REGULATION DORA

A complete Guide to **compliance for the financial sector**

yogosha

TABLE OF CONTENTS

TABLE OF CONTENTS

DORA: A COMPLETE GUIDE TO COMPLIANCE FOR THE FINANCIAL SECTOR

Looking for a practical guide to DORA compliance? Here's a 17-point checklist to get you ready for the Digital Operational Resilience Act, the EU's core regulation for digital finance.

This article is primarily intended for Chief Information Security Officers (CISOs), but may be useful for Data Protection Officers (DPOs) and legal departments. It is the outcome of a personal work based on the final text of DORA, which will be regularly quoted as source.

Nevertheless, as exhaustive as they aim to be, these few pages cannot substitute for the necessary diligence of each and every one regarding compliance, nor for the expertise of any legal expert. It is therefore up to each individual to ensure proper compliance, and this article shouldn't be taken as anything more than what it is: a humble guide, written with caution and rigor. Anyway, no more disclaimer, and let's get to the heart of the matter.

WHAT IS THE DORA REGULATION?

The DORA Regulation (No. 2022/2554), or Digital Operational Resilience Act, is **a major piece of European Union legislation on cybersecurity for financial entities**, such as banks or credit institutions.

Which law prevails between DORA and NIS2?

If you're aware of the DORA Regulation, you couldn't miss the NIS2 Directive. It was adopted on the same day, and strengthens cybersecurity requirements across the EU, including for banks and financial market infrastructures.

So, which prevails between DORA and NIS2 when it comes to digital finance? Well, it's simple: **DORA is «lex specialis» of NIS2, a principle which states that a specific law takes precedence over a general one.** In reality, DORA clarifies and complements NIS2 more than it supplants it.

> "This Regulation constitutes lex specialis with regard to Directive (EU) 2022/2555. At the same time, it is crucial to maintain a strong relationship between the financial sector and the Union horizontal cybersecurity framework as currently laid out in Directive (EU) 2022/2555" –
>
> DORA, Recital 16

Read also: NIS2 Directive, our Step-by-Step Guide to Compliance

WHAT IS THE PURPOSE OF DORA?

DORA's objective is clearly stated in its Recital 105 (a preamble that precedes a piece of legislation and explains its motivations): **«to achieve a high level of digital operational resilience for regulated financial entities".**

That's all well and good, but what does «digital operational resilience» mean? Well according to the text of DORA itself, it is:

> "**the ability of a financial entity to build, assure and review its operational integrity and reliability** by ensuring, either directly or indirectly through the use of services provided by ICT third-party service providers, the full range of ICT-related capabilities needed to address the security of the network and information systems which a financial entity uses, and which support the continued provision of financial services and their quality, **including throughout disruptions" – DORA**, Article 3(1)

Defense is good, resilience is better!

What does this definition of digital operational resilience mean? Quite simply, **financial entities must no longer just defend themselves, they must resist.** The real challenge of DORA is the reliability and integrity of financial services, even in case of disruptions, incidents, attacks... In other words, if something goes wrong! The financial sector should be able to defend its assets (data, software and hardware), but it is no longer an end in itself. With DORA, defense serves a higher purpose: resilience.

WHEN WILL THE DORA REGULATION COME INTO FORCE?

The DORA Regulation will come into force on the 17th of January 2025, i.e. 24 months after its publication in the Official Journal of the EU. Should you want to check for yourself, the date is clearly stated in Article 64.

Towards a clarification of regulatory technical standards by ESAs and ENISA in early 2024

As you will see, some of the policies and procedures introduced by DORA are, to date, still a bit nebulous. Nevertheless, this should become clearer by early 2024.

Article 15 states that the European Supervisory Authorities (ESAs) and the European Union Agency for Cybersecurity (ENISA) must propose common draft regulatory technical standards by January 17, 2024. These drafts will specify different parts of the legislation, from the components of the ICT response and recovery plans to the testing of ICT business continuity plans.

However, the regulation is already quite extensive and there's no need to wait until 2024. There's no shortage of challenging projects and it's best to get started as soon as possible.

SANCTIONS UNDER THE DIGITAL OPERATIONAL RESILIENCE ACT

If we stick to the final texts, DORA is much less coercive than NIS2. Where NIS2 gives quantified administrative fines, DORA prefers to leave the assessment of the sanction to the Member States and their competent authorities.

Note that this does not mean that there are no sanctions! Article 50(4) of DORA clearly states that the competent authorities may **«adopt any type of measure, including of pecuniary nature,** to ensure that financial entities continue to comply with legal requirements.» These same authorities are also entitled to make public statements indicating the nature of the violation and the identity of the person (natural or legal) responsible.

DORA COMPLIANCE: A 17-STEP ACTION PLAN

At this point, we've already covered the «when» and «why» of DORA compliance. But as you might expect, it's the «how» that represents the bulk of the work. As always with compliance matters, it's all about taking it one step at a time. These few pages are here to help you get started.

Without further ado, let's get down to business with our action plan to prepare DORA as well as possible before January 17, 2025.

01 KNOW IF YOU ARE AFFECTED BY THE DORA REGULATION

Before worrying about DORA compliance, you should know if you're affected. The Digital Operational Resilience Act applies to **21 types of entities**. Here they are as described in Article 2:

- **credit institutions;**
- **payment institutions**, including payment institutions exempted pursuant to Directive (EU) 2015/2366;
- **account information service providers**;
- **electronic money institutions**, including electronic money institutions exempted pursuant to Directive 2009/110/EC;
- **investment firms**;
- **crypto-asset service providers** and issuers of asset-referenced tokens;
- **central securities depositories**;
- **central counterparties**;
- **trading venue**s;
- **trade repositories**;
- **managers of alternative investment funds**;
- **management companie**s;
- **data reporting service providers**;
- **insurance and reinsurance undertakings**;
- i**nsurance intermediarie**s, reinsurance intermediaries and ancillary insurance intermediaries;
- **institutions for occupational retirement provision**;
- **credit rating agencies**;
- **administrators of critical benchmark**s;
- **crowdfunding service providers**;
- **securitisation repositories**;
- **ICT third-party service providers.** (Yes, it's broad.)

DORA: THE LIST OF EXCEPTIONS

Certain entities are explicitly excluded from the scope of DORA by Article 2(3). We encourage you to read the list below to see if you are among the lucky ones.

A word of caution: the exceptions mentioned in DORA often echo exceptions in other legislations, which themselves have countless ramifications. In order to keep it short, we won't go into the details of all the legislations mentioned by DORA. Nevertheless, you will find links to the laws in question if you need to know more about a particular sector.

