance covering a superset of areas covered in the four ISO standards in question, both within the entity and across contractual relationships. Strong involvement of CAs.
10. Improvement	Places great emphasis on IT resilience improvement over time on a multi-faceted level.

Table 6 – DORA

4. DORA high-level compliance checklist

4.1 Checklist content

Based on the review of the DORA regulation and the supporting material framing it, we proceeded to develop an Excel checklist assessing high-level readiness in addressing specific areas of focus and significant risks linked to them based on our judgment. The Checklist is organized in a Topic(s) – Task(s) – Risk(s) – Control(s) – Test(s) format where each DORA topic of focus is linked to one or more risks and each risk is linked to its respective control. Each control linked to a specific risk may be associated with multiple tests (as in multiple subtests within the corresponding Test linked to the specific Risk), as risks, controls and tests are inherently comprehensive in nature and address multiple assessment points. For instance, Risks R23 and R24 on ICT Third-Party Risk Management and, more specifically, on Contractual Oversight:

R23. Insufficient controls supporting ICT service provider agreements

is linked to

C23. Establishing strategies and policies that follow the dedicated RTS JC 2024 53 which covers mandatory content of contracts with ICT service providers that "*limit the physical or logical access to information assets and ICT assets to what is required for legitimate and approved functions and activities only, and establish to that end a set of controls that address access rights and ensure a sound administration thereof*" and implementing them including risk assessments and audits

which in turn could be indicatively associated with the following tests:

T23i. Review of a sample of current contracts for the presence of necessary provisions **T23ii.** Review evidence of regular assessment of risks linked to current contracts and risks related to critical dependencies **T23iii.** Review past audits performed

and **R24.** Insufficient oversight of contractual relationships

is linked to

C24. Efficient monitoring and auditing of provided services stemming from contractual relationships based on C9 through maintenance and regular review of ROI templates specified in JC 2023 85 at the highest level of granularity possible. FEs shall report at least yearly to the CAs on the number of new arrangements on the use of ICT services, the categories of ICT third-party service providers, the type of contractual arrangements and the ICT services and functions which are being provided and have, upon request, the full ROI available along with any information deemed necessary under the prism of effective supervision

which in turn could be indicatively associated with the following test:

T24. Review ROI reporting vs the review sample defined in T23i and that it is regularly updated

It should be noted that the number of tests assigned to controls were set arbitrarily in order for the scoring calculation described in the following subsection to be performed. We therefore identified 25 comprehensive risks R1-R25 linked with 25 controls C1-C25 pertaining to 8 broad topics following the structure of DORA chapters:

1. Scope & Proportionality (GENERAL PROVISIONS): Covering risks associated with DORA compliance not being proportionate to the scope of the entity.

2. ICT Risk Management Framework - Comprehensive Documentation, Internal Governance, commitment, processes, communication, monitoring, allocation of resources (ICT RISK MANAGEMENT): Covering broad areas of risks from Governance and Operational in nature to risks related to processes and their documentation, DORA

documentation management and budgeting issues that might hinder addressing set objectives.

3. A. ICT Systems, protocols & tools B. Protection & Prevention C. Detection, Response & Recovery/ D. Asset Management & Identification / Vulnerability Management E. Backup policies & recovery methods (ICT RISK MANAGEMENT): Covering broad areas of risks pertaining to ICT systems, protocols & tools, preventing measures and mechanisms for detecting anomalous activities and ICT-related incidents, response strategies and procedures, asset and vulnerability management and backup and recovery methods.

4. Threat Intelligence & Information Sharing Arrangements (INFORMATION SHARING ARRANGEMENTS): Covering risks relevant to risk mitigation strategies based on informed insight on the cyber threat landscape and risks stemming from information sharing arrangements.

5. Incident Management & Reporting (INCIDENT MANAGEMENT): Covering risks relevant to the areas of detection and management, classification of major incidents, notification and reporting procedures and estimation of aggregated annual costs and losses caused by major ICT related incidents.

6. DORT programme, Vulnerability Assessment, TLPT (DIGITAL OPERATIONAL RESILIENCE TESTING): Covering risks relevant to the level of resilience to ICT-related disruptions through systematic and effective testing of digital infrastructures.

7. Contractual Oversight (ICT THIRD-PARTY RISK MANAGEMENT): Covering risks relevant to the level control over operational risks, information security and business continuity across the entirety of the cycle of contractual arrangements.

