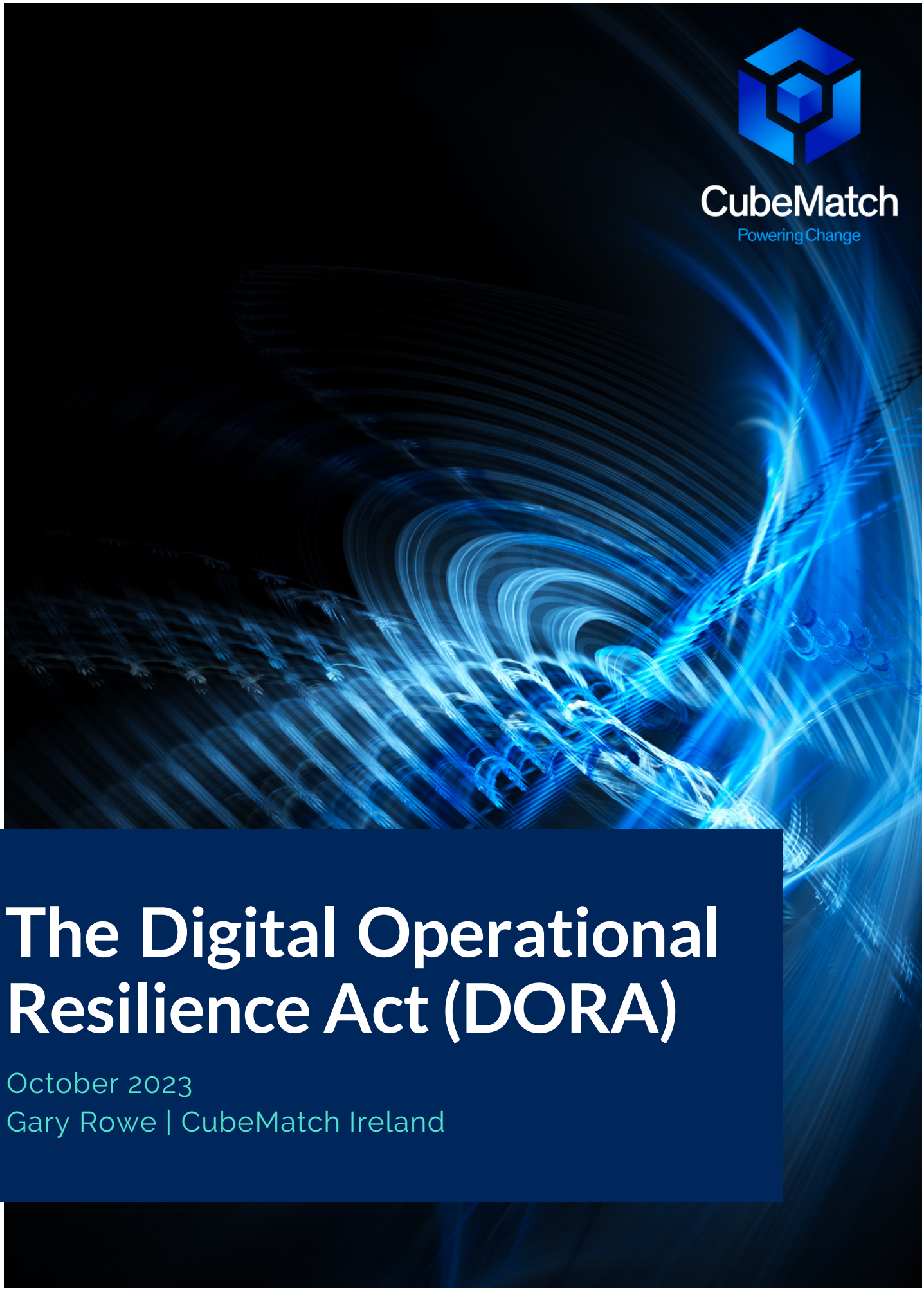

The Digital Operational Resilience Act (DORA)

October 2023

Gary Rowe | CubeMatch Ireland

TABLE OF CONTENTS

INTRODUCTION

In the face of a changing threat landscape due to the interconnected ICT (Information and Communication Technology) services used across the financial markets in the EU, the Digital Operational Resilience Act will be coming into force at the beginning of 2025 to provide more harmonised regulations. It will require Risk Management, Testing, and Third-party Resilience Management frameworks to be adopted, in a risk-based and proportionate manner, within which the financial entities can operate. It will sit on top of existing Cyber Security and Resilience regulations, and provide a means for each nation-state to cooperate and standardise their requirements on their financial entities for resilience; and in the reporting required from them in the case of any incidents that threaten their continuity of providing their business services and functions. Where a company provides a service to others whose resilience is deemed critical to the EU as a whole, the DORA Risk Management framework must be adopted by them also.