Are excluded from the scope of DORA:

- **managers of alternative investment funds** as referred to in Article 3(2) of Directive 2011/61/EU;
- **insurance and reinsurance undertakings as referred to** in Article 4 of Directive 2009/138/EC;
- **institutions for occupational retirement provision which operate pension schemes which together do not have more than 15 members in total;**
- **natural or legal persons exempted pursuant to Articles 2 and 3** of Directive 2014/65/EU;
- **insurance intermediaries, reinsurance intermediaries and ancillary insurance intermediaries** which are microenterprises or small or medium-sized enterprises The definition is given in Article 4(60) of DORA: which employs fewer than 10 persons and has an annual turnover and/or annual balance sheet total that does not exceed 2 million euros;
- **post office giro institutions** as referred to in Article 2(5), point (3), of Directive 2013/36/EU.

It should be noted that Member States may choose to exclude from the scope of DORA some very specific national credit or investment entities, as referred to in Article 2(5) of Directive 2013/36/EU. In France, for example, the State could choose to spare the "Caisse des dépôts et consignations".

02 KNOW THE REQUIREMENTS SET BY DORA

As previously seen, the goal of DORA is to elevate the digital operational resilience of financial organizations. To achieve this, Article 1 sets specific requirements for the security of network and information systems, namely:

- requirements applicable to financial entities in relation to:
  - **information and communication technology (ICT) risk management;**
  - **reporting of major ICT-related incidents to the competent authorities** and notifying, on a voluntary basis, of significant cyber threats;
  - **reporting of major operational or security payment-related incidents** to the competent authorities;
  - **digital operational resilience testing;**
  - **information and intelligence sharing** in relation to cyber threats and vulnerabilities;
  - measures for the sound **management of ICT third-party risk;**
- requirements in relation to the contractual arrangements concluded between ICT third-party service providers and financial entities;

As you might expect, these requirements are the focus of the rest of this article.

03 CREATE AN ICT RISK MANAGEMENT FRAMEWORK

This is a BIG piece of the legislation. The Digital Operational Resilience Act highlights the absolute necessity of having an ICT risk management framework.

> "Financial entities shall have **a sound, comprehensive and well-documented ICT risk management framework** as part of their overall risk management system, which enables them to address ICT risk quickly, efficiently and comprehensively and to ensure a high level of digital operational resilience."
>
> DORA, Article 6(1)

For information, **is defined as an ICT risk:**

> "Any reasonably identifiable circumstance in relation to the use of network and information systems which, if materialised, may compromise the security of the network and information systems, of any technology dependent tool or process, of operations and processes, or of the provision of services by producing adverse effects in the digital or physical environment;"
>
> DORA, Article 3(5)

DORA: PROTECTING SOFTWARE, HARDWARE AND DATA

The framework must detail the elements put in place to protect the organization's ICT and information assets. Again, let's refer to Article 3 for definitions:

- **"information asset":** a collection of information, either tangible or intangible, that is worth protecting;
- **"ICT asset":** a software or hardware asset in the network and information systems used by the financial entity;

In other words, financial sector players must protect not only their software and physical equipment (servers, endpoints, etc.), but also the data. This is a logical and welcome legislative shift. After all, attacking a data center is never an end in itself: the true goal is the access to the data.

When we will talk about assets in the rest of this article, it is to be understood as «information assets» and «ICT assets» according to the previous definitions.

WHAT MUST YOU INCLUDE IN THE ICT RISK MANAGEMENT FRAMEWORK?

Still under Article 6, **the mandatory ICT risk management framework must include at least:**

- the strategies, policies, procedures, ICT protocols and tools that are necessary to protect:
    - **all information and ICT assets**, including softwares, hardware, servers, etc.;
    - **all physical components and infrastructures** relevant to the protection of these assets, such as premises or data centers.

As you will soon realize, DORA operates like a Russian doll of policies. This risk management framework will itself be fueled by the creation of other policies specific to different topics, from business continuity to recovery plans.

It should be noted that organizations must keep this documentation available to the relevant authorities, who may request access to it. They can also request a report on the review of the framework, which brings us to the next point.

UPDATE THE FRAMEWORK AT LEAST ONCE A YEAR

No way to write the framework and then let it gather dust in corners. It needs to be updated:

- **at least once a year** (or periodically for microenterprises);
- or upon the occurrence of major ICT-related incidents;
- or following supervisory instructions;
- or conclusions derived from relevant digital operational resilience testing or audit processes.

IMPLEMENT AN ISMS WITH DORA IN MIND

If you have not already done so, it is essential to implement an ISMS to support the risk management framework introduced by DORA. Having an Information Security Management System (ISMS) helps to reduce digital risks, by structuring the entity's information security management through a systemic approach.

ISO 27001, A STANDARD FOR CERTIFICATION

NIS2 suggests future European certification frameworks for cybersecurity. But until then, the international standard ISO 27001 remains a reference for the creation of an ISMS. Achieving ISO 27001 certification requires hard work, organization and most of all, time. Therefore, it should be one of the priorities of any CISO dealing with DORA.

A SIMPLIFIED ICT RISK MANAGEMENT FRAMEWORK FOR DESIGNATED ENTITIES

Some entities are entitled to a «simplified ICT risk management framework» pursuant to Article 16 of DORA. This is a lighter version of the mandatory management framework required by the Regulation.

Here is the list of entities that qualify for this simplified framework:

- small and non-interconnected investment firms;
- payment institutions exempted pursuant to Directive (EU) 2015/2366;
- institutions exempted pursuant to Directive 2013/36/EU – see our section on DORA's scope exceptions;
- electronic money institutions exempted pursuant to **Directive 2009/110/EC**;
- and small institutions for occupational retirement provision – those operating pension schemes with fewer than 100 members in total.

04 AUDIT THE ICT RISK MANAGEMENT FRAMEWORK ON A REGULAR BASIS

The ICT risk management framework «shall be subject to internal audit by auditors on a regular basis» (Article 6.6). There should be a clear segregation between ICT risk management functions, control functions, and internal audit functions To this end, Article 6(4) of DORA directs financial entities to adopt the Three Lines of Defense (3LoD) model.

ADOPT THE THREE LINES OF DEFENSE (3LOD) MODEL

The 3LoD model allows for an organizational separation of responsibilities and risk governance. In practice:

- **A first line of defense by the operational teams, those who are on the ground.** They are responsible for simplifying risk management for the next lines, by taking into account the risk factors. For instance, for a development team, this may involve clearly defining the responsibilities of each person, or adopting a culture of cybersecurity by design with secure development methods.

