valantic

DORA & TLPT

Strengthening digital resilience through threat intelligence and simulated cyber attacks

How financial institutions comply with the Digital Operational Resilience Act (DORA)

Table of contents

With DORA (Digital Operational Resilience Act), the EU aims to establish a universal framework for the management and mitigation of ICT risks in the critical financial sector. By harmonising risk management rules across the EU, DORA aims to eliminate the gaps, overlaps and conflicts that could arise between different regulations in different EU member states. Important: The DORA directives are mandatory for safety-critical companies in Germany and Europe.

Thomas Lang

thomas.lang@mc.valantic.com

After more than 20 years as a consultant and entrepreneur, Thomas Lang's ability to adapt quickly, even in critical situations, has become second nature to him. He remains calm in every situation, can separate the important from the unimportant and gives things structure. This helps him to maintain an overview in difficult situations. In addition to cyber security & compliance, his consulting focus includes IT strategy, project governance and controlling, crisis management and IT infrastructure & operations.

DORA is mandatory, otherwise fines may be imposed

For companies, this means that DORA has been mandatory since 17 January 2025 and applies to all financial institutions in the EU.

This includes traditional financial actors such as banks, investment firms and credit institutions as well as non-traditional actors, including crypto-asset service providers and crowdfunding platforms. All DORA requirements must be fully complied with.

And beware: Leading supervisory authorities can impose fines of 1% of the provider`s average global daily turnover in the previous financial year. These penalties can continue on a daily basis for up to six months. In addition, DORA provides that members of management can be held personally liable in the event of gross negligence or wilful misconduct.

Cybersecurity: Allianz Risk Barometer 2025 and Bitkom

The reason for the stricter security requirements: Cyber incidents such as ransomware attacks, data protection breaches and IT failures rank first among global risks in the Allianz Risk Barometer (2025) - once again. In concrete terms, this means:

- **Cyber attacks threaten the existence of entire companies,** for example, production comes to a standstill, deliveries, payments or access to own systems or data are no longer possible.
- In addition to the financial impact, damage is also caused by the **publication of internal data, intellectual property, business secrets of partners**, confidential **data of natural persons** etc.

The prevailing opinion in companies is often: It won`t affect us. But companies under attack are not isolated cases. The digital association Bitkom conducts an annual study that is representative of the economy as a whole and came to the following conclusions in 2024:

- 8 out of 10 companies are affected by data theft, espionage or sabotage.
- The total annual loss amounts to EUR 267 billion.
- 31% of affected companies report damage caused by ransomware.
- Two thirds of companies feel their existence is under threat.

The current risk trends for financial institutions

First the good news. According to valantic`s analyses, advanced persistent threats (APTs) - i.e. state-controlled actors - are currently less relevant. However, this analysis is heavily dependent on geopolitical developments and can change quickly.

Ransomware has consistently topped the list of top threats for most companies in Germany for years. Financial companies also fall victim to ransomware time and again, which steals and encrypts data and only releases it again after a ransom has been paid. For example, Deutsche Leasing, a partner of Kreissparkasse Köln was a victim to the BlackBasta ransomware group in 2023.

Hacktivism, especially through DDoS attacks, is now part of everyday life for the German financial industry and will remain so for the time being, according to valantic`s security experts. DDoS attacks usually only last a short time and cause hardly any long-term damage.

The interconnectedness of the financial sector - especially in the case of savings banks - also increases the risk of supply chain incidents through compromise of service providers and business partners. Threat actors are increasingly attempting to compromise organizations via partner companies, particularly due to the high level of regulatory protection in the financial sector.

These attack patterns are currently threatening the financial industry

Particularly striking for the financial sector is **social engineering**, a technique in which cyber criminals specifically exploit human weaknesses to **gain access to confidential information, compromise systems** or **to persuade people to take certain actions**. In doing so, they manipulate the trust, helpfulness or carelessness of their victims by **deception and psychological tricks**.

The use of **stealer malware** is experiencing an **increasing relevance** for the entire cybercriminal ecosystem, including ransomware and APT groups. The purchase of credentials usually provides easier **access to corporate networks** than exploring and exploiting a technical vulnerability. Attacks on banking accesses offer a particularly attractive target after the accounts have been compromised by attackers, especially via simple transfers.

