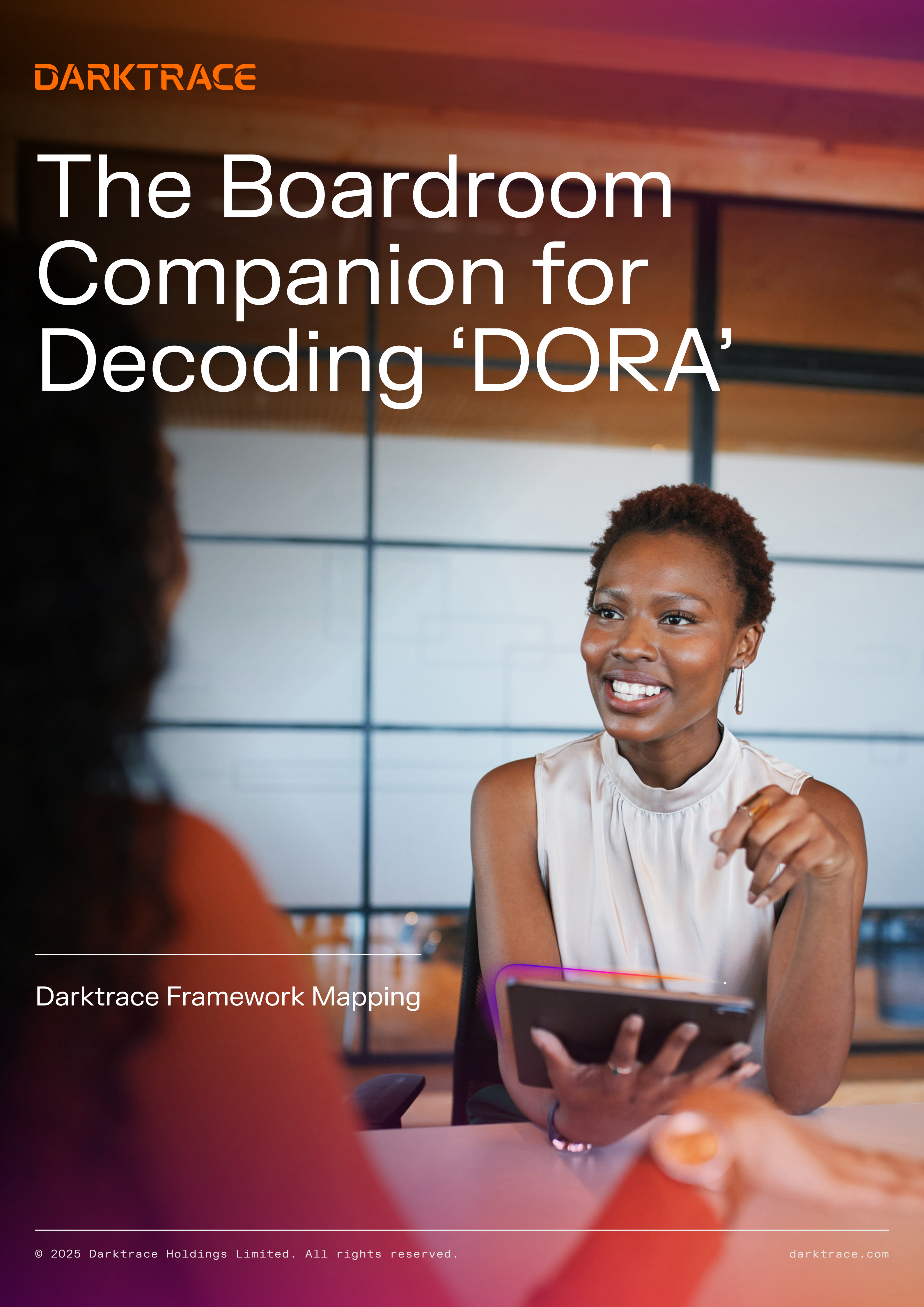

DARKTRACE

The Boardroom Companion for Decoding ‘DORA’

Darktrace Framework Mapping

Contents

Executive Summary

What is DORA?