- **A second line of defense by the risk management and compliance functions**, such as the CISO. This second line is responsible for controlling the first. This involves creating monitoring processes, implementing the entity's overall risk management strategy, or ensuring that all the company's functions are working in accordance with risk management policies – so HR, sales, marketing, C-Levels, everyone!

- **A third line of defense by independent internal auditors**. They must ensure that the defenses put in place by the previous two lines are bulletproof. In other words: a holistic control of the risk management application. The auditors must verify the processes and their correct execution, and then write detailed audit reports. DORA states the obvious, but internal auditors must have «sufficient knowledge, skills and expertise» in ICT risk management.

For the 3LoD model to succeed, **each line must be completely independent** – especially the last. As such, DORA states that organizations must ensure «adequate separation and independence of ICT risk management functions, control functions and internal audit functions» to avoid conflicts of interest. It's time to revisit Montesquieu and the separation of powers!

It's difficult to detail a universal 3LoD model that can be replicated everywhere, since it must be intrinsically tied to the business, the structure and the functions of each organization. However, you'll find many resources on the web to guide you in the implementation of your fortifications. The latest model from the **IIA (Institute of Internal Auditors)** is a good starting point.

ENTITY RESPONSIBILITY EVEN WHEN OUTSOURCING

The DORA allows for the outsourcing of «the tasks of verifying compliance with ICT risk management requirements», whether to external or internal actors. However, the financial entity remains fully responsible for this verification. Simply put: don't expect to pass the buck for negligence to a vendor, the liability lies with the financial entities.

05 DEFINE A «DIGITAL OPERATIONAL RESILIENCE STRATEGY»

The ICT risk management framework must come with a digital operational resilience strategy. These are two sides of the same coin: where the risk management framework has a holistic approach, the resilience strategy has a practical approach. It should specify the methods put in place to address risks and attain specific objectives.

According to Article 6(8), this resilience strategy must:

- **explain how the framework supports the financial entity's business strategy and objectives**;
- **establish the risk tolerance level for ICT risk**, in accordance with the risk appetite of the financial entity, and by analyzing the impact tolerance for ICT disruptions;
- **set out clear information security objectives**, including key performance indicators and key risk metrics;
- **explain the ICT reference architecture** and any changes needed to reach specific business objectives;
- **outline the different mechanisms put in place to detect ICT-related incidents**, prevent their impact and provide protection from it;
- **evidence the current digital operational resilience situation** on the basis of the number of major ICT-related incidents reported and the effectiveness of preventive measures;
- **implement digital operational resilience testing**;
- **and outline a communication strategy for ICT-related incidents** that require disclosure.

Depending on the scale of the group, it's fully possible to set up a global multi-vendor strategy. The strategy should then explain the rationale behind this choice, and detail the key dependencies on different suppliers.

MONITOR AND IMPROVE THE EFFECTIVENESS OF THE STRATEGY OVER TIME

Article 13 calls on financial entities to monitor the effectiveness of the implementation of their digital operational resilience strategy. This includes mapping the evolution of ICT risk over time, and analyzing the frequency, types, magnitude and evolution of incidents. Emphasis is placed on the follow-up of cyber attacks and their patterns, in order to understand the evolution of the entity's risk exposure level, especially for critical or important functions.

The strategy should be continuously improved by lessons learned from:

- **mandatory reviews after a major incident** – see #11;
- **difficulties encountered in activating business continuity plans** and response and recovery plans – see #8 and #9;
- **surveillance of cyber threats** and information-sharing arrangements – see #13;
- **operational resilience tests** – see #14 and #15.

A report must be made to the management body of the entity at least once a year (Article 13.5). It should include the findings of the previous points, as well as recommendations.

06 DEPLOY MECHANISMS FOR ASSET PROTECTION AND RESILIENCE

The resilience strategy should «outline the different mechanisms put in place to detect ICT-related incidents, prevent their impact and provide protection from it.» There is no secret here, you will need to rely on a range of appropriate procedures and tools.

MINIMUM PROTECTION AND RESILIENCE REQUIREMENTS

To protect assets in line with Article 9, the solutions and processes in place must at least:

- **ensure the security** of the means of transfer of data;
- **minimize the risk** of corruption or loss of data, unauthorized access and technical flaws that may hinder business activity;
- **prevent the lack of availability**, the impairment of the authenticity and integrity, the breaches of confidentiality and the loss of data;
- **ensure that data is protected** from risks arising from data management, including poor administration, processing-related risks and human error.
- **ensure sound network and infrastructure management**, that may include automated mechanisms to isolate affected information assets in the event of cyberattacks;

To prevent contagion, **the network connection infrastructure** must be designed in a way that allows it to be instantaneously severed or segmented, especially for interconnected financial processes. In other words, everything has to be able to be disconnected on the fly if something goes south.

MORE AND MORE POLICIES TO DOCUMENT

Financial entities must also document:

- **an information security policy** defining rules to protect the availability, authenticity, integrity and confidentiality of assets and data, including those of their customers, where applicable;

- **policies that restrict access (physical or logical) to assets and data** based on functions, roles and missions;

- **policies and protocols for strong authentication mechanisms** and encryption key protection measures. There are many paths forward, starting with the adoption of 2FA as the default authentication method for all employees;

- **policies, procedures and controls for ICT change management**, including changes to software, hardware, firmware components, systems or security parameters. They should be based on a risk assessment approach and be an integral part of the financial entity's overall change management process. The ICT change management process must be approved by the proper hierarchical body;

- **appropriate and comprehensive documented policies for patches and updates.**

07 INSTALL DETECTION SOLUTIONS

Proper asset protection requires proper detection capabilities for anomalies, incidents and cyber attacks. This means EDRs, XDRs, scanners, SIEMs, etc. Article 10 of DORA specifies that financial entities must allocate «sufficient resources and capabilities».

To meet the requirements of the Regulation, **the detection mechanisms must:**

- enable multiple layers of control, define alert thresholds and criteria to trigger and initiate incident response processes, including automatic alert mechanisms for relevant staff (the SOC for example);

- and be tested regularly.

We recommend you to read **our article about EDR solutions** as well as the one on **SIGMA rules**, a collaborative tool that allows to standardize detections whatever the SIEM. Useful if you decide to migrate to another solution in the context of DORA.

08 DRAFT AN ICT BUSINESS CONTINUITY POLICY

THE DORA REGULATION REQUIRES THAT:

"**Financial entities shall put in place a comprehensive ICT business continuity policy,** which may be adopted as a dedicated specific policy, forming an integral part of the overall business continuity policy."