In most cases, geopolitically motivated attacker groups use **(D)DoS attacks** to paralyse websites and services in the financial sector for a short period of time.

The immediate potential consequences of (D)DoS attacks are **service interruptions**. An overload of the servers may result in the bank‘s online services, such as **Internet banking, mobile apps and customer support no longer being available**.

Loss of trust:

Customers are particularly affected as they have no access to their accounts and cannot carry out transactions, resulting in **frustration and loss of trust.**

Absolute standstill of important processes:

Depending on the intensity and protection, important business processes can be disrupted, including transactions, the processing of payments and the customer deposit business, resulting in a **direct financial loss.**

RECOMMENDATIONS FOR ACTION

How to improve your protection

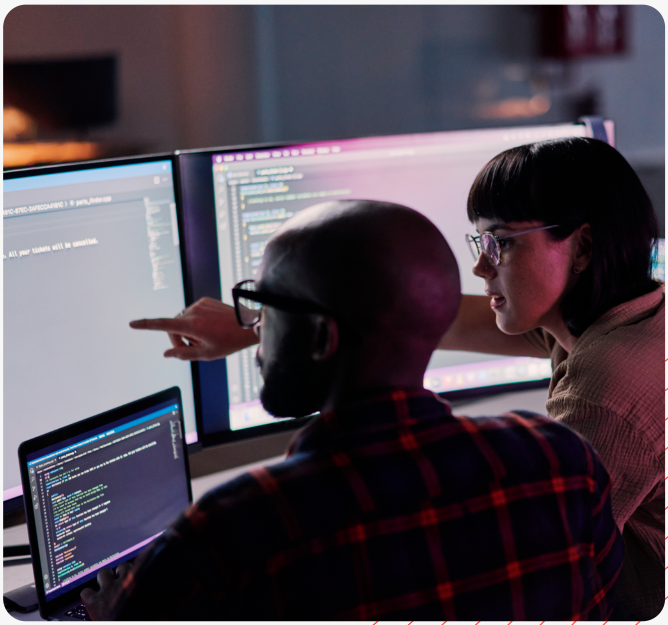
Threat: Social Engineering

Awareness training: Regular training for employees on how to recognise and defend against social engineering attempts.

Verification processes: Implementation of procedures that secure important transactions and changes through multiple confirmations.

Zero-Trust Principle: Minimising internal and external trust and limiting access rights to the bare minimum.

Threat Intelligence: Continuous procurement of information on current trends and attacker groups in order to stay one step ahead of impending threats.



Threat: Stealer Malware

Endpoint security: Use of anti-malware and anti-virus software with real-time protection and automatic detection.

Two-factor authentication (2FA): Introduction of 2FA for all employees and customers to secure access data.

Darknet monitoring: Alerting of (access) data offered for sale in relevant darknet forums, marketplaces or Telegram channels.

Threat: DDoS attacks

DDoS defence services: Use of cloud-based solutions for filtering and defence against DDoS data traffic.

Network segmentation: Isolation of critical systems to minimise the impact of an attack.

Load tests: Carrying out regular load and stress tests to check the stability of the infrastructure.

SIMULATED CYBER ATTACKS

Threat-led Penetration Tests (TLPT)

In order to become and remain resilient, DORA recommends, among other things, assessing systemic technological risks using **TLPT (Threat-led Penetration Testing)**, i.e. simulated cyber attacks that are individually adapted to the respective organization. For particularly critical companies in the financial sector, TLPTs are mandatory every three years by BaFin and the Deutsche Bundesbank, and the companies concerned are called upon to organise certified and qualified external service providers themselves.