DORA is the European Union’s Digital Operational Resilience Act (EU Regulation 2022/2554) (“DORA”)

Who is impacted by DORA?

Financial institutions who are operating in the European Union – see Article 2(1) to confirm whether your organisation falls within its scope. 3rd party providers may fall in scope for some requirements.

When did DORA come into force?

16th January 2023, with mandatory compliance by 17th January 2025.

Why was DORA enacted?

To encourage more diligent oversight by financial institutions by having proper procedures in place to prevent and recover from threats to operational capabilities. Putting aside finances to compensate for events once they have occurred is no longer sufficient.

What are the consequences of non-compliance?

- Fines for financial institutions of up to 2% of worldwide turnover, or EUR 20million, whichever is higher. Individual fines of up to EUR 1 million.
- Fines for third party providers of up to EUR 5 million or 1% of worldwide turnover for each day of non-compliance, for up to 6 months. Individual fines of EUR 500k.
- Reputational consequences, regulatory consequences, and termination of key contracts are a consideration for both parties.

How do you comply with DORA?

Financial institutions should consider the following approach to ensure that they have identified and taken appropriate steps towards compliance:

- Conducting gap analyses of existing processes and functions to determine where there are deficiencies, and take appropriate steps to address them.
- If using third parties to assist in filling identified gaps, choose wisely and make sure appropriate terms and conditions are in place which properly reflect the product/service being purchased. A one-size-fits-all approach is unlikely to be sufficient.
- Allocate appropriate and realistic budgets to cybersecurity strategy, so that a strong cyber resilience programme can be implemented.
- Put in place an effective ISMS policy which covers detection, response and recovery.

Setting the scene

First appearing on the scene in 2020 as part of the European Union's Digital Finance Package, DORA was enacted into European Law in January 2023 to consolidate existing legislative frameworks for financial institutions in Europe, and elevate and introduce standards to address key gaps.

One of these gaps, was the level of oversight and responsibility that financial institutions must have to ensure that their systems can withstand and respond to cyber threats. Traditionally, a trend of allocating finances to compensate for losses incurred as a result of a breach has been the preferred method of dealing with cyber attacks. However, given the increasing number of attacks across all industries (including banking, insurance and investment firms) and growing concerns over the damage caused by successful breaches, this approach was deemed insufficient.

Recognising the significant upheaval that enacting DORA-compliant processes may have on financial institutions which fall within its remit, financial institutions were provided with a two-year grace period to make the necessary changes. The deadline for making these changes was 17th January 2025, at which point the European Commission would start policing compliance with DORA through a number of designated 'supervisory authorities'. The risks for failing to comply with DORA post-17th January 2025 are set out in the 'CORE CONCEPTS' section below.

Core concepts

Technology (or 'ICT' as it is referred to in DORA), has become essential to the success of European Union financial institutions, and whilst technology can be a great asset, it can also be a burden if not utilised intuitively. As businesses increasingly rely on technological infrastructure, threat actors are exploiting the expanding attack surface with more sophisticated tactics and resources.

DORA is comprised of five core concepts which can help mitigate the capabilities of these threat actors; however, an effective cybersecurity strategy is essential to fulfilling their requirements. Whilst Darktrace's products have not been specifically designed with DORA in mind, Darktrace has a wealth of experience in deploying its proprietary cybersecurity software to thousands of organisations since its inception, including the financial sector. Where we believe our products can be a tool in your arsenal in relation to each of the following concepts, we have specified as such.

Darktrace ActiveAI Security Platform™

Darktrace's ActiveAI Security Platform is designed to detect, prevent and respond to cyber threats, which in turn could assist financial institutions with their obligations to withstand and recover from an attack.

It is comprised of 6 core products which adapt to your specific environment and provide you with the tools you need to stay ahead of potential attackers. It is important to note that the requirements at Articles 5 – 15 do not apply to the small list of exempted organisations which are listed in Article 16. If you believe you may be subject to an exemption, please refer to Article 16(1) of DORA.