– **DORA, Article 11**

This ICT business continuity policy must allow for:

1. **the continuity** of the financial entity's critical or important functions;

2. **a quick and effective response** to all ICT-related incidents in a way that limits damage and prioritizes the resumption of activities and recovery actions;

3. the activation of dedicated plans to **contain each type of incident and prevent** further damage, as well as tailored response and recovery procedures – cf. #9;

4. **the estimation of preliminary impacts**, damages and losses;

5. **proper crisis management and communication measures** for internal teams, external stakeholders and relevant authorities – cf. #10.

Again, it's critical to prevent, contain and remediate, but most of all to ensure the resilience of services.

Test continuity plans at least once a year

Once again, DORA's text is very down to earth. Measures must be documented, but also tested for effectiveness. Article 11(6) requires financial organizations to test :

- ICT business continuity plans and ICT response and recovery plans :
  - **at least once a year;**
  - as well as when there are substantial changes to ICT systems that support critical or important functions.

- as well as crisis communication plans.

Testing plans must incorporate cyberattacks and switchover scenarios between the primary ICT infrastructure and the redundant capacity, backups and redundant facilities enforced by DORA.

Keep a record of activities in the event of a disruption

Should these plans be activated, entities must keep “readily accessible records of activities before and during disruption events» as per Article 11. If requested by the competent authorities, organizations must also provide an estimate of the aggregate annual costs and losses incurred by major incidents.

09 PROVIDE BACKUP, RESTORATION AND RECOVERY PROCEDURES (AND RELATED POLICIES)

The Digital Operational Resilience Act seeks to minimize disruption and downtime to systems and data. Concretely, this translates into three work streams: **backup, restoration and recovery**. These are broken down into policies, which are themselves part of the ICT business continuity policy.

FINANCIAL ENTITIES MUST THEREFORE PUT IN PLACE:

- **backup policies and procedures** that specify:
  - the scope of the data covered by the backup;
  - and its minimum frequency, depending on the criticality of the information or the confidentiality level of the data;

- **restoration and recovery procedures and methods.**

Activating a backup system must not compromise the availability, authenticity, integrity or confidentiality of the data. This means no freezing of services while rolling back the system. Furthermore, DORA (Art. 12.4) introduces an obligation of redundant ICT capacities. They must be duplicated in order to ensure a relay if the original system should fail.

Regarding restoration, if an entity decides to restore backup data using its own systems, it must ensure that they are physically and logically segregated from the source system.

Finally, **all backup, restoration and recovery procedures must be tested periodically** pursuant to Article 12(2).

It should be noted that most of these requirements do not apply to micro-enterprises, or may be assessed according to their risk profile. On the other hand, central securities depositories are subject to additional requirements, such as having a secondary data processing site. If necessary, everything is outlined in Article 12(5).

10 PREPARE CRISIS COMMUNICATION PLANS

Article 14 of DORA is short but to the point. It clarifies the obligations of financial entities regarding communication during incidents.

«Financial entities shall have in place crisis communication plans enabling a responsible disclosure of, at least, major ICT-related incidents or vulnerabilities to clients and counterparts as well as to the public, as appropriate.»

– **DORA, Article 14(1)**

In addition to these externally-focused communication plans, organizations should have similar plans for internal use and external stakeholders. In the event of an incident, the internal communication policy should distinguish between:

- staff who need to be informed;
- and staff who are actively involved in ICT risk management, especially with respect to response and recovery.

DESIGNATE A CRISIS COMMUNICATIONS OFFICER

DORA requires that at least one person be designated as responsible for this matter. It may be wise to sync up with the legal, comm and marketing teams on the posture to be taken, and the processes to be implemented.

«At least one person in the financial entity shall be tasked with implementing the communication strategy for ICT-related incidents and fulfill the public and media function for that purpose.»

– **DORA, Article 14(3)**

The communication plan brings us right to the next point, as it must be part of the incident management process.

11 ESTABLISH AN INCIDENT MANAGEMENT PROCESS

With DORA, it is mandatory for financial entities to implement an incident management process - ICT related of course, which is meant throughout this paper. This incident management process feeds into the ICT business continuity policy (see #8) and the resilience strategy (#5), which are themselves part of the ICT risk management framework (#3). When we told you that DORA was organized like a matryoshka of policies...

DORA: AN OBLIGATION TO RECORD ALL INCIDENTS

This process is not an end in itself: it must **record all significant cyber threats and all incidents** (not just the most important ones). It goes without saying that recording all incidents is impossible without a flawless detection capability – see #6 of this article.

Pursuant to Article 17, the incident management process shall:

- put in place **early warning indicators;**
- establish procedures to **identify, track, log, categorize and classify incidents** according to their priority and severity, and according to the criticality of the services impacted;
- **assign roles and responsibilities** that need to be activated for different incident types and scenarios;
- **set out plans for communication** to staff, external stakeholders and media;
- ensure that at least **major incidents are reported to relevant senior management**, and inform the management body of at least major incidents, explaining the impact, response and additional controls to be established;
- **establish incident response procedures** to mitigate impacts and ensure that services become operational and secure in a timely manner.

CLASSIFICATION OF INCIDENTS UNDER DORA

According to Article 18 of DORA, financial entities must classify incidents based on the following criteria:

1. **the number and/or relevance of clients or financial counterparts affected** and, where applicable, the amount or number of transactions affected by the incident, and whether it has caused reputational impact;

2. **the duration of the incident**, including the service downtime;

3. **the geographical spread** with regard to the areas affected by the incident, particularly if it affects more than two Member States;

4. **the data losses that the incident entails**, in relation to availability, authenticity, integrity or confidentiality of data;

5. **the criticality of the services affected**, including the financial entity's transactions and operations;

6. **the economic impac**t, in particular direct and indirect costs and losses, in both absolute and relative terms.

Organizations must also determine **whether or not a cyberthreat is significant** on a similar basis to the list above.

DORA sets the broad guidelines for incident classification, but the exact thresholds are still unclear. They will be defined by the ESAs, the ECB and ENISA, which have until January 17, 2024 to submit their recommendations to the Commission. So, we'll have to wait and see, even if common sense and the knowledge of your organization should allow you to set a first classification grid that is personal to you.

MANDATORY POST-INCIDENT REVIEWS

Article 13 requires organizations to conduct **mandatory post-incident reviews after the occurrence of a major incident** that disrupts their core activities.

These reviews must determine :

- if the established procedures were followed;

- and whether they were effective in terms of :
  - the promptness in responding to security alerts and determining the impact of the incident and its severity;
  - the quality and speed of performing a forensic analysis;
  - the effectiveness of incident escalation within the financial entity;
  - the effectiveness of internal and external communication

Changes that have been made as a result of post-incident reviews should be kept available to the competent authorities.

