RISK LEDGER

The Digital Operational Resilience Act (DORA)

A Comprehensive Guide to TPRM Compliance

Evelyn Partners and Risk Ledger – Our Experts

Mark Hendry
Partner
Evelyn Partners
mark.hendry@evelyn.com

Emily Hodges
Chief Operating Officer
Risk Ledger
emily@riskledger.com

Callum Maxwell
Senior Manager
Evelyn Partners
callum.maxwell@evelyn.com

Chris Luenen
Content Marketing Manager
Risk Ledger
chris@riskledger.com

Key Dates

27 December 2022

DORA published in the Official Journal of the European Union as Regulation (EU) 2022/2554

29 September 2023

European Supervisory Authorities' technical standards submitted to EU Commission.

16 January 2023

DORA entered into force

17 January 2025

Implementation deadline. DORA will apply from this date.

Overview

The Digital Operational Resilience Act (DORA) is a comprehensive regulation introduced by the European Union to strengthen the financial sector's resilience against ICT-related disruptions and threats.

DORA aims to consolidate and upgrade ICT risk requirements throughout the financial sector to ensure that all participants of the financial system are subject to a common set of standards to mitigate ICT risks to their operations.

Key objectives of DORA:

Enhance and streamline the financial entities' conduct of ICT risk management

Establish a thorough testing of ICT systems

Increase supervisors' awareness of cyber risks and ICT-related incidents faced by financial entities

Introduce powers for financial supervisors to oversee risks stemming from financial entities' dependency on ICT third-party service providers

Create a consistent incident reporting mechanism

Ensure sound monitoring of ICT third-party risk

Identify and mitigate concentration and systemic risks to financial entities and the sector as a whole

Overview

DORA is part of the European Commission's Digital Finance Package, which aims to support the EU's digital transition in finance while regulating its risks.

The regulation represents a significant shift in how financial institutions approach operational resilience and cybersecurity, moving from a fragmented, sector-specific approach to a unified, cross-sector framework.

Five Reasons to Care about DORA

Personal Liability for Leadership

Board members and senior management are now personally accountable for DORA compliance. This shift in responsibility means that ICT risk management is no longer just an IT issue, but a critical boardroom concern.

Hefty Financial Penalties

Non-compliance can result in severe financial penalties for FS firms, for ICT third-parties as well as for individuals and board members. The exact fines and penalties for FS firms will be determined by individual EU member states, while the Lead Overseer (one of the ESAs) can impose administrative penalty payments of up to 1% of the average daily worldwide turnover in the preceding business year on ICT third parties.

Global Reach and EU Presence Requirement

DORA's impact extends beyond EU borders. Critical ICT service providers based outside the EU must establish a subsidiary within the EU for oversight purposes. This requirement has significant operational and strategic implications for global organisations.

Implications for Intra-Group ICT Providers

The draft Regulatory Technical Standards JC 2023 84 also considers intra-group ICT service providers as a subcategory of ICT third party service providers, and thus treats them in the same way.

Implications for UK Entities Post-Brexit

Despite Brexit, UK financial institutions and ICT service providers considered critical and offering services in the EU, directly or indirectly, must comply with DORA for their EU operations. This extends DORA's reach to entities based outside the EU.

Key Pillars of DORA

ICT Risk Management	• Requires financial entities to have a comprehensive and well-documented ICT risk management framework • Mandates regular review and updating of the framework • Emphasises the need for clear roles and responsibilities in ICT risk management • Robust and thorough business continuity policies, along with disaster recovery plans, must be established to guarantee a swift recovery following any ICT-related incident
Incident Classification and Reporting	• Establishes a harmonised approach to classifying ICT-related incidents, as set out in DORA and developed by ESAs • Requires financial entities to report major ICT-related incidents to competent authorities within 24 hours • Mandates root cause analysis and follow-up reporting for major incidents • Provide initial, intermediate, and final reports on ICT-related incidents to the firm's users and clients
Digital Resilience Testing	• Introduces requirements for regular testing of ICT systems and controls • Mandates advanced testing, including threat-led penetration testing, for significant financial entities and certain critical ICT third party providers • Aims to identify vulnerabilities and improve overall cyber resilience
Third-Party Risk Management	• Sets out stringent requirements for managing ICT third-party risk • Mandates risk assessment and due diligence processes to be conducted on ICT third-party service providers • Requires contractual arrangements to include comprehensive service level agreements as well as clear exit plans for ICT third parties that support critical or important functions, and which must be reviewed regularly. • Requires the continuous monitoring of critical ICT third party security postures for the full contract lifecycle. • Requires an acute awareness, and mitigation, of any risks posed by sub-contracting and potential concentration risks.
Information Sharing	• Encourages financial entities to strengthen their collective resilience through collaboration among financial entities. • Suggests participating in trusted communities for the secure exchange of sensitive information. • Aims to foster a culture of proactive defence by exchanging cyber threat intelligence and best practices.