Furthermore, the reporting of incidents that affect critical business functions in a financial entity will become a more level playing field across the different nations in the EU, with harmonised requirements being set across the European Union.

Together, these regulations and frameworks will mean that, by institutions taking control and responsibility for their resilience at a senior management level and proving it through the implementation of detailed testing, cyber-attacks and 3rd-party ICT service outages across the EU will be contained and resolved in the most efficient and effective ways, and with significantly less risk of contagion across the market and national boundaries.

WHY IS IT IMPORTANT?

Many of the complex systems used every day in the financial sector incorporate Information and Communication Technology (ICT) to increase their efficiency and accuracy. However, this increasing dependency – especially on remote ICT Service Providers - also introduces additional risks and vulnerabilities which can make financial entities more exposed, both directly and indirectly, to cyber-attacks or incidents.

Additionally, these ICT services are often offered across borders and if not managed properly, their associated ICT risk could lead to disruptions of financial services that would have far-reaching effects on other companies, sectors, or even the rest of the economy.[1] It is the growing risk of such cross-border and cross-sectoral disruptions to the financial markets in the EU which highlights the importance of a harmonised and proportionate approach to operational resilience across all of the EU, which has led to the creation of the Digital Operational Resilience Act **(DORA).**

Notably, as systems become more and more interdependent on remote service providers, resilience legislation is also being brought forward in the US, UK and Singapore etc., as these threats to the economy emerge and grow in all geographic areas.

1. *Digital Operational Resilience Act (DORA): public consultation on the first batch of policy products, June 2023.*

WHAT IS IT?

The DORA (Cyber Risk Gmbh, 2023) will bring front and centre the cyber risks and potential for ICT-related incidents that are being faced by – and can affect - all financial entities across the EU, enhance cooperation among the competent authorities in the EU's finance sectors by bringing together authorities from different sectors and jurisdictions and harmonising their ICT and cyber risk management and reporting.

It introduces a framework to oversee the systemic and concentration risks posed by the financial sector's reliance on ICT 3rd-party service providers. Alongside this, there will be an EU-level oversight framework for the critical ICT service providers to ensure that the ICT risks posed to financial entities are appropriately managed proportionately to their size and the importance of the services provided.

It is a cross-sectoral regulation, applying to more than 20 different types of financial entities, with more than 50 authorities – from national authorities to the European Central Bank and ENISA - taking part in the development of the policy products mandated by the DORA for each financial entity. Extending this harmonisation, DORA is *lex specialis*[2] to (and thereby take precedence over) both the NIS Directive 2 and Article 11 and Chapters III, IV and VI of the CER Directive.

Lastly, it will bring in standardised reporting of incidents that affect important and critical business functions & services (IBS/IBF) of financial entities and their third-party ICT service providers that might be shared nationally or even EU-wide, according to its inherent risk and potential impact to other financial entities, or even economies.

2. *An act that includes specific regulations that override earlier general regulations on the same topic.*

HOW IT MAY AFFECT YOU

The responsibility and accountability for the resilience of each financial entity and 3rd-party ICT service provider will rest with the senior management of each organisation. They must set out the policies required for each of the areas covered by DORA, and ensure that all of the required procedures, processes and resources are documented, implemented, maintained, and proven effective through detailed testing, up to and including threat-led penetration testing of the larger organisations in each market. The results of this testing must be available to the national bodies, who will ensure that – commensurate with their size and what they provide – the financial entities and 3rd-party ICT service providers comply with all of the facets of DORA.

If you are a financial entity, you need to create the policies and procedures required to lay out your resilience plans and strategies across the facets of DORA:

- ICT Risk Management,
- The Classification of ICT-related Incidents,
- ICT Incident Management and Reporting,
- Testing of the Operational Resilience of your ICT systems, and
- The Management of ICT Third Party Risks.

You will need the trained resources with the required tools available to implement and test them, and to have the required framework(s) fully in place across your organisation to coordinate all of the separate streams and silos that could be involved in an incident, from discovery through to resolution. Along with this, you should prepare all potential communications to your customers, your peers, the regulator, and national and possibly international bodies, in such a way as to minimise the risk of ensuing reputational damage and litigation arising from their wording.

WHAT TO DO NOW

To have all of the parts in place to work together and provide resilience to your business operations, you must first have a detailed register of what business services, functions and/or data you provide, and the potential impact on your business – and potentially the economy – of the interruption of any of those services.