WHAT IS A «MAJOR INCIDENT»?

Ah, that's a million-dollar question ! Here's the definition as given by the regulation:

"Major ICT-related incident": an ICT-related incident that has a high adverse impact on the network and information systems that support critical or important functions of the financial entity;

– DORA, Article 3(10)

Let's also slip in the definition of a «significant cyber threat» :

"Significant cyber threat": a cyber threat the technical characteristics of which indicate that it could have the potential to result in a major ICT-related incident or a major operational or security payment-related incident;

– DORA, Article 3(13)

12 WRITE AND DOCUMENT YOUR INCIDENT RESPONSE PLAN

One of the first things you should do to fuel the incident management process is to draft (or revise) your Incident Response Plan (IRP). It will prove invaluable when faced with an obligation to respond – whether to partners, customers, or competent authorities.

There are many useful resources on the web for creating your IRP. Keep in mind that it must comply with the response obligations introduced by DORA, which brings us directly to the next point.

FIND OUT WHICH «COMPETENT AUTHORITY» YOU SHOULD REPORT TO

First of all, it should be noted that the **competent authorities are not the same for all financial entities.** The subject is far too broad for us to detail them all here. Therefore, we refer you to Article 46 of DORA, the aptly named «Competent Authorities», which will clarify your own situation. Please note that the principle of proportionality that we discussed earlier applies here. If you are subject to more than one national authority, the State will have to decide which one prevails.

Furthermore, under Article 19(1), States are free to impose on one or more of the financial entities on their territory **a dual response obligation:**

- to the competent authority under DORA;
- but also to the competent authorities or to the Computer Security Incident Response Centers (CSIRT) designated under NIS2.

This is not mandatory, but possible. It is therefore up to each entity to verify its own situation.

RESPONSE OBLIGATIONS TO COMPETENT AUTHORITIES

By now, you should know which competent authority you are dealing with; the question remains as to when to contact it.

In the event of a major incident, Article 19(4) provides that financial entities must submit to the relevant competent authority:

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

Financial entities may also notify, **on a voluntary basis, significant cyber threats** to the relevant competent authority where they believe it is relevant to the financial system, service users or customers.

Note also that the DORA Regulation allows for outsourcing of reporting obligations to a third party service provider - see Article 19(5). Nevertheless, the financial entity remains fully responsible for complying with its requirements. Here again, no way to put the blame on a vendor!

WHAT ARE THE TIMELINES FOR DORA RESPONSE OBLIGATIONS?

The timeframes that apply to each notification are still unknown, and must be specified by the ESAs, ENISA and the ECB by January 17, 2024. Nevertheless, we believe it is safe to assume that the timelines under DORA will be similar to those introduced by the NIS2 Directive, which requires:

- an initial notification within 24 hours after the occurrence of the major incident;
- an intermediate notification within 72 hours;
- a final report at the latest one month after the first notification.

Again, there is no indication that DORA will align with NIS2, this is just a guess on our part. If you want to know more about those response obligations, we recommend you to read **our NIS2 compliance guide.**

RESPONSE OBLIGATIONS TO CUSTOMERS

DORA does not only bring response obligations to the competent authorities, but also to customers! Here is the excerpt in question, which is perfectly clear:

> **"Where a major ICT-related incident occurs and has an impact on the financial interests of clients**, financial entities shall, without undue delay as soon as they become aware of it, inform their clients about the major ICT-related incident and about the measures that have been taken to mitigate the adverse effects of such incident.
>
> **In the case of a significant cyber threat**, financial entities shall, where applicable, inform their clients that are potentially affected of any appropriate protection measures which the latter may consider taking."
>
> – **DORA, Article 19(3)**

This customer outreach will obviously need to be based on your crisis communication plans – a matter addressed in section 10.

13 MONITOR CYBER THREATS

Knowledge is a weapon, in cybersecurity perhaps even more than elsewhere. Attackers compete in ingenuity to achieve their goals, and underestimating them would be a big mistake. A CISO therefore needs to be aware of the shifting cyber threat landscape. The annual OWASP Top 10 is a good start, but it is far from sufficient to understand all the risks. Monitoring must be assiduous, collective and continuous.

Cyber intelligence is a topic brought up by DORA in its Article 13. It states that **financial entities must have the capacity and manpower to gather information on vulnerabilities and cyber threats.** They must also continuously monitor technological developments to determine the impact their deployment may have on cybersecurity and digital operational resilience requirements.

Our recommendation is to **set up an internal intelligence unit**, composed of the most aware individuals on cyber topics, with regular sharing of findings. But this is just one of many avenues to explore.

AN ANNUAL REPORT PUBLISHED BY THE ESAS ON MAJOR INCIDENTS IN THE FINANCIAL SECTOR

Article 22 of DORA requires ESAs to publish an annual, anonymized, aggregated report on major ICT incidents. The report should include, at a minimum, the number of major incidents, their nature and impact, the corrective actions taken and the costs. It will be accompanied by warnings and «high-level statistics".

It is safe to assume that this annual report will be a staple of cyber intelligence in the financial sector.

CYBER THREAT INFORMATION SHARING ARRANGEMENTS BETWEEN FINANCIAL INSTITUTIONS

Mutual assistance within the banking system is encouraged by DORA. Chapter VI provides that financial entities may create arrangements to share information and intelligence on cyber threats among themselves, including indicators of compromise, techniques and tactics, and procedures and tools.

This information sharing between financial institutions should:

- **aim to enhance** the digital operational resilience of entities;
- take place within **trusted communities** of financial entities;
- be based on mechanisms that **protect the potentially sensitive nature of the information** shared. These exchanges must be conducted in full respect of business confidentiality, GDPR and guidelines on competition policy.

The sharing arrangements must define the concrete modalities of sharing (where, how?) and the conditions of participation to be respected - for financial entities as well as for public authorities and ICT service providers. In addition, any financial entity participating in such a scheme must notify the relevant authorities.

14 CONDUCT «DIGITAL OPERATIONAL RESILIENCE TESTING»

We're tackling another big piece of the regulation here. Digital operation resilience testing is an integral part of the digital operation resilience strategy, and DORA devotes its entire Chapter IV to it. We will refer to them as «resilience tests» or «security tests» for ease of reference.

Let's be clear from the outset that most of these requirements do not apply to microenterprises. If this is your case, we invite you to read Chapter IV (especially Article 25.3) to determine what is applicable or not. There's no need to drag out the suspense any longer, so let's get down to business.