DORA's Scope

1. Banking Sector

- Credit Institutions
- Payments Institutions
- Electronic Money Institutions

2. Investment Sector

- Investment Firms
- UCITS management companies
- Alternative investment fund managers

3. Insurance Sector

- Insurance / reinsurance undertakings
- Insurance intermediaries

4. Market Infrastructure

- Central security depositories
- Trading venues
- Trading repositories

5 . Digital Finance

- Crypto Asset Service Providers
- Crowdfunding service providers

6. Other Financial Entities

- Credit rating agencies
- Audit firms

7. ICT Third-Parties

- Critical ICT 3rd Party service providers
- Includes cloud, software, and analytic service providers

DORA has a proportionality principle!

- Requirements depend on the size of the entity, its nature, and risk profile
- Smaller and less complex organisations will have fewer requirements

DORA's Scope

DORA's scope encompasses a wide range of entities across the financial services sector. **It applies to traditional institutions like credit institutions, payment institutions, and electronic money institutions, as well as investment firms, Fintech's and crypto-asset service providers.** The regulation also covers crucial market infrastructure entities such as central securities depositories, central counterparties, trading venues, and trade repositories.

Asset management is within DORA's purview, including managers of alternative investment funds and management companies. The scope extends to entities involved in data services and reporting, the insurance sector (including various types of intermediaries), and other financial service providers such as credit rating agencies, auditors, and crowdfunding service providers.

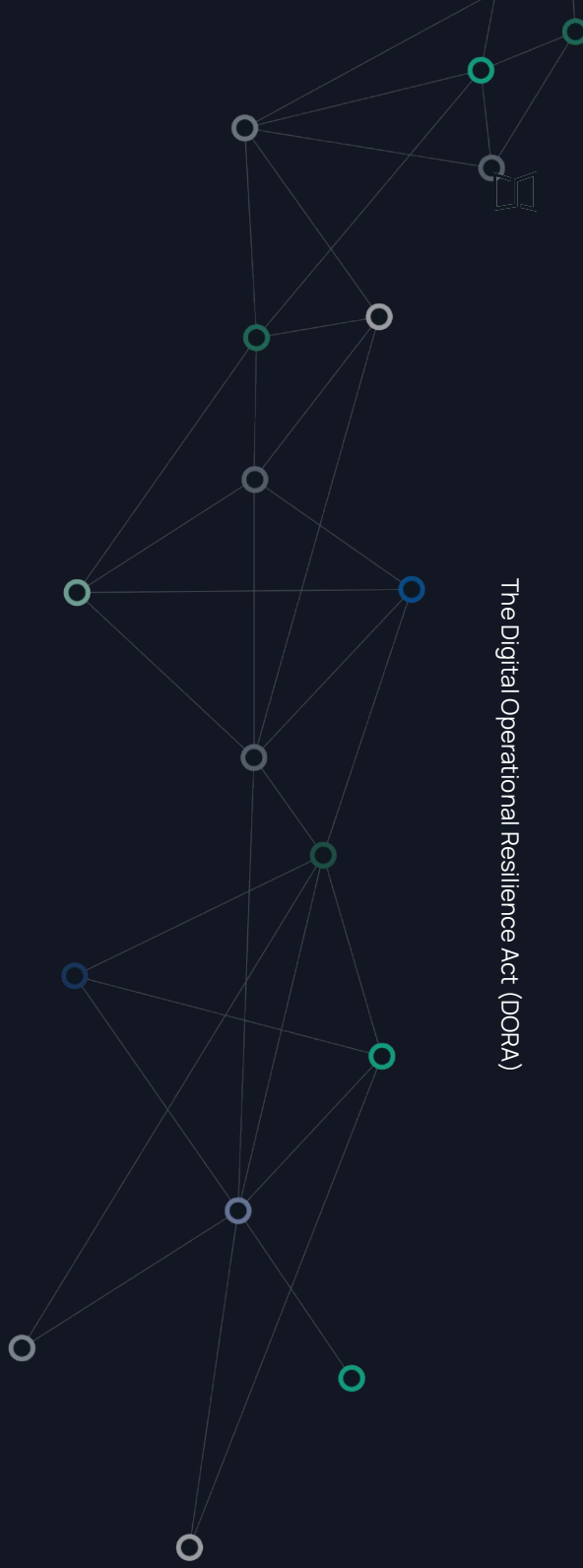
Notably, DORA's reach extends beyond financial entities to encompass ICT third-party service providers supporting critical or important functions. This inclusion recognises these providers' critical role for the financial sector's operational resilience and represents a significant expansion of regulatory oversight into the tech providers servicing the financial industry.