1. ICT Risk Management

Key Articles: Chapter II contain details of ICT Risk Management requirements.

ICT Risk Management is the purpose of DORA. To manage risk, they need to be identified, assessed, and have measures to mitigate their impact. This is an ongoing and continuous obligation, so whilst it is wholly appropriate for financial institutions to conduct a gap analysis and implement measures at the outset, an appropriate information security management system ("ISMS") is needed to test the effectiveness of those measures. This ISMS needs to be reviewed regularly.

Cyber threats present a very real and ever-present risk to the highly valuable information that is held by financial institutions. Threat actors are constantly attempting to exploit vulnerabilities and deficiencies in the networks of financial institutions with increasingly sophisticated efforts.

One example is Ransomhub, a RaaS (Ransomware-as-a-service) that launches targeted attacks commonly exploiting known vulnerabilities in internet-facing applications and uses phishing and spear-phishing attacks to gain entry, along with credential stuffing and brute- force attacks to exploit weak authentication mechanisms.

It is therefore imperative that financial institutions either build their own systems to manage these types of threats (which can be an infinitely expensive process) or utilise the services of experienced third parties who already have the relevant tools and expertise. Where third parties are instructed, their criticality and involvement will need to be carefully mapped.

Article	Requirement	Darktrace Features
7	Financial institutions must use and maintain updated ICT systems which are appropriate, reliable, equipped with sufficient capacity to deal with processing and volume of data, and technologically resilient.	Darktrace's products do not conduct this exercise for customers, but we have a wealth of experience in working with organisations of all sizes. Our tools are updated regularly and automatically with no hidden costs for version updates. Our products can also assist with mapping systems, protocols and tools in your network, and can be configured to alert and prevent the use of specified systems, protocols and tools which may be less secure.
8	Financial institutions are required to identify risks and assess cyber threats and ICT vulnerabilities which are relevant to their functions, and risk exposure to/from other financial institutions, on a continuous basis.	Darktrace / Proactive Exposure Management can provide visibility of systems and key information about their type and status, including any risks, threats and vulnerabilities which have been identified therein using either third—party integrations or our own native active scanning. These risks are prioritised and quantified based on inherent risk and weakness.
9	Financial institutions are required to continuously monitor and control the security and functioning of ICT systems.	Darktrace's products conduct monitoring in real-time to identify potential risks using threat detection capabilities which are based on your pattern of life.
9	Financial institutions are required to establish a sound network and infrastructure management structure using appropriate techniques, methods and protocols that may include implementing automated mechanisms to isolate affected information assets in the event of cyber-attacks.	This can be achieved through the use of any of Darktrace's core platform products that come with Autonomous Response capabilities.
10	Financial institutions are required to have mechanisms in place which promptly detect anomalous activities.	Darktrace's products are designed to detect anomalies across your estate.
11	Financial institutions are expected to have a robust business continuity policy in place, which specifies methods to quickly, appropriately and effectively respond to ICT-related incidents.	The use of Darktrace products can be used by financial institutions in achieving these aspects of the requirements. Additionally, Darktrace / Incident Readiness & Recovery can be used to simulate incidents and therefore inform how this process can be designed.
12	Financial institutions are required to develop and document backup policies and procedures specifying scope and frequency of backups, and restoration and recovery procedures and methods.	Whilst Darktrace does not provide backup or storage solutions for its customers, we understand that this is a key concern. Darktrace / Incident Readiness & Recovery's incident response playbooks can help to inform this process, by providing out of the box best practices for incident response delivered through AI compiled playbooks which can be customized to account for an organization's specific policies and procedures.
13	Financial institutions are required to gather information on vulnerabilities and cyber threats and analyse the impact they are likely to have on their infrastructure and analyse the impact they have on their operations.	Darktrace provides various mechanisms to continuously refine prioritisation, detection and response logic, and categorisation of events. Darktrace supports a robust feedback workflow to support this requirement and we are happy to engage in reviews with our customers on a periodic basis, through the deployment of a dedicated Customer Success Manager to look after customers during their deployments.
14	Financial institutions are required to have effective communication plans in place to streamline communications on ICT-related matters both internally and externally.	Darktrace / Incident Readiness & Recovery's communication center allows organizations to assign incident responders and stakeholders to different groups and streamline their communications. Similarly, it can develop playbooks which can be customized to reflect an organization's communication plan.