This must also include what each service is dependent on, especially all 3rd-party ones such as

- Data Centres,
- Data Analytics services,
- Software & hardware providers,
- Cloud services, storage & backups,
- Communication channels both inwards and outwards (e.g.: email, phone, websites etc.),
- Remote servers,
- Remote access,
- Payment Services & payment-related solutions, etc.

There can be hidden concentration risks, where although you may use separate 3rd-party ICT service suppliers for each service, some or all of them may in turn be dependent on one service provider. All of these are potential risks, and you must be sure that you fully understand the full ramifications of the loss of any one or group of such suppliers to your business, whether that loss is for a matter of minutes, hours, or days … and identify the thresholds for each that demarcate the differences between a trivial incident up to a more serious threat to your ability to continue your business.

You should have a communications plan in place for each identified potential ICT Service incident so that if one affects any of your critical business functions or services, management will be quickly and accurately informed of the full extent of the problem and what their available options are, so that they can make the optimum business decisions in a fast and effective way. Such incidents rarely confine themselves to just one silo of the operation of the business, and a coordinated approach is required across the different streams affected, both technical and business-related.

For your ICT Service providers, your contracts must include precise quantitative and qualitative performance targets *[including during the period before termination of service]*, must ensure that they will take part in your Business Continuity plans and testing [up to and including Threat-Led Penetration Tests, where required], and that they will supply assistance in the case of an incident, at no extra cost.[3] Should any 3rd-party ICT supplier fail to meet your service level agreements or security requirements, you need to be able to speedily terminate their contract and switch over to another supplier without impacting your business. All of your contracts with 3rd-party ICT service providers need to be examined and reworked where necessary before DORA comes into operation.

You must set up a testing framework for the ongoing testing and proving of your operational resilience; DORA not only requires a comprehensive framework to manage your ICT Risks but also one to ensure that your policies, strategies and defences are effective at protecting your business operations in the face of disruptions to the services you rely on (as identified in your register). This testing can, for certain organisations, cover Threat-Led Penetration Tests *(with your 3rd-party ICT service providers also involved).*

Senior management must set out their policies on each of the areas of DORA, and the required procedures, processes and strategies be created, signed off on and then tested, taking on board that the testing may require addition resources - and their associated additional costs and tools. The test results should inform back onto the processes and any improvements noted and implemented. The proof of and results from all such testing must be documented and available to be audited.

Should any loss of service occur, if the incident passes the specified threshold for being reported on then you must inform the parties required by the DORA.[4] Part of this reporting may be to customers and/or peers, so the wording must be carefully considered to minimise the risk of reputational damage and/or litigation arising from it; it is highly recommended to have these wordings prepared in advance with inputs from Legal and Compliance expertise, with clear documented instructions on their use *(including when, and to whom)* for the comms team who would be involved for the incident.

3. Or at a pre-agreed cost (determined 'ex ante' - not at a cost only calculated during or after the incident).
4. Standard Forms, Templates, and Procedures will be produced by the ESAs during 2024.

IN DETAIL - WHAT BECOMES LAW ON JANUARY 17TH, 2025

The Digital Operation Resilience Act (DORA) (EUR-Lex, 2022) entered into force on 16 January 2023, and will apply from 17th January 2025, bringing harmonisation of the following areas relating to operational resilience for the financial sector:

- ICT risk management,
- ICT incident management and reporting,
- Testing of the operational resilience of ICT systems, and
- The management of ICT third party risks.

The Policies required of Financial Entities and Third-Party ICT Service Providers:

The DORA, in bringing together and harmonising all aspects of controlling the risks involved in using Third Party Providers (TPPs) of ICT Services, addresses multiple areas and the European Supervisory Authorities (ESAs) will be producing a set of delegated Acts[5] that back it up, to be finalised by July 2024 (Joint Commission of the European Supervisory Authorities, 2023). These will complement & expand on the articles already in the DORA, covering the following areas:

The ICT Risk Management Framework - Art. 16(3)

The proposed Risk Management framework (ESAs, 2023) sets out requirements for all financial entities with respect to their:

(i)ICT security policies, procedures, protocols and tools, including requirements on:

a. Governance,
b. ICT risk management,
c. ICT asset management, encryption and cryptography,
d. ICT operations security, and network security,
e. ICT project and change management, and physical security, and
f. ICT and information security awareness and training.

(ii)Human resources policy and access control,
(iii)ICT-related incident detection and response,
(iv)ICT business continuity management,
(v)Reporting on the ICT risk management framework review, and
(vi)Proportionality.

