DORA: a pragmatic approach for pension funds

Embracing DORA Compliance in a pragmatic way to improve protection from cyber threats for pension funds

BDO Belgium
Risk Advisory – Cyber Security

The upcoming DORA legislation is causing a stir in the financial sector, including within pension funds. But why is DORA so important? In our increasingly interconnected world, emphasising **the importance of cyber security** is stating the obvious. The news is full of stories about the ever-increasing cyber attacks that seem to move closer every week. As Pension Funds manage large amounts of personal data and an important amount of funds, they are a prime target for hackers. Think about phishing attacks piling up in our mailboxes, or ransomware attacks that crippled multiple organizations the last couple of years.

In response to the **escalating wave of cyber threats**, the European Commission has taken a proactive approach by formulating **a regulation to aid the financial sector in protecting itself against such cyber threats**. The Digital Operational Resilience Act, or DORA, seeks to **strengthen the operational resilience** (or robustness) of the **financial industry and related sectors** – which explicitly includes pension funds. Embracing this new regulation with a pragmatic approach can transform DORA f**rom a burden into a source of added value** for your organisation and prevent you from becoming yet another victim of cyber crime.

Risks & consequences

Incidents within the financial sector predominantly emerge from the **pursuit of financial gain**, primarily orchestrated by **cyber criminals**. The sector is especially at risk due to the high volume of personal data that is kept by pension funds as well as the high amounts of funds that are managed within pension funds. Most pension funds **highly rely on third parties**, such as **pension administrators and asset managers**, which **expands the potential attack surface**. Just last year, a third party to a Dutch pension administrator was hacked, which exposed data from thousands of participants[1] .

From our experience, ransomware, malware, and (spear) phishing are the primary tactics used by threat actors. When these breaches happen, hackers do more than just steal data; they can interrupt operations and financial streams. This, in turn, can lead to (GDPR) fines and a decrease in trust in the pension fund.

[1] https://pensioenpro.nl/fonds-abn-amro-geraakt-door-hack-bij-postverzendbedrijf

Understanding DORA compliance

The DORA regulation represents comprehensive European Union legislation aimed at **boosting the overall level of operational resilience** within the EU. DORA is a "lex specialis", meaning it takes precedence over other similar regulations such as NIS2, should confusion arise. Have a look at our articles on NIS2[2], [3].

The DORA is composed of five key pillars:

1. ICT Risk Management;
2. ICT-related Incident Reporting;
3. Digital Operational Resilience Testing;
4. ICT Third Party Risk Management; and
5. Threat Intelligence and Information Sharing.

DORA's primary purpose is to increase and harmonize operational resilience and cyber security across the financial industry. Similar to NIS2, it recognizes our increased digitalisation and interconnectedness, and reliance on digital services and third-party providers (TPPs) for our operations. Both regulations warn that this leads to increased cyber risk and vulnerability to cyber threats and ICT disruptions, which must be addressed.

In addition to the regulation itself, detailed standards and templates are being developed by the regulators to further clarify certain requirements – the so-called Regulatory Technical Standards (RTS) and Implementation Technical Standards (ITS).

It's worth noting that, like all regulations, non-compliance could lead to stricter sanctions and potential accountability for senior management in cases of negligence.

[2] https://www.bdo.be/en-gb/insights/articles/2024/nis2-strengthening-cyber-security-across-europe
[3] https://www.bdo.be/en-gb/insights/articles/2024/adoption-of-nis2-directive-in-belgium

Why BDO is your ideal partner for DORA

Our cyber security experts not only assist you in **becoming DORA compliant**, but we also transform this challenge into **an opportunity to enhance your overall security and resilience.**

BDO is well known within the pension fund industry as internal auditor, risk manager and DPO. We are therefore ideally positioned to understand the challenges that DORA brings for the pension fund sector, and to help you implement a pragmatic, proportionate and risk-based approach to compliance.

Our commitment to you

A clear and concise action plan to ensure compliance with DORA, that's our minimum golden standard.

- **Leveraging industry standards and best practices:** we utilise renowned industry standards and frameworks to perform comprehensive assessments that are **tailored to your specificities and needs**. Our team of consultants works across various industries and has seen many approaches and best practices. It goes without saying that we bring this knowledge to the table when defining a cyber security strategy together with you.
- **Improved cyber resilience:** together we will strengthen your organisation's ability to detect, respond, and recover from cyber incidents effectively, minimising the impact on your operations.
- **Fresh perspectives:** BDO brings a fresh and unbiased perspective to evaluate your cyber security infrastructure, ensuring a comprehensive and impartial analysis. Our objective viewpoint is untainted by internal biases and can reveal vulnerabilities that might otherwise be overlooked.
- **Expertise and specialisation:** our team of consultants have extensive experience in the financial sector, including the pension fund sector. Our team includes seasoned cyber security experts. They are well-versed in the latest threats, vulnerabilities, and best practices. They bring a depth of knowledge and share it with you to be leveraged by your company.

What you can expect from us

- DORA awareness session: a comprehensive presentation to the board or daily management of the pension fund vis-à-vis DORA and what it means for pension funds.
- **Gap analysis:** identify weaknesses and vulnerabilities in your existing cyber security organisation, identifying must-haves to ensure DORA compliance but also nice-to-haves based on your desired security level.
- **Customised action plan:** a tailor-made action plan with **clear, concrete and actionable steps** to improve your cyber security posture and resilience.
- **Implementation support:** our experts guide your team in implementing the recommended security measures to better protect your organisation and ensure DORA compliance.

A pragmatic approach: proportionality for Pension Funds

Investing in cyber security can be a significant commitment for you, from a financial and resource perspective. As market leader, BDO is uniquely positioned to fully understand the challenges for Pension Funds to comply with such stringent regulation, which is why we have developed a **pragmatic approach** for pension funds to comply with DORA according to the **proportionality principle**. We believe following a **risk-based approach** that complies with the spirit of the law is sufficient for Pension Funds.

Want to get even more out of your DORA compliance assessment?

If your organisation is considering to adopt a cyber security recognition, such as an **ISO27001** certification, the DORA compliance assessment offers an excellent stepping stone. Our experienced team of ISO27001 Lead Auditors and Lead Implementers can guide you through the key challenges you will face and identify the major potential pitfalls to obtaining your desired certifications and attestations.

Let's get in touch!

Don't delay protecting your organisation any further. Reach out to one of our cyber security experts to discover how you can benefit from our pragmatic compliance assessment regarding the new DORA regulation.

Contact

SAM NELEN
Head of Cyber
Risk Advisory
Tel.: +32 486 91 12 20
E-mail: sam.nelen@bdo.be

THOMAS CORNELIS
Manager
Risk Advisory
Tel.: +32 493 64 49 01
E-mail: thomas.cornelis@bdo.be

TESSA PAUWELS
Junior Manager
Risk Advisory
Tel.: +32 476 61 75 66
E-mail: tessa.pauwels@bdo.be

▶ **Follow us**
▶ **www.bdo.be**