

AN EU-WIDE STANDARD FOR PENTESTING

***Digital Operational Resilience Act
(DORA)***

SECURA

Vestdijk 59
5611 CA Eindhoven
Netherlands

Karspeldreef 8
1101 CJ Amsterdam
Netherlands

T +31 (0)88 888 3100
E info@secura.com
W secura.com

Follow us on   



*In September 2020, the European Commission released a new draft framework “**Digital Operational Resilience Act**” (DORA) for ICT risk management that will apply to financial institutions within Europe. The goal of this framework is to create a harmonized risk management tool for improving cybersecurity and resilience. The DORA covers the entire financial sector across both small and large enterprises. The final version is expected to come fully into effect by the end of 2022 depending on feedback received from market stakeholders.*

1. Goals of this Framework

The DORA framework aims to establish standards for organizations to increase the overall cybersecurity posture of financial institutions across the EU. The framework can be broken down into **four main points**, namely:

1. Financial entities are required to follow cybersecurity practices related to data security and protection. Organizations are required **to limit access to ICT systems and data, develop secure methods to transfer information, implement strong authentication mechanisms, and design network connection infrastructure in such a way to limit downtime**. The regulation allows some flexibility on the specific protocols and processes used to achieve its general goals in this regard.
2. Entities are required **to establish business continuity and disaster recovery plans** which would need be tested at least annually and after any substantive change to respective ICT systems. The legislation does not foresee strict recovery objectives, but takes a flexible approach allowing financial institutions to determine their objectives as they see fit.
3. The draft requires that **firms develop a policy that specifies data backup and recovery methodologies**. Financial entities would have to create and maintain redundant ICT systems to ensure the availability and integrity of data. The proposal also includes specific requirements to ensure that third party ICT providers maintain more than one data processing sites, and requirements that CPPs can efficiently recover transactions from a disruption.
4. The proposal requires **institutions to map potential risks and perform root-cause analysis on ICT-related incidents**. This includes a yearly risk assessment of legacy ICT systems. It also mandates a communication strategy which **requires responsible disclosure of ICT incidents to clients, stakeholder, and the public, if appropriate**.

2. Harmonization of Penetration Testing across the European Union

The DORA builds on current legislation surrounding penetration testing to create a more standardized framework. Many financial market infrastructures (FMIs) are already required by law to perform testing in accordance with **Threat-Led Penetration Testing Frameworks (TLPT)**. The DORA builds upon this base by increasing the number of institutions that are required to undergo testing by third-party penetration testers.

The DORA also attempts to harmonize cross-border penetration testing. It creates standardization across EU-nation states so that penetration testing will only have to be performed once per target regardless of country. It accomplishes this by expanding on the current TIBER-EU framework, and allows for a standardized methodology.

European Supervisory Authorities (ESAs) are asked to develop criteria for penetration test recognition across member states. The goal of this is to create recognition of penetration tests across the European Union in order to reduce complexity and duplication.

Does DORA apply to me?

The DORA attempts to cover the broad financial sector, hence firms listed below are expected to be included:

- Banks
- Credit Unions
- Fintechs
- Clearing Houses
- Stock Exchanges
- Third-party service providers to financial institutions (cloud service providers, MSPs, etc)
- Investment Firms
- Credit Rating Agencies
- Insurance Firms



3. Stringent Requirements on Outsourcing IT Functions

The proposal incorporates numerous elements from the ESAs guidelines on outsourcing relating for example to diligence, information security and exit strategies. This includes various elements that must be included when contracting third party ICT services such as access, audit and termination rights. To highlight: **the draft legislation includes a requirement to maintain a register of information on contractual agreements with ICT third-party service providers and a requirement to perform pre-contractual analyses.**

These analyses need to explicitly include an **assessment of concentration risks and the substitutability of the provider.** When contracting with a provider based in a third-country, financial entities will be required to consider issues relating to data protection, law enforcement and insolvency law. This might have substantial impact when outsourcing to China, India, Vietnam, and the Philippines, for example.