Implications for UK Financial Institutions

While DORA isn't currently law in the UK, it will likely apply or be mirrored in UK legislation. UK authorities have hinted at adopting similar regulations. All organisations, whether in the EU, UK, or elsewhere, should assess whether they will fall within the scope of DORA or similar regulations and prepare accordingly.

See Appendix I for further information.

DORA'S Requirements



The Digital Operational Resilience Act (DORA)

2024

DORA's Requirements:
ICT Risk Management

DORA mandates that financial entities establish and maintain a robust, comprehensive, and well-documented ICT risk management framework. This framework must be regularly reviewed and updated to adapt to evolving threats. Clear roles and responsibilities for ICT-related functions need to be defined within the organisation.

Entities are required to implement appropriate and proportionate security strategies, policies, procedures, protocols, and tools to ensure resilience. Additionally, DORA emphasises the need to address risks related to legacy ICT systems, recognising the potential vulnerabilities in older technologies.

For TPRM, this means extending risk management strategies and frameworks to all third-party providers, ensuring their risk management practices align with the organisation's and including them in overall ICT risk assessments and frameworks. Critical Third Party Providers **(CTPPs) are subject to additional oversight and must comply with stricter regulatory requirements.** This approach helps identify and mitigate risks across the entire service provider network.

- **Do we have a comprehensive ICT risk management framework?**
- **When was our last framework review?**
- **Are ICT roles and responsibilities clearly defined?**
- **Are our security policies up to date?**
- **How are we addressing risks in legacy systems?**

DORA's Requirements:
ICT-Related Incident Reporting

Under DORA, financial entities must establish and implement a management process to monitor and log ICT-related incidents. These incidents are to be classified based on criteria specified in the regulation. **A key requirement is the timely reporting of major incidents to relevant competent authorities within specified timeframes.**

Moreover, entities are obligated to inform clients and counterparts that are potentially affected by a major ICT-related incident, ensuring transparency and allowing for appropriate risk mitigation measures to be taken by affected parties.

TPRM implications include setting up clear incident reporting procedures with third-party providers, ensuring they can meet DORA's reporting requirements, and quickly assessing the impact of third-party incidents on critical services. Financial entities should also consider how any incidents at one of their critical ICT third parties feed into their required exit plans, and whether any contractual clauses have to be added to the contracts with service providers supporting critical or important functions to that effect.

- **Is our incident monitoring process effective?**
- Do we have established relationships with the suppliers' security teams?
- **Can we classify incidents according to DORA criteria?**
- **Are we prepared to report major incidents within the required timeframe?**
- **Do we have a process to inform affected clients and counterparts?**
- Do you have a full register of all your suppliers and information on their security controls at hand that you can quickly consult for context when an incident occurs?

DORA's Requirements:
Digital Operational Resilience Testing

DORA requires financial entities to establish a robust and comprehensive digital operational resilience testing programme. This programme **should include a full range of appropriate tests, such as vulnerability assessments and scans, open-source analyses, network security assessments, gap analyses, physical security reviews, and source code reviews** where feasible.

Penetration tests, threat scenario-based tests, as well as operational continuity and disaster recovery tests are also mandated. For significant financial entities, DORA introduces the requirement of advanced testing using threat-led penetration testing (TLPT). All tests of ICT tools, systems, and processes should be based on thorough risk assessments, well-defined test plans and regular internal audits. These internal audits should embed operational resilience thinking across all reviews to ensure a 'resilience by design' culture.

From a TPRM perspective, some critical third-party providers will have to be included in resilience testing programmes. This may require negotiating rights to test third-party systems and coordinating penetration testing with key service providers.

- **Do we have a comprehensive digital operational resilience testing programme in place?**

DORA's Requirements:
ICT Third-Party Risk Management

DORA places significant emphasis on ICT third-party risk management. Financial entities are required to implement a comprehensive strategy for ICT third-party risk, which should be integrated with the overall business strategy. **They must maintain a detailed Register of Information (RoI) relating to all contractual arrangements involving ICT services provided by third-party providers. Given the comprehensive nature of these RoI's, they will likely have to be compiled from various tools and sources such as contract lifecycle and supplier management systems, third-party risk management registers as well as, in most cases, from unstructured data derived from contracts as well as open source information.**

Assessing potential concentration risk associated with these arrangements is crucial. Before entering into any contractual agreements, entities must conduct comprehensive risk assessments and due diligence on prospective ICT third-party service providers. For critical or important functions, contractual arrangements must meet specific requirements outlined in DORA. Importantly, the regulation mandates continuous monitoring of ICT third-party service providers to ensure ongoing compliance and risk management.