8. Service Provider Assessment (ICT THIRD-PARTY RISK MANAGEMENT): Covering risks relevant to monitoring of ICT dependencies and assessment of the level of implementation of provisions covered in contractual arrangements and of compliance with regulatory requirements.

It should also be noted that Risks, Controls and Tests were selected to cover most areas highlighted in the RTS relevant to the ICT risk management framework, namely: ICT risk management, ICT asset management, Encryption & Cryptographic Controls, Development & Maintenance of ICT systems, ICT operations, Identity Management & Access Control / Human resources, ICT-related incident Management, ICT business continuity, Capacity & Performance Management, Vulnerability & Patch management, Data & System Security, Logging, ICT change management, Network Security Management, Security information in transit while limiting overlaps across Tests.

For each of the topics assessed, we set out indicative references to DORA chapters and relevant RTS where appropriate. Further, we arbitrarily set 59 tests in total to support the respective controls and, for each of the tests, the response output is a compliance level from 0-100%, namely the level of compliance in terms of the outlined control in the Checklist that the relevant tests indicated. The Checklist ultimately depicts a risk score per risk and the response compliance level for each topic (sum of average compliance level per risk which in turn is derived by averaging the compliance level of tests linked to each specific risk) and an Overall Inherent Risk Score which is a high-level assessment of DORA readiness, the calculation of which we will proceed to analyze in the following section. Test periodicity is also depicted in order to keep track of which tests are performed annually, semi-annually or during in-between intervals that have to be specified. Each Overall Risk Score, either Inherent or Residual is interpreted based on the following Scale:

RS	Risk Level	Summary
1	Very Low	Tests indicated an overall positive outlook
2	Low	Tests indicated corrective actions are required within a reasonable timeframe
3	Medium	Tests indicated corrective actions are required within a relatively short timeframe
4	High	Tests indicated immediate corrective actions are required
5	Critical	Critical issues identified

As we will proceed to describe in the following section, the Checklist, should the maturity of the entity be at a level that the entity can also assess whether the applied controls are efficient and to what extent in terms of potential risk mitigation, also covers a simplified risk assessment and planning process.

4.2 Overall Inherent Risk Score calculation

In this section, we will proceed to analyze a simplified approach via which, based on the performance outcome on each of the tests (% Compliance Level), an Overall Risk Score is derived indicative of a high-level outlook of the entity on the assessed topics. The calculations were based on test level and ultimately led to results on risk level. All DORA Chapters leading to the topics assessed were assumed to be of equal importance. It was also assumed that the risk score for each risk comprised of the Probability of the risk materializing (within x years depending on what is relevant per area assessed), its potential Total Impact and the level of Non-Compliance (100% - % Compliance Level) on risk level (that was derived on the outset by averaging test non-compliance scores for risks associated with multiple tests). Impact was assigned values from 1 to 5 and Probability and Non-Compliance Level were also scaled as such with a band approach for Probability and a simple linear contribution of % points for Non-Compliance Level:

	Probability		
Scale	Prob.(%)	Prob. Descr (alternatively)	NC(%)
1	<=5	Over 3 years	20
2	5<P<=10	Every 2-3 years	40
3	10<P<=35	Annually	60
4	35<P<=50	Monthly	80
5	>50	Weekly	100

It should be noted that for the development of the Checklist we used the first definition for probability scaling given that some risks may not have been monitored to

that level of detail prior to the more stringent regulatory landscape in order for the second approach to be applicable across all risk areas.

According to the Basel III framework, operational risk comprises that of loss resulting from inadequate or failed internal processes, people and systems or from external events, including legal risk, but excluding strategic and reputational risk. As such and in order to limit as well as account for interdependencies, we decided to make the following assumptions. We defined Total Impact as a result of Financial, Operational and Reputational Impact comprising the average of the three impacts. Operational and Reputational Impact were simply assigned a value from 1-5 depending on their significance per test. Financial Impact is assumed to derive taking into consideration the Explicit Financial Impact component that occurs in the case of specific tests with explicit and quantifiable financial impact and is assigned a value of 1-5 based on a taxonomy taking into account the severity of realized occurrences of such events (in financial volume) and the Implicit Financial Impact which is dependent on Operational and Reputational Impact and derived from the formula: *¾* Reputational Impact + ¼* Operational Impact*, assuming that implicit Financial Impact always exists and mostly stems from reputational issues and a part of it from operational issues that call for corrective actions. In order to be more conservative, Total Financial Impact was set to result from the formula: *max((Explicit Financial Impact + Implicit Financial Impact)/2, Implicit Financial Impact)*.