MAP YOUR INFORMATION SYSTEM

Before testing your digital assets, you need to identify them. It is unthinkable to perform a proper test before having mapped your entire information system. This complete inventory is not only dictated by common sense, but also by the final text of DORA since it is **a mandatory element of the ICT risk management framework** mentioned at the beginning of this article. This step will allow you to:

- have a global view of the organization's assets ;
- then to classify them by criticality and risk level.

A RESILIENCE TESTING PROGRAM TO BE PERFORMED AT LEAST ONCE A YEAR

In the words of DORA, financial entities shall ensure **"at least yearly, that appropriate tests are conducted on all ICT systems and applications supporting critical or important functions.»** (Article 24.6).

These reviews are grouped into a digital operational resilience testing program which must take **a risk-based approach**. It should include "a range of assessments, tests, methodologies, practices and tools."

Article 25 of DORA specifies **some typologies of tests, such as:**

- vulnerability assessments and scans;
- open source analyses – see our article **Understanding OSINT, its tools, benefits and risks;**
- 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.**

These tests may be performed in-house or by external vendors. If testing is performed by an in-house tester, financial entities should allocate sufficient resources to the test and ensure that conflicts of interest are avoided during the design and execution phases of the test.

A VULNERABILITY OPERATIONS CENTER (VOC) TO DETECT AND PRIORITIZE VULNERABILITIES

Should you choose a service provider to conduct certain security tests, the Yogosha **Vulnerability Operations Center (VOC)** offers several approaches to reduce digital risks:

- Vulnerability Disclosure Programs (VDP)
- Pentest as a Service
- and Bug Bounty

Obviously, all the operations we propose to the financial sector are done in strict compliance with the new DORA requirements.

PENTEST AS A SERVICE

Our platform enables the digitization of pentesting activities, with real-time results and faster launches than with traditional penetration testing. Our technology makes the discipline more efficient and fluid, both for your internal red teams and for external researchers.

In addition to offering technology, we perform penetration testing with members of the **Yogosha Strike Force:** a private and selective community of security researchers, each with their own expertise and skills.

Read also: **Pentest as a Service vs traditional pentesting, which differences?**

BUG BOUNTY

When a sufficiently advanced level of security is reached, penetration tests show their limits. **Bug Bounty** then allows to face the reality of the field, by asking ethical hackers to test all or part of a system. Bug Bounty has a pay-per-result logic (no detection = no expense), while allowing the discovery of complex and high-risk vulnerabilities that may be missed by other more calibrated forms of audits.

We could go on for hours about the merits of bug bounty, but this article is already long enough. So we'll just say three things:

- **The Yogosha Strike Force is a community of elite hunters**, where each member has been carefully selected based on their skills – unlike most bug bounty platforms that are open to anyone.

- **Our Vulnerability Operations Center (VOC**) provides a holistic view of your attack surface through detailed analytical dashboards - number and types of vulnerabilities discovered, perimeters where detections are most frequent, etc. Risk mapping, vulnerability prioritization... Does this remind you of the requirements of a certain European regulation?

- **The Yogosha VOC can be SaaS or Self-Hosted.** The self-hosted model is particularly suitable for sensitive and critical systems, as it allows strong data partitioning, full control of the execution context and centralization of all security activities on the same platform, even if they are carried out across multiple entities. An ideal deployment for large financial sector groups.

Read also: **Bug Bounty: the ultimate guide to a successful program**

DORA: AN OBLIGATION TO REMEDIATE ALL DISCOVERED VULNERABILITIES

There is no point in detecting vulnerabilities if they are not patched afterwards. DORA formalizes **remediation for all vulnerabilities discovered during testing:**

> "Financial entities, other than microenterprises, shall establish procedures and policies **to prioritize, classify and remedy all issues** revealed throughout the performance of the tests and shall establish internal validation methodologies to **ascertain that all identified weaknesses, deficiencies or gaps are fully addressed."**
>
> – DORA, Article 24(5)

That means that even «low» or «medium» vulnerabilities cannot be left out. Remediation must be total. This is a topic that must be addressed in collaboration with the development teams, the CTO and any other appropriate manager.

GIVE BUSINESS TEAMS THE TIME TO REMEDIATE

Remediation is too often seen as an «extra» task, to be done when a developer has some free time. Yet it is something that should be fully integrated into the schedule of technical teams.

While the most critical vulnerabilities must be addressed immediately, the others can for instance be addressed in a weekly or monthly Bug Day, depending on the size of the teams. Regardless of the approach chosen, it is important to realize that **remediating vulnerabilities is at least as important as developing new features.**

ENCOURAGE SECURE DEVELOPMENT METHODS

Cybersecurity by design is a topic that is on everyone's lips, and for good reason. It's crucial to build security into products and services from the very beginning. This is an approach advocated by NIS2, but also the EU Cybersecurity Act of June 2019.

Obviously, one cannot expect a CISO to train dev teams in secure development practices. Nevertheless, nothing prevents you from going the extra mile and making people aware of this subject. Here again, this is a mission that can be carried out hand in hand with the SOC teams, the CTO or internal security experts. From training to workshops and CTF (Capture The Flag), there are plenty of possibilities.

A VOC TO BRING DEV AND SEC TEAMS TOGETHER

One of the goals of our Vulnerability Operations Center is to **break down the barriers between the different operational roles.** Development teams are too often separated from security teams. Vulnerability detection can be a sore point for some developers, who may see it as evidence of a poorly done job. Remediation can then only be experienced as a punishment.

OUR VOC ALLOWS YOU TO BRING TOGETHER ALL THE COMMUNITIES:

- your security teams;
- your technical teams, such as developers;
- your partners' teams, like their red teamers or pentesters;
- and the hunters of the Yogosha Strike Force.

The convergence of professions within the same platform allows for better understanding and, ultimately, better collaboration. If one of our hackers discovers a vulnerability, he or she will surely be able to guide the developer in the remediation. Similarly, you could invite your partners' red teams to participate in a joint pentest operation. And if we think big, we can imagine that everyone meets in real life during a **Live Hacking Event...**

15 PLAN «THREAT-BASED PENETRATION TESTS» (TLPT)

In the previous section, we discussed the «traditional» testing that is the annual responsibility of all entities within the scope of DORA. But **some organizations are subject to an additional testing requirement,** aka «threat-based penetration testing», or TLPT.

WHICH ENTITIES ARE SUBJECT TO ADVANCED SECURITY TESTING?