With regard to TPRM, DORA stipulates that financial institutions "may only enter into contractual arrangements with ICT third-party service providers that comply with appropriate information security standards" and to "take due consideration of the use, by ICT third-party service providers, of the most up-to-date and highest quality information security standards."

- **Is our ICT third-party risk strategy integrated with our business strategy?**
- **Is our third-party service provider register up to date?**
- **Have we assessed potential concentration risks?**
- **Are we conducting thorough due diligence on new providers?**
- **Do our contracts for critical functions meet DORA requirements?**
- **How are we continuously monitoring our ICT third-party providers?**

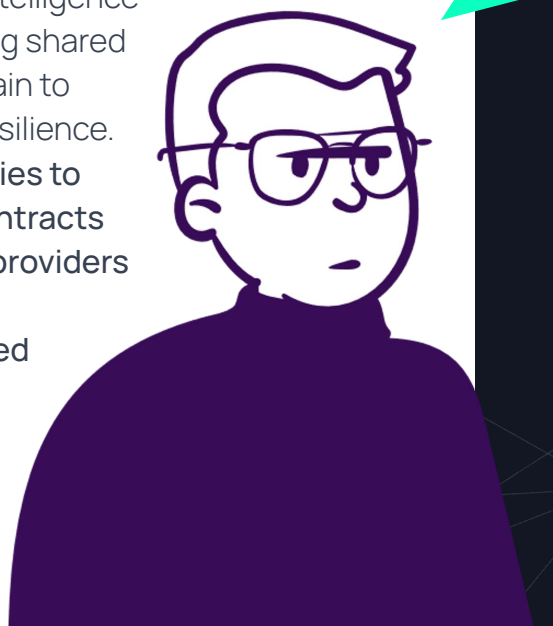
DORA's Requirements:
Information Sharing

DORA promotes a collaborative approach to cybersecurity by requiring financial entities to participate in EU-wide information sharing arrangements. This participation aims to enhance overall cyber awareness within the financial sector.

To facilitate this sharing, **entities must establish appropriate protections for the exchange of sensitive information, ensuring that valuable insights can be shared without compromising security.** Additionally, financial entities are required to report on their participation in these information-sharing arrangements to competent authorities, allowing for oversight of this collaborative effort to improve sector-wide resilience. Among leading information-sharing networks for the financial sector, FS-ISAC stands out, which is also running their own community for FS firms on Risk Ledger to facilitate greater collaboration on identifying shared concentration and systemic risks to the sector.

For TPRM, this requirement involves considering whether and how to include third-party providers in these initiatives. This could mean establishing protocols for sharing threat intelligence with key providers and applying shared insights across the supply chain to enhance overall ecosystem resilience. **DORA requires financial entities to include provisions in their contracts with ICT third-party service providers for incident notification and cooperation during ICT-related incidents.**

- **Are we participating in EU-wide information sharing arrangements?**
- **Do we have proper protections for sharing sensitive information?**
- **Are we reporting our information-sharing activities to authorities?**
- **How can we improve our collaborative cybersecurity efforts?**



Critical Third Parties under DORA

Key Considerations

- Preparedness for direct oversight by EU financial supervisors
- Ability to meet stringent security and resilience standards
- Readiness to provide comprehensive information and access for audits
- Capacity to support financial entities in their DORA compliance efforts
- Development of robust business plans

Critical Third Parties under DORA

Contractual Arrangements

DORA introduces 'critical ICT third-party service providers' (CTPPs), essential to the financial sector. These include cloud platforms, data analytics providers, and other key ICT services crucial for financial entities' operations.