2. Incident Reporting for ICT-Related Incidents

Key Articles: Chapter III contains details of the Incident Reporting requirements.

Financial institutions can only respond to incidents if they are aware they have occurred. Effective testing and measurement of response processes require consistent incident reporting, evaluation of solution efficiency, and thorough analysis of results. The requirement to test is key under DORA, and it is important to have a robust process in place to ensure that cooperation with regulators, supervisory authorities and affected parties is as effective as possible. A robust incident response process will assist in minimising and mitigating the fallout of the attack and put best foot forward for improving processes to prevent future attacks.

This is also useful to consider in the context of the 'information sharing' requirement which forms Concept 5 of the DORA requirements. Through the standardisation of templates and format of reporting, it simplifies the process that regulators and reporting bodies will undertake to consider the wider impact of frequency and type of attacks which plague the cyber industries, and allow them to assess the criticality of the issue industry-wide.

Article	Requirement	Darktrace Features
18	Financial institutions are required to classify the impact of incidents appropriately. This includes specifying key properties such as: ▪ Duration of the attack ▪ Systems and data which have ben affected ▪ Scope of data loss ▪ Geographical impact (i.e. global or jurisdiction-specific) ▪ Criticality of services (i.e. are they part of an important or a critical function?) ▪ Economic impact	Darktrace can assist with some of the hardest aspects of this type of reporting, and make the process more streamlined and faster to undertake. Darktrace's visibility and forensic capability through detailed log creation and PCAP retrieval can inform many of the required questions which customers can then use to structure their reporting. Darktrace's Cyber AI Analyst can provide powerful assistance in determining the scope of an incident, its root cause and time of origin.
19	Financial entities are required to report major ICT-related incidents to the applicable supervisory authority in a manner similar to that under GDPR. There are prescriptive requirements for the format of this notification which are covered in Article 20. More information is expected on what these templates will look like in due course.	Darktrace / Incident Readiness & Recovery can assist with this process through the preparation of incident reports, which can be used to simplify the reporting process. The incident report documents the specifics surrounding the events of an incident from the point at which the incident began, how it was contained, and the recovery steps which were taken. This information can then be taken and used to populate whichever template a notification must be provided in.

3. Operational Resilience Testing

Key Articles: Chapter IV contains details of the Operational Resilience Testing Requirements.

Waiting for an incident to occur is not an effective way to approach cyber-readiness strategy. Operational resilience testing must form part of an effective disaster recovery and business continuity plan to ensure that financial institutions understand what their capabilities and limitations are in the event of a crisis. It is, after all, too late when the crisis occurs. Testing should occur on a regular basis, and good practice would be for tests to be undertaken at each material change in the infrastructure and following the implementation of recovery-measures in the unfortunate event that a financial institution has fallen victim to an attack..

Article	Requirement	Darktrace Features
24	Financial institutions are required to implement and maintain a digital operational resilience testing program which identifies weaknesses, deficiencies and gaps in their operational resilience, applying a range of assessments, tests, methodologies, practices and tools.	Darktrace / Incident Readiness & Recovery's simulations provide an intuitive and flexible way to leverage actual historical incidents mapped against an organisations assets in order to conduct realistic testing of resilience processes.
25	The range of assessments, tests, methodologies, practices and tools which are mandated under Article 24, are specified here. These tests include: ▪ 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	Darktrace / Proactive Exposure Management and Darktrace / Attack Surface Management conduct continual assessment and analysis of an organizations assets and network configuration in order to identify and prioritize risk factors. They can, therefore, be a useful tool in any CISO's arsenal.