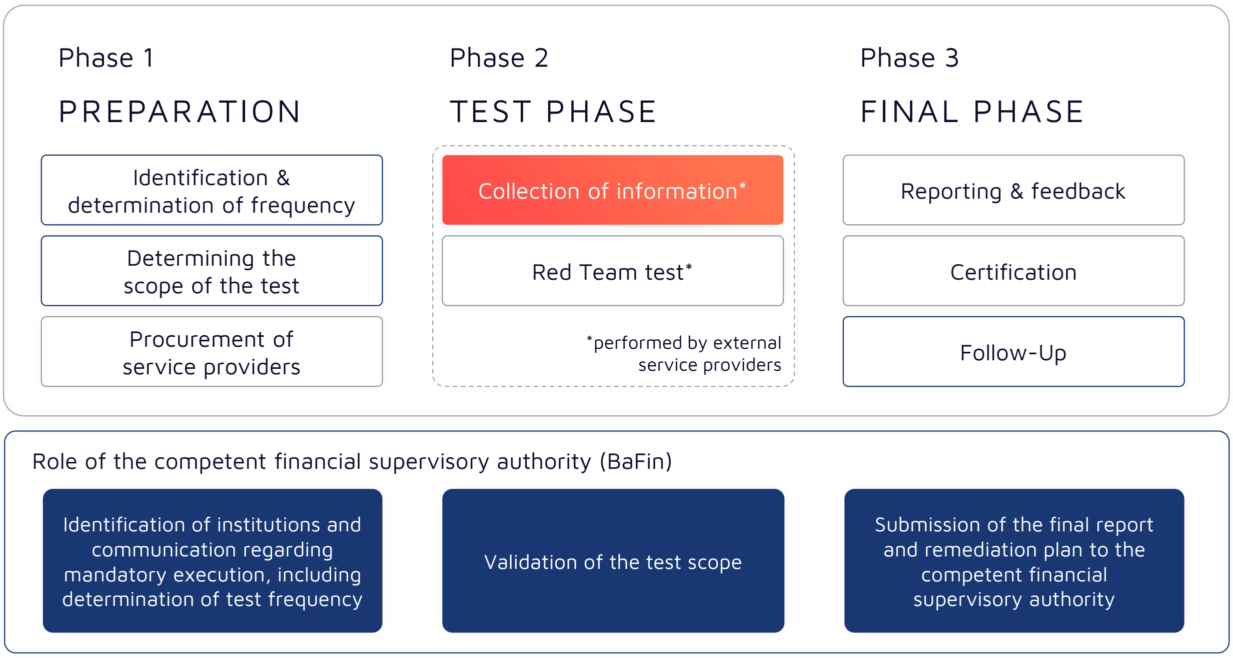
Good preparation, for example with the support of an experienced cybersecurity service provider, is crucial for success and time is of the essence. The BaFin and the Deutsche Bundesbank have set the bar high: external service providers must have experience with threat intelligence and offender profiles, threat analyses and open-source and must also be independent. These qualifications, including appropriate references, must all be proven. The controlling team is provided by BaFin. The aim is to draw up an individualised Targeted Threat Intelligence Report.

An overview of the actors required for threat-driven penetration tests in accordance with Article 26(11) of the DORA

- **TLPT Cyber Team (TCT):** the personnel within the TLPT authority who monitor TLPT operations.
- **Control Team:** Manages the financial organization`s TLPT and takes care of procurement, risk assessment and operational management while maintaining the confidentiality of the tests.
- **Blue Team Defender:** The defence team that attempts to fend off simulated or real cyber threats.
- **Threat Intelligence Provider:** An external service provider that simulates the collection of information by hackers using reliable sources.
- **Red Team Attacker:** Acts either as an internal or external service provider and acts as an attacking team.

How pentests work: planning, test and finalisation phase

An overview of the individual phases of a mandatory DORA threat-led penetration test, from planning to analysing the results and lessons learned:



Phase 1

PREPARATION

Identification & determination of frequency

Determining the scope of the test

Procurement of service providers

Phase 2

TEST PHASE

Collection of information*

Red Team test*

*performed by external service providers

Phase 3

FINAL PHASE

Reporting & feedback

Certification

Follow-Up

Role of the competent financial supervisory authority (BaFin)

Identification of institutions and communication regarding mandatory execution, including determination of test frequency

Validation of the test scope

Submission of the final report and remediation plan to the competent financial supervisory authority

Source: valantic – Own illustration based on Bundesbank and BaFin

The pentests simulate a cyberattack by the Red Team on the basis of a risk profile created in advance, analyse the results and then close the gaps and security deficits identified by the test. This significantly increases the company`s resilience.