Oversight Framework

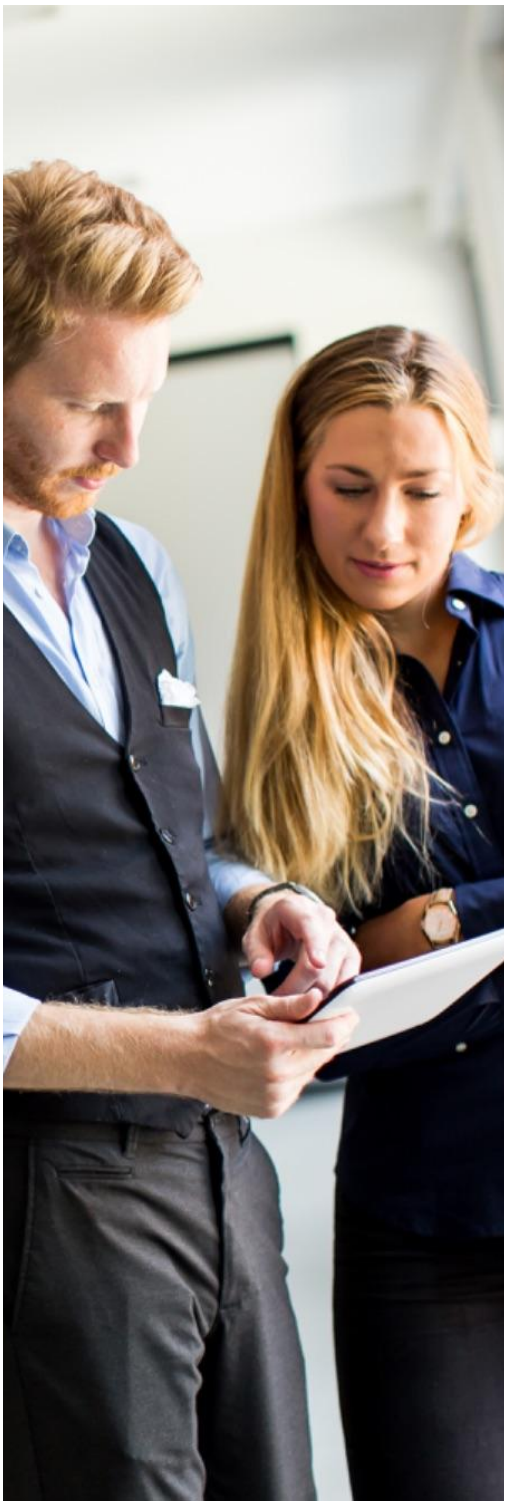
DORA establishes direct supervision of CTPPs by EU financial supervisors. This framework addresses concentration and systemic risks in the financial sector's ICT ecosystem.

Key Requirements for Financial Entities

Financial entities must maintain a register of ICT third-party arrangements, conduct due diligence, ensure DORA-compliant contracts, and continuously monitor CTPPs supporting critical functions.

Risk Management Implications

Financial entities must manage both their own ICT risks and those of CTPPs. This includes assessing concentration risks, potential failures, and the impact of CTPP disruptions on operations and the broader financial system.



Contractual Arrangements under DORA

Service Definition and Performance Monitoring

Contracts must provide a detailed description of all services, clearly delineating responsibilities between parties. Specific, measurable performance metrics must be established, along with mechanisms for continuous monitoring and enforcement. The agreement should include provisions for regular performance reviews.

Data Governance and Security

Agreements must identify all data processing locations and outline comprehensive data protection measures aligned with relevant regulations. The contract should detail security protocols for data confidentiality, integrity, and availability, including procedures for breach notification.

Audit and Regulatory Compliance

Contracts should grant unrestricted audit rights to the financial entity and provide for regulatory authorities' access. The service provider should be obligated to maintain detailed logs, assist in regulatory investigations, and adhere to evolving regulatory requirements. Provisions for joint audits and penetration testing should be included to ensure thorough oversight.

Exit Strategy and Operational Continuity

The contract must define termination rights and include a detailed exit plan ensuring smooth transition of services. Provisions for data portability and rules on subcontracting should be specified. The service provider should be required to assist in migration efforts.

DORA mandates contractual safeguards for ICT third-party services in the financial sector. These requirements aim to enhance transparency, control, and risk mitigation in service relationships.

By specifying key contractual elements, DORA seeks to strengthen the resilience and security of the financial industry's digital ecosystem.

DORA on Sub-contracting and Concentration Risks

DORA emphasises reducing concentration risk in financial services supply chains.

Key areas of focus here include:

- **Non-substitutable ICT Providers** - DORA highlights the risks associated with relying on ICT service providers that cannot be easily replaced, recognising the potential for disruption if these providers face issues.
- **Multiple Critical Arrangements** - The regulation addresses the risks of having multiple critical or important functions dependent on the same ICT third-party service provider or closely connected providers.
- **Systemic Risk and Fourth-Party Risk** - DORA emphasises the potential systemic risk inherent in the increasing trend towards outsourcing and the concentration of ICT third-party providers. This emphasis underscores current inadequacies in understanding and mitigating potential fourth-party risk – risks arising from subcontractors and other fourth parties. Moreover, it addresses the potential systemic risks to the financial sector as a whole that can result from commonly shared suppliers, i.e. CTPPs that serve many financial services clients at the same time.