For the purpose of the calculations, we proceeded to assign weights to the three aforementioned risk factors. Given that Compliance Level can drive Probability and the former is quantified based on tests performed whereas the latter is more arbitrary plus the fact that Compliance should be rewarded as it can potentially limit both Probability and Impact, it was chosen for Non-Compliance to be more heavily weighted relative to Probability. Impact was chosen to be the driving factor of the assessment, as criticality is a core concept of DORA. Therefore, Impact was assigned a weight of 0.6, Non-Compliance Level a weight of 0.25 and Probability a weight of 0.15 (weights summing to 1). It was also assumed that Compliance Level across tests was independent from that of other tests which, in essence, is not realistic across all cases. For example, a subtest of T17 is linked to T15. However, as priorly mentioned, an effort was made to

keep interdependencies for indicative tests outlined in the checklist limited hence their comprehensive nature. For the purpose of the analysis, we chose to randomly assign Compliance Levels per test. We also assigned Probability and Explicit Financial, Reputational and Operational Impacts arbitrarily yet based on the fact that most of the risks are high impact and that the entity has a level of maturity indicative of relatively moderate to high probabilities of occurrence of risks (max 50%). The formula used to derive the initial unweighted Risk Score for each Risk was the following, capturing relative importance between the risk factors involved instead of implying a directly proportional relationship between Probability and Impact:

$$RS_{unweighted} = \left(\sum_{k=0}^{R} (0.6 * \text{Total Impact} + 0.25 * (100\% - (\sum_{k=0}^{t} \%\ \textit{Compliance Level per Test per Risk})\text{Scaled} / t) + 0.15 * \text{ProbabilityScaled}) / R\right),$$

where t is the total number of tests per risk and R is the total number of risks

However, based on the fact that some topics are linked to multiple risks and those risks are linked to multiple subtests while others are not, we proceeded to apply risk score-based test weights as well, based on: the unweighted RS we calculated, the total number of tests performed for checklist purposes and the assumption that each test risk has an equal contribution among tests within the same risk. Therefore, the weight for each subtest was derived as such:

$$\text{Test weight} = ((1-RS_{unweighted}/5)/T)/t_{sub},$$

where t_{sub} is the total number of subtests per risk and T the total number of tests performed during the assessment.

The sum of each T weight of each of the subtests associated with a risk comprised the risk's T weight. This weight was applied to the % Compliance Level per risk and a weighted % Compliance Level capped at 100% was derived resulting in a weighted % Non-Compliance level which was scaled and used for the derivation of the $RS_{weighted}$ per risk, and in turn led to an Overall Risk Score that was slightly upwards revised compared to the unweighted Overall Risk Score. The weighted Non-Compliance level affected as a result only critical Impact risks.

4.3 Residual Risk Score calculation & Planning

Additionally, to the aforementioned process, we proceeded to also introduce the aspect of Control(s) strength. Controls can be assessed in terms of their efficacy in addressing the outlined risk areas and rated as such:

Control Strength	Description
1	High - Needs Minor Improvement
2	Moderate - Needs Substantial Improvement but Mitigates Risk
3	Low - Needs Major Improvent / Risk Retention

When this applies to the Inherent Risk Score as described in the previous section, the risk level is modified as depicted in the following Residual Risk Matrix:

Residual Risk Matrix (if Open Regulatory Finding(s) not exists)				Residual Risk Open Regulatory Finding(s) exists Controls are rendered ineffective
Inherent Risk Level	Control Strength			
	1	2	3	
5	3	4	5	5
4	2	3	4	4
3	2	2	3	3
2	1	1	2	2
1	1	1	1	1

Given how effective the Controls in place are from 1 (High Control Strength) to 3 (Low Control Strength), the Inherent Risk Score is modified following the logic that a High control strength efficiently mitigates risk, Moderate Control Strength slightly mitigates risk and a Low Control Strength results in risk retention as it is practically ineffective.

Further on this, an additional factor taken into consideration was whether there are open regulatory findings outstanding per Risk. In that case, Control Strength is not recognized and the Risk Score remains at Inherent Risk Level. As such, we end up with an Overall Residual Risk Score. In the case that the entity has not reached a level of maturity where outstanding Controls efficacy can be assessed, the current tool operates only as a Checklist and the risk score Remains at Inherent Risk Score level.