The main objective of the expanded scope is to **prevent supply chain attacks.** These attack vectors are an increasingly common method to compromise an organization. A recent example can be drawn from The Reserve Bank of New Zealand, New Zealand's Central Bank.

The New Zealand's Central Bank used a third-party file-transfer application namely Accellion to share sensitive information with external stakeholders. An attack on Accellion lead to the disclosure of the documents that were shared on the file transfer application which included both personal and commercial information.¹ Such events are to be prevented.



¹ <https://www.rbnz.govt.nz/our-response-to-data-breach>



Therefore, the use of Critical Third-party ICTP

Providers (so-called CTPPs) will be regulated. European Supervisory Authorities (ESAs) of each member state would be designated as Lead Overseers for each critical third-party ICT provider. They will give recommendations to CTPPs particularly upon security, contractual terms, and sub-outsourcing. These recommendations will then be monitored and enforced by national authorities. The lead overseer would be able to impose penalties on CTPPs particularly in order to compel compliance with their investigations; penalties would amount to 1% of their average daily global turnover on a daily basis. Additionally, Article 28.9 notably states that financial entities shall not make use of an ICT third-party service provider established in a third country if that provider would be designated as critical if it was established in the EU.

Clarification surrounding Incident Reporting

The DORA attempts to standardize incident reporting requirements and to clarify the types of incidents that are required to be reported. Financial firms have been increasingly under attack and the conflicting and differing rules for reporting can often hinder the incidence response process. The DORA clarifies these rules by creating a common reporting template that can be followed for incident reporting. The DORA does not aim to replace or override current incident reporting standards such those linked to the GDPR.

Timeline

The DORA is currently in the proposal phase within EU law. **The decision to implement the act into law is estimated to be made around the end of 2021.** Once adopted, it will apply to all EU member states after twelve months except for Article 23 (Advanced testing of ICT tools, systems and processes based on threat led penetration testing) and Article 24 (Requirements for testers), which will only come into force 24 and 36 months after resolution. Potentially, this indicates that companies may have to be compliant by the end of 2022, however legislation has not been finalized. Additionally, it is quite plausible that the DORA will grow and apply to other critical sectors with time.

4 Becoming Compliant – with Secura’s Support

Diving into the regulation and preparing for compliancy with DORA should be in your 2021 goals. For larger firms with substantial audit and compliancy teams, it is worthwhile to start investigating this regulation now to ensure that the required process steps can be embedded into existing process flows. Especially for supply chain security, this can prove to be a huge benefit to ensure the right agreement with vendors is in place.

For smaller firms this can be a more daunting task. A first deep dive in cyber security and often process documentation is worthwhile to start this process. By doing so, it is possible to make a gap analysis which can determine weak spots within the organization and where to increase the organization's overall security posture.

Secura provides security advice, testing, training, and certification services for our customers. This covers all aspects such as people, policies, processes, and technology. This goes beyond Internal Penetration Tests, which are the mandatory part of the DORA framework.

Additionally, **Secura is one of the parties to perform TIBER Red Teaming exercises in the financial sector according to the scheme devised by the Dutch Central Bank and now rolled out across Europe in the TIBER-EU scheme.** In addition to supporting firms to reach compliance, our services provide insight into security. This is our ultimate goal to support you to make the right decisions for your risk appetite.

Common DORA Abbreviations




- **CTTP** - Critical third-party ICT providers
- **DORA** - Digital Operational Resilience Act
- **ESA** - European Supervisory Authorities
- **FMI** - Financial market infrastructures
- **TLTP** - Threat-led penetration testing frameworks.

About Secura

Secura is your independent cybersecurity expert. Secura provides insights to protect valuable assets and data. We make cybersecurity tangible and measurable in the field of IT, OT and IoT. With security advice, testing, training and certification services, Secura approaches cybersecurity holistically and covers all aspects from people, policies, organizational processes to networks, systems, applications and data.

For more information, please visit: secura.com.

Keep updated with the latest insights on digital security and subscribe to our periodical newsletter: www.secura.com/subscribe.

Follow us on   

Contact us today at
info@secura.com or
visit secura.com for
more information.

SUBSCRIBE

TO OUR NEWSLETTER