Requirements for Financial Firms

- **Risk Assessment:** Firms must identify and assess all relevant risks in relation to their contractual arrangements with ICT service providers, including with some key sub-contractors that support critical functions.
- **Avoiding Concentration:** Firms are explicitly instructed to ensure that their practices do not contribute to reinforcing ICT concentration risk.

Continuous Monitoring and Exit Strategies

DORA mandates financial entities to manage ICT third-party risks through continuous monitoring and exit planning. These strategies aim to enhance operational resilience by overseeing ICT providers and preparing for potential disruptions. Entities must assess critical ICT providers' performance and risk management, while developing tested exit strategies for smooth transitions in case of contract terminations.

Continuous Monitoring

Financial entities must establish an appropriate Oversight Framework to continuously monitor and review ICT third-party service providers' security controls and wider performance. This monitoring focuses particularly on critical ICT third-party service providers. As part of this process, entities are required to assess the overall ICT risk management of these providers. This includes evaluating their data handling practices, specifically examining whether the CTTP can ensure the availability, authenticity, integrity, and confidentiality of data, whether personal, sensitive, or non-personal.

Exit Strategies

DORA requires financial entities to develop comprehensive and documented exit strategies, especially for arrangements supporting critical or important functions. These strategies must be sufficiently tested to ensure their effectiveness. The primary purpose of these exit strategies is to prepare for potential contract terminations. Such terminations may be necessary in cases of significant breaches of laws, regulations, or contractual terms by the ICT third-party service provider. Additionally, exit strategies should be implemented if the continuous monitoring process reveals evidenced weaknesses in the provider's ICT risk management practices.

Key Regulatory Technical Standards under DORA

Regulatory Technical Standards (RTS) are critical for DORA's effective implementation, translating its principles into specific, actionable requirements. They ensure consistent application across the EU financial sector, providing essential guidance on ICT risk management, incident reporting, and third-party oversight, thus enabling financial entities to align precisely with DORA's framework and enhance their digital operational resilience. Some examples include:

RTS on ICT Risk Management Framework	• Harmonises ICT risk management across financial sectors • Specifies key elements of a simplified ICT risk framework • Complements DORA with additional risk management requirements
RTS on criteria for the classification of ICT-related incidents	• Defines criteria for classifying ICT-related incidents as major. • Establishes criteria and thresholds for determining when an incident is considered major. • Helps financial entities determine which incidents require reporting.
Implementing Technical Standards (ITS) to establish the templates for the register of information.	• Sets out the details for the standardised Register of Information to be maintained by financial entities and used to report information on their contractual arrangements with ICT third-party service providers to the ESAs. • Establishes the specific reporting requirements and procedures for financial entities to submit their RoI's to the competent authorities. • Provides guidelines to competent authorities on how to assess and analyse the information received.
RTS to specify the policy on ICT services supporting critical or important functions provided by ICT third-party service providers (TPPs)	• Specifies the content of the policy on ICT services supporting critical or important functions, including risk assessment, documentation, and monitoring requirements. • Establishes criteria for financial entities to assess the criticality or importance of functions supported by ICT services. • Defines requirements for contractual arrangements with ICT third-party service providers, including service level agreements, termination rights, and exit strategies.

Key Regulatory Technical Standards under DORA

RTS and ITS on the content, format, templates and timelines for reporting major ICT-related incidents and significant cyber threats	• Establishes the content, timelines, and procedures for financial entities to report major ICT-related incidents and significant cyber threats to competent authorities. • Specifies standardised templates and forms for reporting incidents and threats, aiming to harmonise the reporting process. • Introduces proportionate reporting requirements, including extended timelines for intermediate and final reports, streamlined reporting fields, and provisions for weekend reporting and aggregated reporting.
RTS on the harmonisation of conditions enabling the conduct of the oversight activities	• Specifies the information ICT third-party service providers must provide when voluntarily requesting to be designated as critical. • Establishes the content, structure, and format of information critical ICT third-party providers must submit to the Lead Overseer, including a template for subcontracting arrangements. • Outlines the details for competent authorities' assessment of measures taken by critical ICT third-party providers based on the Lead Overseer's recommendations.
RTS specifying the criteria for determining the composition of the joint examination team (JET)	• Establishes criteria for determining the composition of joint examination teams, ensuring balanced participation from ESAs and competent authorities. • Specifies the designation process, tasks, and working arrangements for joint examination team members. • Outlines procedures for assessing team effectiveness and managing confidential information access.
RTS on threat-led penetration testing (TLPT)	• Specifies criteria for identifying financial entities required to perform threat-led penetration testing (TLPT), including impact-related factors, financial stability concerns, and ICT risk profiles. • Establishes requirements and standards for the use of internal testers, testing methodology, and approach for each phase of TLPT, including scope, results, closure, and remediation. • Outlines the type of supervisory and other relevant cooperation needed for TLPT implementation and mutual recognition, particularly for financial entities operating in multiple Member States.