Think like a cybercriminal

Penetration tests themselves, i.e. the actual attack, follows a simplified, precise „plan" that not only pen-testers but also cyber criminals follow.

1 Exploration

Collecting important information about a target system in order to better attack the affected company. For example, the aim could be to find information that can be used for a social engineering attack.

2 Scanning

Uses technical tools to expand the attacker`s knowledge of the system. For example, the Nmap security scanner is used to scan for open ports.

3 Gaining access

Using the data collected during the reconnaissance and scanning phase, the attacker can penetrate the system and take control of parts of it. The penetration testing platform Metasploit, for example, can be used to automate attacks on known vulnerabilities such as open, unprotected ports.

4 Maintaining access

Maintaining and disguising access is important in order to stay in the target environment permanently and collect as much data as possible. In the past, target systems have been compromised for months or even years without the victim, i.e. the attacked company, knowing about it.

5 Covering tracks

The attacker removes all traces and all types of collected data and log events in order to remain anonymous.

Staying one step ahead of cyber criminals

Many cyberattacks don`t usually happen out of the blue, but rather with an announcement, so to speak. This is because cyber criminals are now organised like companies and operate based on a division of labour. The „business" has become increasingly commercialised. Particularly in the initial reconnaissance phase (see above: Thinking like a cybercriminal), cybercriminals planning an attack search forums and marketplaces for information, passwords, access data and leaks that have already been captured and are now being sold on.

This is because around 95% of the internet is „hidden". This so-called **Deepweb** includes content that is not indexed by conventional search engines. This includes **sensitive** or **confidential** Information that is not publicly accessible. The **Darkweb** harbours **forums**, **marketplaces** and **communities** where valuable, critical data that is useful for a cyber attack is traded.

To stay one step ahead of cyber attackers, valantic offers a darknet monitoring service. If, for example, sensitive access information of company xy is offered for sale on the darknet, it is to be expected that an attack on the company concerned will take place in the near future. For reasons of cyber security, primarily in the area of **threat intelligence**, a look into the dark and deep web is therefore **essential**.

The security package from valantic

Professionally conducted threat-led penetration tests provide real, data-based insights and identify technological and organizational vulnerabilities that your company was previously unaware of. The test results provide valuable insights and help you to make your organization more secure and resilient against cyber attacks.

As an experienced, external threat intelligence provider, valantic supports you throughout the entire TLPT process. This helps you avoid unpleasant surprises when the results of the mandatory tests are reported to the Bundesbank.

Every industry has its own special features. We analyse industries and derive any special attack risks, procedural patterns or recognisable threats that may exist and take these into account in our analyses. The highest quality standards can only be achieved by experts. Our team brings together former hackers, SOC specialists, admins, consultants, investigators and many more.

Our range of solutions goes far beyond TLPTs: with regular threat analyses and real-time monitoring, we always keep your security measures up to date and proactively support you in identifying and closing security gaps. Thanks to continuous monitoring, our customers are optimally prepared for TLPTs at all times - without any unpleasant surprises.

valantic

About us

valantic is one of the fastest growing digital consulting, solutions and software companies on the market. more than 500 blue-chip customers already rely on valantic - including 33 of 40 DAX companies and a large number of international market leaders. With more than 4,000 digitalization experts, valantic is represented in 18 countries worldwide.

Around 2,000 successful digitalization projects in the last five years have shown that valantic‘s experts understand their customers‘ challenges precisely. From strategy to tangible implementation, they have the necessary expertise to accompany projects from start to finish and make them successful. In doing so, they combine technological competence with industry knowledge and humanity.

valantic advises companies on all challenges of digital transformation, helps them to better manage their corporate performance and to leverage the potential of data and artificial intelligence. In addition, valantic supports its customers in optimally shaping the customer experience, profitably using core digitalization technologies and optimizing company processes across the board.

valantic
Management Consulting GmbH
Dreieich Plaza 2A
63303 Dreieich
Germany
Tel. +49 6103 50 86 0
Mail info@mc.valantic.com

www.valantic.com

October 2025