5. These draft technical standards have been developed in accordance with Articles 15, 16(3), 18(3), 28(9) and 28(10) of DORA (Regulation (EU) 2022/2554). The ESAs expect to submit these draft technical standards to the European Commission by 17 January 2024.

There will also be a simplified ICT risk management framework that applies to only five categories of smaller/less interconnected financial entities[6] and complements the requirements set out in Article 16 of DORA in the following areas:

- ICT risk management framework,
- Further elements of systems, protocols, and tools to minimise the impact of ICT risk,
- ICT business continuity management and
- Report on the ICT risk management framework review.

The Classification of ICT-related incidents - Art. 18(3)

The proposed Classifications (ESAs, 2023) will supply harmonised requirements for financial entities on:

(i)the classification of ICT-related incidents by financial entities,

(ii)the classification approach and materiality thresholds for determining major ICT-related incidents to be reported from financial entities to competent authorities,

(iii)the criteria and the thresholds to be applied when classifying significant cyber threats, and

(iv)the criteria to be applied by competent authorities (CAs) for the purpose of assessing the relevance of major ICT-related incidents to relevant competent authorities in host Member States and the details of the information to be shared with them.

The templates for the Register of Information - Art.28(9)

The draft ITS (ESAs, 2023) establishes harmonised templates for the registers of information to be maintained by financial entities covering all contractual arrangements on the use of ICT services provided by ICT third-party service providers at individual, consolidated, and sub-consolidated level (Article 28(3)).

The templates have been designed taking into account the threefold purpose of the register of information:

(i)the register of information is part of the ICT risk management framework of financial entities (Article 28(1)),

6.Smaller less interconnected financial entities are: (i) small and non-interconnected investment firms, (ii) payment institutions exempted pursuant to Directive (EU) 2015/2366; (iii) institutions exempted pursuant to Directive 2013/36/EU in respect of which Member States have decided not to apply the option referred to in Article 2(4) of this Regulation; (iv) electronic money institutions exempted pursuant to Directive 2009/110/EC; and (v) small institutions for occupational retirement provision

(ii)the register of information enables the effective supervision of financial entities' (Article 28(3)), including:

(iii)the designation of third-party service providers as critical at the level of the EU by the ESAs in the context of the oversight framework (Chapter V, Section II).

To simplify setting out the registers by the financial entities, the draft ITS contains two different sets of templates for the registers at an individual entity level (ESMA, 2023) and the sub-consolidated and consolidated level (ESMA, 2023).

Critical or Important ICT services performed by ICT third-party providers – Art. 28(10)

This will set out the requirements (ESAs, 2023) for all phases that should be undertaken by financial entities regarding the life cycle of ICT third-party arrangements management. In particular, the draft RTS specify the content of the policy regarding the use of ICT services supporting critical or important functions by dealing with the following aspects:

(i)the pre-contractual phase (i.e.: planning of contractual arrangements including the risk assessment, the due diligence and the approval process of new or material changes to those third-party contractual arrangements),

(ii)the implementation, monitoring and management of contractual arrangements for the use of ICT services supporting critical or important functions,

(iii)the exit strategy and the termination processes. The standards have been developed leveraging the experience with management outsourcing arrangements.

CONCLUSION

Digital Operational Resilience is usually challenged by incidents related to IT systems and services, and there are technical solutions to protect and restore them. However, it is the business operations that rely on IT systems and services that are affected by – but must keep functioning through - such incidents; Operational Resilience is the ability of a business to still operate effectively in the face of such threats to its services.

The threat landscape is more varied than ever and more dangerous; and to best succeed in such an environment requires joined-up thinking – within organisations, within nations, and across the markets of the EU. The DORA is all about harmonising the different national regulations for resilience and reporting, setting out the same rules across the nations of the Union to make the communication of threat intelligence easier and more transparent; and providing the same criteria for reporting and resilience requirements to all organisations in a proportionate way.

Senior management must set the policies that underpin the frameworks of the financial organisations, to ensure that:

- All operational risks have been identified, quantified and controls and mitigations have been put in place,
- All of the procedures and processes are effective and proven through their regular testing and by the actioning subsequent findings,
- All required national - and Union-wide bodies where required - are kept informed of and aware of the incidents and threats faced by institutions and their third-party ICT service providers,
- All third-party suppliers of ICT services fully support the resilience of their peers and the financial entities that use their services,
- Through the use of harmonised regulations, standardised templates and forms, and incident reporting, the institutions and third-party ICT service providers across the EU can work together to mount a significantly more interlocked and resilient face to the ever-growing threats to their services.