Appendix 1

Which non-EU organisations fall under the remit of DORA

Organisations without offices in the EU that may fall under DORA's remit include:

1. **Financial entities:**
    - Third-country financial entities operating in the European Union, even without a physical presence. This could include:
        - Alternative Investment Fund Managers (AIFMs) established outside the EU but managing or marketing funds in the EU
        - Third-country firms providing investment services or performing investment activities through the establishment of a branch in the Union

The exact scope depends on the specific EU sectoral laws for each type of financial entity. For example, UCITS management companies are required to be established in the EU, so third-country UCITS managers would not be directly in scope.

2. **ICT third-party service providers:**
    - ICT service providers established outside the EU may be designated as "critical" by the European Supervisory Authorities (ESAs) if they provide services to in-scope EU financial entities. This could include providers of:
        - Cloud computing services
        - Software services
        - Data analytics services
        - Network infrastructure services
        - Data centre services

Appendix 1

Organisations outside the EU falling under the remit of DORA.

Some example scenarios

Based on the available information, here are ten examples of when non-EU based financial services entities may have to comply with DORA:

1. A third-country Alternative Investment Fund Manager (AIFM) managing or marketing funds in the EU.
2. A non-EU investment firm providing investment services or performing investment activities through a branch established in the EU.
3. A third-country financial entity operating in the European Union, even without a physical presence, if it falls under one of the categories covered by DORA.
4. A non-EU based payment institution or electronic money institution offering services in the EU.
5. A third-country crypto-asset service provider authorised under MiCA (Markets in Crypto-Assets Regulation) to operate in the EU.
6. A non-EU based crowdfunding service provider authorised to operate in the EU under relevant EU regulations.
7. A third-country firm acting as a delegate for an EU-based financial entity that is subject to DORA (indirect compliance may be required).
8. A non-EU parent company of an EU financial services firm providing ICT services to its EU subsidiary.
9. A third-country ICT service provider designated as "critical" by the European Supervisory Authorities (ESAs) for its services to in-scope EU financial entities.
10. A non-EU financial entity that belongs to a group where other entities within the group are subject to DORA, potentially requiring group-wide compliance measures.

NOTE: It's important to note that the exact scope of DORA's application to third-country entities may vary depending on the specific type of financial entity and the relevant EU sectoral laws. In some cases, there remains a lack of clarity regarding the precise territorial scope, and further guidance from regulators may be needed.

We have taken great care to ensure the accuracy of this publication. However, the publication is written in general terms and you are strongly recommended to seek specific advice before taking any action based on the information it contains. No responsibility can be taken for any loss arising from action taken or refrained from on the basis of this publication.

E: mark.hendry@evelyn.com I www.evelyn.com
Evelyn Partners Group Limited
45 Gresham Street, London EC2V 7BG

Evelyn Partners Group Limited
Issued by the Evelyn Partners group of companies (the "Group") which comprises Evelyn Partners Group Limited and any subsidiary of Evelyn Partners Group Limited from time to time. Registered in England at 45 Gresham Street, London EC2V 7BG. No. 08741768.

Evelyn Partners LLP
The title 'Partner' does not mean that the individual is necessarily a partner of Evelyn Partners LLP. For a full list of LLP partners, please refer to Companies House or request directly from us. Registered in England at 45 Gresham Street, London EC2V 7BG. No. OC 369631.

CLA Evelyn Partners Limited
Registered to carry on audit work in the UK and Ireland and regulated by the Institute of Chartered Accountants in England and Wales for a range of Investment business activities. Registered in England at 45 Gresham Street, London EC2V 7BG. No. 04469576.

Regulated by the Instituted of Chartered Accountants in England and Wales / Institute of Chartered Accountants in Ireland for a range of investment business activities. Registered to carry on audit work in the UK and Ireland and regulated for a range of investment business activities by the Instituted of Chartered Accountants in England and Wales / Institute of Chartered Accountants in Ireland.