Following this process, the Checklist results in a Planning process that ranks the Risk IDs from highest to lowest risk and provides a descriptive overview of the distribution of Risk IDs across the aforementioned 5 Risk Bands. Provided a detailed

Audit Universe that links Risk IDs to functional areas, processes and subprocesses the process could ultimately lead to an Audit Plan.

5. Conclusions

Considering the objectives addressed by the current essay, namely the review of the DORA regulation, the dedicated RTS pertaining to DORA Pillars developed by CAs and the relevant ISO standards in conjunction to identify risks to digital operational resilience, it is evident that significant strides have been made in the direction of a harmonized digital resilience across the EU financial sector, in alignment with global best practices and existing guidelines and regulations. While DORA provides a sector-specific focus, it can leverage methodologies and global applicability and this synergy is encouraged throughout its documentation. Further, significant effort has been made towards the development of templates and guidelines indicative of the level of control, understanding and commitment that entities within its scope are required to establish towards their digital operational resilience outlook, including contractual oversight and assessment of risks stemming from complex supply chains due to third-party dependencies and, of course, the level of commitment towards regular monitoring, leveraging reporting, test results and lessons learned for achieving continuous improvement and robust resilience.

Further, the simple exercise of the checklist development complements the aforementioned review of the efforts made, as many identified risks based on our judgement, are addressed via the DORA material, where specific guidelines of various levels of detail are provided under the prism of supporting monitoring and auditing efficiency both on the part of the entities assessed and the CAs overseeing regulatory compliance.

The described methodology was of course over simplified with assumptions that can be modified to account for dependencies and other aspects appropriate to the purpose and nature of the checklist and its tests and the scope of such an endeavor. What we outlined simply constituted an attempt to develop a comprehensive DORA Checklist, linking it to some high-level conclusions regarding the entity's outlook relevant to risks to digital operational resilience leaving plenty of room for more granular modifications. However, despite its simplicity, it could provide a basis for more granular analyses with tests of level of detail proportionate to specific areas or specific critical systems with a, for instance, weighting methodology addressing test

significance per component and taking into account interdependencies in risks that entail both documentation and implementation related issues that are interconnected and should be evaluated in conjunction. The checklist tool could also include KPIs, quantifying for instance, y-o-y compliance change or risk score change. For qualitative tests such as the existence of documented policies or the conduction of regular audits that are more static in nature compared to those associated with testing, monitoring of systems and reporting, there could be regular reviews of whether previous findings were addressed or whether the ICT risk management framework was appropriately updated post significant findings calling for remediation actions. Additionally, Residual Risk could take into account more factors that make sense for the specific entity such as, for instance, whether there are new developments pending within the risk area that call for the prioritization of processes involved in terms of auditing.

What is overall evident following the points addressed for the purposes of the current essay is that, amongst an increasingly evolving digital landscape and emerging challenges, DORA's implementation offers an opportunity to refine regulatory mechanisms and foster collaboration amongst stakeholders in the direction of ultimately enhancing resilience and, as its developments unfold, will surely provide valuable insights.

Appendix

Abbreviation	Definition
DORA	Digital Operational Resilience Act
ESAs	European Supervisory Authorities
EBA	European Banking Authority
EIOPSA	European Insurance and Occupational Pensions Authority
ESMA	European Security and Markets Authority
ENISA	European Union Agency on Cybersecurity
TIBER	Threat Intelligence-Based Ethical Red Teaming
ECB	European Central Bank
P2P	Peer-to-Peer
De-Fi	Decentralized Finance
AML	Anti-Money Laundering
TSPs	Technical Service Providers
CEBS	Committee of European Banking Supervisors
ICAAP	Internal Capital Adequacy Assessment Process
BCM	Business Continuity Management
RTS	Regulatory Technical Standards
SSM	Single Supervisory Mechanism
OSIs	On-site Inspections
SREP	Supervisory Review and Evaluation Process
3LOD	Three Lines Of Defense
NIS	Network Information Security
CER	Critical Entity Resilience
ROI	Register Of Information
TTPs	Trusted Third Parties
TLPT	Threat-Led Penetration Test
JC	Joint Committee
CDRs	Commission Delegated Regulations
NIST	National Institute of Standards and Technology
FSB CIRR	Financial Stability Board Cyber Incident Response and Recovery
CPMI-IOSCO	Committee on Payments and Market Infrastructures - International Organization of Securities Commissions
BCBS	Basel Committee on Banking Supervision
FEs	Financial Entities
ISMS	Information Security Management System
CFs	Critical Functions
CCPs	Central Counterparties
CSDs	Central Securities Depositories
EMIR	European Market Infrastructure
CSDR	Central Securities Depositories Regulation
BIA	Business Impact Assessment
CA	Competent Authority
LEI	Legal Entity Identifier
TTI	Targeted Threat Intelligence
RT	Red Team
WT	White Team
BT	Blue Team
GTL	Generic Threat Landscape
PSD2	Payment Services in the Internal Market
PSPs	Payment Service Providers