Well, that's simple: it's up to the competent authorities. Article 26(8) of DORA grants them the duty to «identify financial entities that are required to perform TLPT [...] based on an assessment of the following:"

- **impact-related factors,** in particular the extent to which the services provided and activities undertaken by the financial entity impact the financial sector;
- **possible financial stability concerns,** including the systemic character of the financial entity at Union or national level, as applicable;
- **specific ICT risk profile,** level of ICT maturity of the financial entity or technology features involved.

Competent authorities should apply the principle of proportionality when deciding on the entities subject to advanced testing.

WHAT IS A THREAT-BASED PENETRATION TEST?

As it stands, the wording is impressive but somewhat cryptic. Let's start with the official definition given by DORA:

> **"Threat-led penetration testing (TLPT)":** 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;
>
> – DORA, Article 3(17)

THE MANDATORY CRITERIA OF A THREAT-BASED PENTEST

The official definition clarifies the concept, but the technical details are still unclear. Fortunately, Article 26 specifies **some mandatory criteria for a threat-based penetration test:**

- **The test must «cover several or all critical or important functions»** of the financial entity;
- **The scope is defined by the entity itself**, but approved by the competent authorities;
    - **If third-party ICT services are included in the scope**, the entity must take «the necessary measures and safeguards to ensure the participation» of the relevant provider. Full responsibility remains with the entity.
- Testing must be performed **on live production environments;**
- **A test must be performed at least every 3 years.** Competent authorities may reduce or increase this frequency for a particular entity based on its risk profile or operational circumstances.
- **At the end of the test**, the financial entity must submit to the competent authorities a summary of the relevant findings, corrective action plans, and documentation demonstrating that the test was performed in accordance with the requirements.
- In exchange, **the authorities issue a certificate** "in order to allow for mutual recognition of threat led penetration tests between competent authorities».

«POOLED TESTING» FOR ICT SERVICE PROVIDERS

There may be times when an ICT service provider cannot be included because it would affect the security of their services or the quality of the test. Similarly, there may be cases where a provider is a supplier to different financial entities. In these cases, DORA provides an exception.

The provider may conduct a «pooled TLPT» involving several financial entities to **which it provides services.** The provider must then:

- agree to the test in writing with the different entities;
- sign contractual agreements with an external tester;
- ensure that the test covers all ICT services that support the critical and important functions of the financial entities;
- conduct the test under the direction of a designated financial entity.

If so, Article 26(4) provides that the group test shall "be considered TLPT carried out by the financial entities participating in the pooled testing."

THE TIBER-EU FRAMEWORK FOR OPERATIONAL REQUIREMENTS

DORA sets the guidelines for threat-based penetration testing, but another European framework takes care of the operational requirements. The **TIBER-EU framework** specifies the rules for the scope of the test, the methodologies and the approach to follow for each specific phase of the test, from build to remediation.

The TIBER-EU framework is currently being rolled out in various EU countries, with the ambition of applying to all. For example, TIBER-BE for Belgium, TIBER-LU for Luxembourg, TIBER-DK for Denmark, etc.

It should be noted that there is currently no certification agency in Europe for TIBER-EU test providers. These accreditations should become clearer over the next few years. As far as DORA is concerned, the ESAs and the ECB have to propose to the Commission joint drafts of technical standards in accordance with the TIBER-EU framework, at the latest by January 27, 2024.

The TIBER-EU framework is a topic in its own right, so there will soon be a dedicated article on our blog – the link will be available here. Until then, we refer you to the TIBER-EU information page published by the ECB (European Central Bank), and the service procurement guidelines.

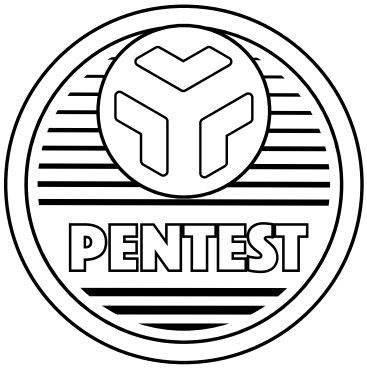
HOW TO CHOOSE AN EXTERNAL TESTER FOR A THREAT-BASED PENETRATION TEST?

First of all, financial entities can use internal testers, with a requirement to **hire an external tester every third test**. A minor exception is that credit institutions classified as large must always rely on an external tester.

That being said, Article 27 of DORA specifically defines **the requirements for testers who may perform a threat-based penetration test**. Testers must:

- be of the **highest suitability and reputability;**
- **possess technical and organizational capabilities** and demonstrate specific expertise in threat intelligence, penetration testing and red team testing;
- **adhere to formal codes of conduct or ethical frameworks**, or be certified by an accreditation body in a Member State;
- provide an independent assurance, or an audit report, in relation to the sound management of risks associated with the carrying out of TLPT, including the due protection of the financial entity's confidential information and redress for the business risks of the financial entity;
- be duly and fully **covered by relevant professional indemnity insurances**, including against risks of misconduct and negligence. (Which is true for

Obviously, there must be no conflict of interest during the conception and execution phases of the test. This will be verified by the relevant authorities, who must also approve the use of testers.



Yogosha).

SECURITY TESTS CONDUCTED BY YOGOSHA

For the record, **we are already taking all necessary measures to meet these requirements – legal, technical and operational.** However, the profoundly unique, complex and confidential nature of these large-scale tests makes it difficult for us to elaborate on the subject publicly. Also, as mentioned above, the provisions of the TIBER-EU framework applicable to test providers remain to be clarified.

In the meantime, feel free to contact us if you have any regulatory needs, whether it is for a threat-based penetration test or for the «classic» resilience tests applicable to all entities in the scope of DORA.

CONTACT US!

16 EDUCATE AND TRAIN TOP MANAGEMENT AND EMPLOYEES ON CYBERSECURITY

It's essential to plan for training, whether for C-Levels or all employees – depending on the skills and responsibilities of each individual. We cannot stress this enough, **but the risk associated with an organization's employees is at least equivalent to – if not greater than – the risk associated with cyber attacks**. To summarize: there's no point in having the best processes and technologies if half of your staff is writing down passwords on papers or passing sensitive information in plain text. If the people who run your organization are not educated in basic cyber hygiene practices, your security will remain a mess.