E: emily@riskledger.com I www.riskledger.com
Risk Ledger Ltd.
Adam House,
7-10 Adam Street,
London,
WC2N 6AA
United Kingdom

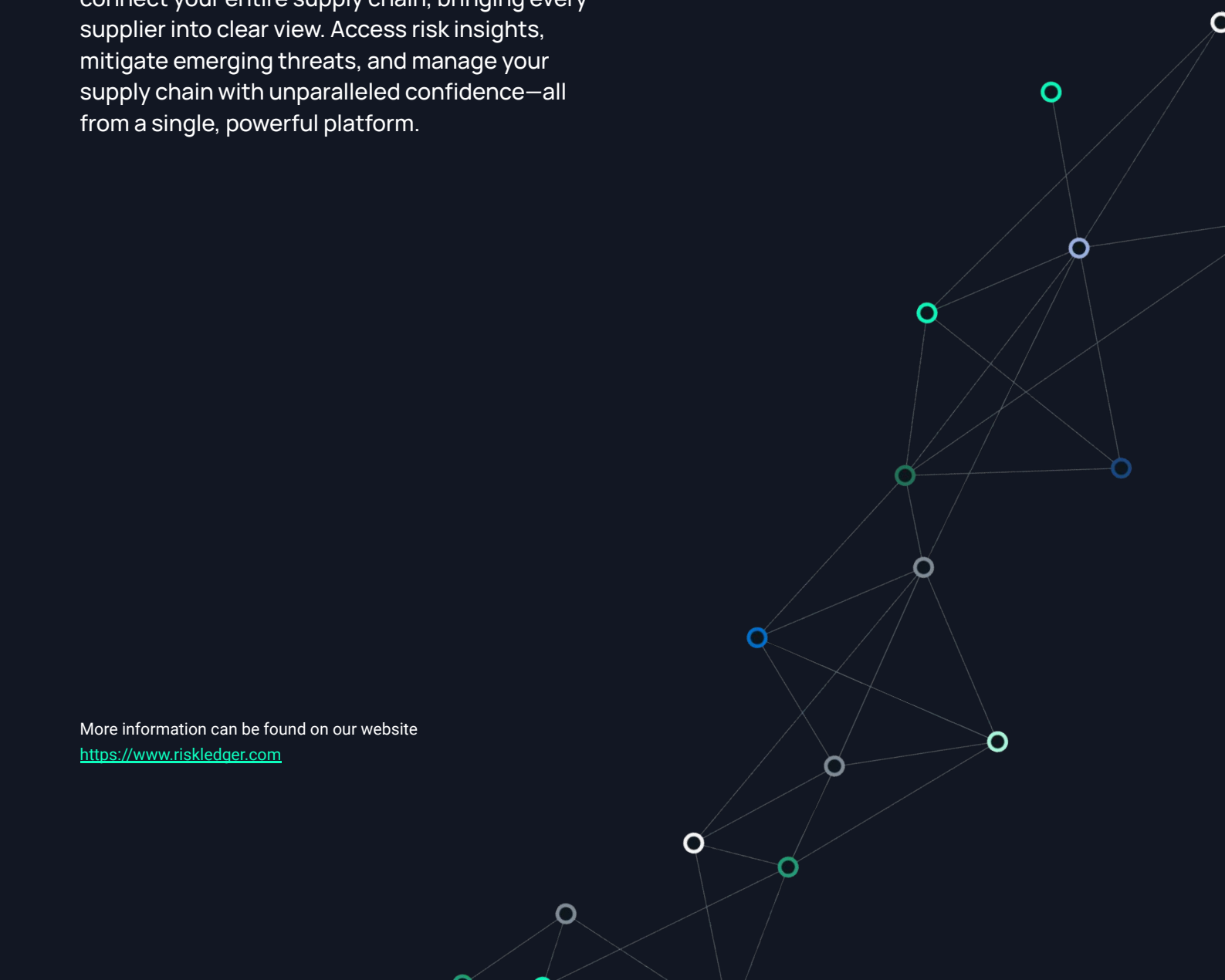
Risk Ledger was founded in 2018 by Haydn Brooks and Daniel Saul, with a mission to shift the way organisations approach cybersecurity and information management in the supply chain.

We are making an impact by changing the way organisations identify, measure and mitigate security risks for themselves, their clients and their suppliers. In doing so, we plan to reduce the number of global data breaches experienced by companies and consumers as a result of supply chain attacks.

We provide organisations, large and small, with the tools and knowledge they need to increase their security maturity. By offering the data and resources needed to efficiently measure and mitigate their levels of cyber risk, we enable organisations to truly understand the entirety of their security landscape.

Thank You.

Risk Ledger transforms third-party risk management by enabling you to onboard and connect your entire supply chain, bringing every supplier into clear view. Access risk insights, mitigate emerging threats, and manage your supply chain with unparalleled confidence—all from a single, powerful platform.



More information can be found on our website
https://www.riskledger.com