BIBLIOGRAPHY

1. Cyber Risk Gmbh. (2023). Digital Operational Resilience act. Retrieved from The Digital Operational Resilience Act (DORA) - Regulation (EU) 2022/2554: https://www.digital-operational-resilience-act.com/
2. ESAs. (2023, June 19). Consultation paper: Draft Regulatory Technical Standards on specifying the criteria for the classification of ICT related incidents, materiality thresholds for major incidents and significant cyber threats under Regulation (EU) 2022/255. Retrieved from European Securities and Markets Authorities: https://www.esma.europa.eu/sites/default/files/2023-06/CP_-_Draft_RTS_on_classification_of_ICT_incidents.pdf
3. ESAs. (2023, June 13). Consultation paper: Draft Regulatory Technical Standards on specifying the criteria for the classification of ICT related incidents, materiality thresholds for major incidents and significant cyber threats under Regulation (EU) 2022/2554. Retrieved from European Securities and Markets Authorities: https://www.esma.europa.eu/document/consultation-paper-draft-rts-ict-risk-management-tools-methods-processes-and-policies
4. ESAs. (2023, June 19). Consultation Paper: On Draft Implementing Technical Standards to establish the templates composing the register of information in relation to all contractual arrangements on the use of ICT services provided by ICT third-party service providers as mandated. Retrieved from European Securities and Markets Authorities: https://www.esma.europa.eu/sites/default/files/2023-06/CP_-_Draft_ITS_on_register_of_information.pdf
5. ESAs. (2023). Consultation Paper: on Draft Regulatory Technical Standards to specify the detailed content of the policy in relation to the contractual arrangements on the use of ICT services supporting critical or important functions provided by ICT third-party service. Retrieved from https://www.esma.europa.eu/sites/default/files/2023-06/CP_-_Draft_RTS_on_policy_on_the_use_of_ICT_services_regarding_CI_functions.pdf
6. ESMA. (2023, July). Annex I for the template register of information at Entity level. Retrieved from European Securities and Markets Authorities: https://www.esma.europa.eu/document/annex-i-template-register-information-entity-level
7. ESMA. (2023, July). Annex II for the template register of information at (sub)consolidated level. Retrieved from European Securities and Markets Authorities: https://www.esma.europa.eu/document/annex-ii-template-register-information-subconsolidated-level
8. EUR-Lex. (2022, December 14). The Digital Operational Resilience Act (DORA) - Regulation (EU) 2022/2554. Retrieved from Access ot European Union Law: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32022R2554
9. Joint Commission of the European Supervisory Authorities. (2023, June 19). DORA: public consultation on the first batch of policy products. Retrieved from European Sceurities and Markets Authority: https://www.esma.europa.eu/sites/default/files/2023-06/DORA_public_consultation_overview_document.pdf

HOW CUBEMATCH CAN HELP

- **WHO WE ARE**

Founded in **2002**, CubeMatch is a **global change and transformation consultancy**, specialising in **Financial Services** and selected as the **chosen partner** for some of the largest and most demanding transformation projects within the Financial Services sector.

CubeMatch is an international brand continuously expanding with **six offices** worldwide : **Dublin, London, Amsterdam, Frankfurt, Singapore and Chennai**. Combining our world class expertise in Financial Services with our rich capabilities in all aspects of change and transformation, we apply a **Multiplier Effect**, helping clients to be more effective today while creating value for tomorrow.

We are **Banking Native**; it runs through our **DNA**. Unlike more general change consultancies, this banking intimacy means we deliver change and transformation programmes that stick, against a backdrop of complex regulations and continuous disruption.

Over the years, we have successfully built a global firm that is uniquely equipped to deliver pragmatic and business-focused results. We have over **400 staff and multi-million euro revenue**. And through our **strategic partnerships** we apply innovation to help organisations operate, compete and deliver at scale. Blending our powerful change capabilities with next generation technology, we deliver **innovation and business agility** to help businesses thrive.

- **OUR GLOBAL SERVICES**

Strategic Change and Programme Delivery

Business and Digital Transformation

Regulatory, Risk and Compliance

Data and Technology

Quality Assurance

Managed Services

- **GET IN TOUCH TODAY**

Visit our website : www.cubematch.com

CubeMatch (Ireland) Ltd
+353 1 253 0020
Ireland@cubematch.com

CubeMatch Ltd (UK)
+44 20 3004 8098
UnitedKingdom@cubematch.com

CubeMatch B.V. (Benelux)
+31 20 312 0404
Benelux@cubematch.com

Other Locations
CubeMatch GmbH (Germany): Germany@cubematch.com
CubeMatch APAC Pte Ltd (Singapore): Singapore@cubematch.com
CubeMatch Claritaz (India): India@cubematch.com

CubeMatch

Powering Change