References

[1] E. Commission, *COMMISSION DELEGATED REGULATION (EU) 2024/1774,* Brussels: Official Journal of the European Union, 2024.

[2] I. A. Tsindeliani, M. M. Proshunin, T. D. Sadovskaya, Z. G. Popkova, M. A. Davydova and O. A. Babayan, "Digital transformation of the banking system in the context of sustainable development," *Journal of Money Laundering Control,* vol. 25, no. 1, pp. 165-180, 2022.

[3] H. S. Scott, *The E.U.'s Digital Operational Resilience Act: Cloud Services & Financial Companies,* Program on International Financial Systems (PIFS), 2021.

[4] E. B. Authority, *Final report on EBA Guidelines on outsourcing arrangements,* European Banking Authority, 2019.

[5] E. B. Authority, *Guidelines on ICT Risk Assessment under the Supervisory Review and Evaluation process (SREP),* European Banking Authority, 2017.

[6] E. C. Bank, *ECB Banking Supervision: SSM supervisory priorities for 2024-2026,* Frankfurt: European Central Bank - Banking Supervision, 2023.

[7] E. C. Bank, "www.bankingsupervision.europa.eu," 26 July 2024. [Online]. Available: https://www.bankingsupervision.europa.eu/press/pr/date/2024/html/ssm.pr240726~06d5776a02.en.html.

[8] E. I. a. O. P. Authority, *DIGITAL OPERATIONAL RESILIENCE ACT (DORA) - REPORTING OF REGISTER OF INFORMATION,OF MAJOR ICT-RELATED INCIDENTS AND SIGNIFICANT CYBER THREATS - UPDATE,* European Insurance and Occupational Pensions Authority.

[9] J. C. o. E. B. Authorities, *Draft RTS to further harmonise ICT risk management tools, methods, processes and policies as mandated under Articles 15 and 16(3) of Regulation (EU) 2022/2554,* European Banking Authority, 2024.

[10] E. C. Bank, *TIBER-EU FRAMEWORK - How to implement the European framework for Threat Intelligence-based Ethical Red Teaming,* Frankfurt am Main: European Central Bank, 2018.

[11] E. P. a. Council, *Regulation (EU) 2022/2554 of 14 December 2022 on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No*

600/2014, (EU) No 909/2014 and (EU) 2016/1011, Strasbourg: Official Journal of the European Union, 2022.

[12] J. C. o. E. B. Authorities, *Joint Guidelines on the estimation of aggregated annual costs and losses caused by major ICT-related incidents under Regulation (EU) 2022/2554,* European Banking Authority, 2024.

[13] J. C. o. t. E. S. Authorities, *JC 2023 85 - Final Report On Draft Implementing Technical Standards on the standard templates for the purposes of the register of information in relation to all contractual arrangements provided by ICT third-party service providers under (EU) 2022/2554,* European Banking Authority, 2023.

[14] J. C. o. t. E. S. Authorities, *Final report on Draft Regulatory Technical Standards to specify the elements which a financial entity needs to determine and assess when subcontracting ICT services supporting critical or important functions as mandated by Article 30(5) of DORA*, European Banking Authority, 2024.

[15] J. C. o. E. B. Authorities, *Draft Regulatory Technical Standards specifying elements related to threat led penetration tests under Article 26(11) of Regulation (EU) 2022/2554,* European Banking Authority, 2024.

[16] J. C. o. E. B. Authorities, *Final Report on Draft RTS specifying the criteria for the classification of ICT related incidents, materiality thresholds for major incidents and significant cyber threats under DORA,* European Banking Authority, 2024.

[17] J. C. o. E. Banking, *Final Report on Draft RTS on the content of the notification and reports for major incidents and significant cyber threats and determining the time limits for reporting major incidents,* European Banking Authority, 2024.