DORA: MANDATORY TRAINING FOR EXECUTIVES AND EMPLOYEES

NIS2 introduces mandatory cyber risk management training for management bodies, but only encourages it for employees. DORA, on the other hand, goes further and imposes **mandatory digital operational resilience training for both executives and employees.** The final text is very clear:

> "Financial entities shall develop **ICT security awareness programmes** and digital operational resilience training **as compulsory modules** in their staff training schemes. Those programmes and training shall be **applicable to all employees and to senior management staff**, and shall have a level of complexity commensurate to the remit of their functions. Where appropriate, financial entities shall also include ICT third-party service providers in their relevant training schemes"
>
> – **DORA, Article 13(6)**

The CISO is probably one of the best placed people to guide the choice of training courses (or at least of providers) in conjunction with Human Resources and the managers of each division. The proper training of employees is a vast project, transversal to different professions, which must be undertaken as soon as possible.

LIVE HACKING EVENTS, A FIELD TRAINING FOR OPERATIONAL TEAMS

At Yogosha, we like field approaches. That's why we organize Live Hacking Events. They bring together clients' internal teams and hackers from the Yogosha Strike Force for a few days.

Let's be clear, these events are not intended to educate top management or just anyone in-house. Rather, they are an excellent training opportunity for operational teams, such as developers or security teams.

A Live Hacking Event challenges teams in real-life conditions, with a true Red Team versus Blue Team philosophy. Our hunters identify vulnerabilities live, and your teams work on remediation in the moment.

Discover our Live Hacking Events

17 ASSESS AND MANAGE ICT THIRD-PARTY RISKS

Supply chain security is at the heart of NIS2, and DORA aligns with it. The Regulation puts a particular emphasis on **risk management related to ICT service providers.**

It should be noted that this workstream belongs to CISOs as well as to legal departments. Many of the DORA requirements related to providers directly affect the content of the contractual agreements dictating the collaboration. We will only briefly discuss this part, where most of the tasks fall into the legal and contractual sphere, rather than the operational one. Instead, we strongly recommend that you read the whole Chapter V of DORA.

It should also be noted that DORA requires financial entities to manage risks related to service providers «in accordance with the principle of proportionality, taking into account the nature, scope, complexity and importance of the dependency relationships» and the risks arising from these arrangements. DORA therefore sets out rules, but calls for good judgment in applying them.

IMPLEMENT A «STRATEGY ON ICT THIRD-PARTY RISK»

Yes, another strategy to create! Article 28(2) requires financial entities to «adopt **a strategy on ICT third-party risk**» and review it regularly.

This strategy must itself include a policy on the use of services that support critical or important functions. The management body must also «regularly» review the risks identified for these same services and contractual agreements. Again, DORA is in line with the governance of NIS2. Cybersecurity shouldn't be the sole responsibility of operational teams, and top management must also be aware of the risks and take ownership of them.

As part of the ICT risk management framework (seen at the beginning of this article), financial entities must also maintain and update «**a register of information in relation to all contractual arrangements** on the use of ICT services provided by ICT third-party service providers.» In plain English: you must have a complete inventory of your entire ICT provider ecosystem. It must clearly distinguish between providers that support critical functions, and those that do not. This register must be provided to the relevant authorities if they request it.

GUIDELINES TO BE FOLLOWED BEFORE CONCLUDING A CONTRACTUAL AGREEMENT

Article 28(4) is very clear on the rules to be followed. Before entering into a contractual agreement for the use of ICT services, financial entities shall:

- assess whether the contractual arrangement covers the use of ICT services supporting a critical or important function;
- assess if supervisory conditions for contracting are met;
- identify and assess all relevant risks in relation to the contractual arrangement, including the possibility that such contractual arrangement may contribute to reinforcing ICT concentration risk;
- undertake all due diligence on prospective ICT third-party service providers and ensure throughout the selection and assessment processes that the ICT third-party service provider is suitable;
- identify and assess conflicts of interest that the contractual arrangement may cause;
- determine in advance, where appropriate, the areas to be audited and the frequency of inspections.

As for the (lengthy) list of the main contractual provisions to be respected, we refer you directly to **Article 30.**

PLAN «EXIT STRATEGIES» FOR KEY PROVIDERS

Article 28(8) calls for financial entities to have «comprehensive and documented» exit strategies for services that support critical or important functions. At a minimum, this exit strategy must include:

- alternative solutions;
- transition plans for removing services and data held by the provider;
- and to safely and fully transfer them to alternative providers or reincorporate them internally.

It is **Article 28(7)** that sets out the conditions under which these contractual arrangements must be terminated - most of the reasons being related to a lack of security or due diligence by the provider.

CRITICAL PROVIDERS IDENTIFIED BY THE ESAS

It should be noted that the ESAs have the power to declare certain service providers as critical to financial entities. The providers in question are then subject to the authority of a primary supervisor, namely an ESA designated for the role. This supervisory framework is extremely dense, spanning over 10 articles of the Regulation. So, if you are interested in this topic, we invite you to read Articles 31 through 44 of DORA.

IN A NUTSHELL

The European financial sector has until January 17, 2025 to prepare for the implementation of the Digital Operational Resilience Act. The task is substantial and will demand rigor, resources and above all, time. Therefore, we advise all CISOs of entities within the scope of the regulation to start working on compliance right away.

The bulk of the work should focus on three main areas:

- the ICT risk management framework;
- digital operational resilience testing;
- ICT third-party risks management.

These key regulatory topics are dissected here into 17 action steps, which we have tried to make as concrete as possible. It is probably wisest to start with the drafting and implementation of mandatory policies brought about by DORA. The regulation is organized as a Russian doll of policies, and a methodological approach is to be preferred.

The ICT risk management framework must be accompanied by:

- a digital operational resilience strategy;
- an ICT business continuity policy;
- backup, restoration and recovery procedures;
- records of activities in the event of disruptions;
- an incident management process;
- an incident response plan;
- crisis communication plans

On the security testing side, it will be necessary to conduct:

- digital operational resilience tests at least once a year;
- for the entities concerned, «threat-based penetration tests» at least every 3 years, in compliance with the TIBER-EU framework.

Finally, managing the risks associated with your third-party ICT service providers will be your last major focus. You will need patience and, most importantly, the support of your organization's legal department. You will need to manage and document the collaboration relationship from start to finish, from mandatory contractual provisions to exit plans for the most sensitive providers. Sprinkle in obligations to monitor cyber threats, or mandatory training for C-Levels and employees, and you have plenty of work to do!

Please contact us if you have any compliance needs related to DORA requirements, especially for:

- **Digital operational resilience testing**, through our pentest and bug bounty operations;
- **Threat-based penetration testing,** through early contact until the TIBER-EU framework becomes clearer;
- **Vulnerability detection, prioritization and management,** through a demo of our **Vulnerability Operations Center (VOC).**

CONTACT US!

Writing: Yogosha – yogosha.com – May 2023 /
Author: Sébastien Palais
Design-production: Pokeslide – pokeslide.com