4. Third-Party Risk Management

Key Articles: Chapter V contains details of third-party risk management requirements. Article 30 sets out the mandatory contracting requirements.

It is inevitable that financial entities will use third party providers to provide some aspects of the services required to build a strong, resilient digital estate. However, there is an onus on financial institutions to ensure that they are using responsible third-party providers. These providers should be able to meet the security criteria which are set out under DORA and ensure that there are suitable, realistic contractual provisions in place which properly reflect the transactions that are being undertaken and the oversight and liability measures which are in place.

It is unlikely that a single solution will fit the entirety of an organizations needs. Thus, it is important for financial institutions to approach providers with flexibility in mind and do not attempt to shoe-horn sophisticated, nuanced ICT-service delivery into clunky standard terms and conditions. Conversely, it is important for ICT-providers to ensure that they are working with financial institutions to ensure that reasonable needs and requirements are met in their contractual provisions.

Darktrace is an industry-recognised leader in cybersecurity and has experience in deploying effective solutions to customers of all sizes, across all industries, worldwide. Our Master Services Agreement is tailored to Darktrace's products and services and so accurately reflects the manner in which any cybersecurity services which Darktrace may provide are delivered to financial services customers. We also have gone to great lengths to review our existing terms and conditions to put in place an additional set of DORA-specific terms to address any gaps in our existing contractual frameworks. This should provide our financial institution customers with comfort that we are keen to ensure that they are compliant with the mandatory contracting requirements under Article 30.

5. Information Sharing

Key Articles: Chapter VI contains details of procedure that must be followed for information-sharing.

Information sharing is a crucial component in preventing malicious third-parties from gaining access to financial institutions' data, and therefore it is promising that financial institutions are encouraged to information share. The benefits of such exercises are that a clear picture of types and frequency of attacks, but also useful tools, processes, techniques and reliable third party providers which have been significantly useful in building one financial institution's strategy. This will, inevitably, increase the resilience of the financial services industry as a whole. If financial institutions wish to opt in, or out, the applicable competent authorities should be notified.

Consequences

The consequences for failing to comply with the requirements of DORA are severe. We have seen significant penalty possibilities under the General Data Protection Regulation of the European Union ("GDPR"), and DORA is no different. GDPR's penalties are fixed at the higher of up to 4% of worldwide turnover, or EUR 20million.

Under DORA, a similar model has been adopted – financial institutions can face penalties of up to 2% of worldwide turnover, or EUR 10million, whichever is higher. Penalties for individuals can be as high as EUR 1million.

Additionally, affected third parties are also captured within its scope. Non-compliant third parties can be fined up to 1% of their average daily global turnover for each day of non-compliance for up to a maximum period of 6 months or EUR 5million.Individuals in this context can face a financial penalty of up to EUR 500,000.

It is also worth considering the wider impact of non-compliance. Financial institutions and their providers should consider whether there could be an impact on any regulated status and the resulting effect on their ability to continue trading in the region, as well as the implications on reputation. It may also be the case that the applicable supervisory authority determines that the contract must be cancelled.

It is highly likely that financial institutions will be required to comply with both DORA and the GDPR due to overlaps in stringent security requirements, so it would not be unrealistic to assume that a breach of both could occur if DORA measures were not adhered. In that circumstance, the impact of fines and penalties could be catastrophic.

Practical next steps

To discuss more about how Darktrace can bolster your current cybersecurity strategy within the context of DORA book a demonstration of our products here.

■ **About Darktrace**

Darktrace is a global leader in AI cybersecurity that keeps organizations ahead of the changing threat landscape every day. Founded in 2013 in Cambridge, UK, Darktrace provides the essential cybersecurity platform to protect organizations from unknown threats using AI that learns from each business in real-time. Darktrace's platform and services are supported by 2,700+ employees who protect nearly 10,000 customers globally. To learn more, visit http://www.darktrace.com.

North America: +1 (415) 229 9100   Europe: +44 (0) 1223 394 100   Asia-Pacific: +65 6804 5010   Latin America: +55 11 4949 7696

darktrace.com | info@darktrace.com