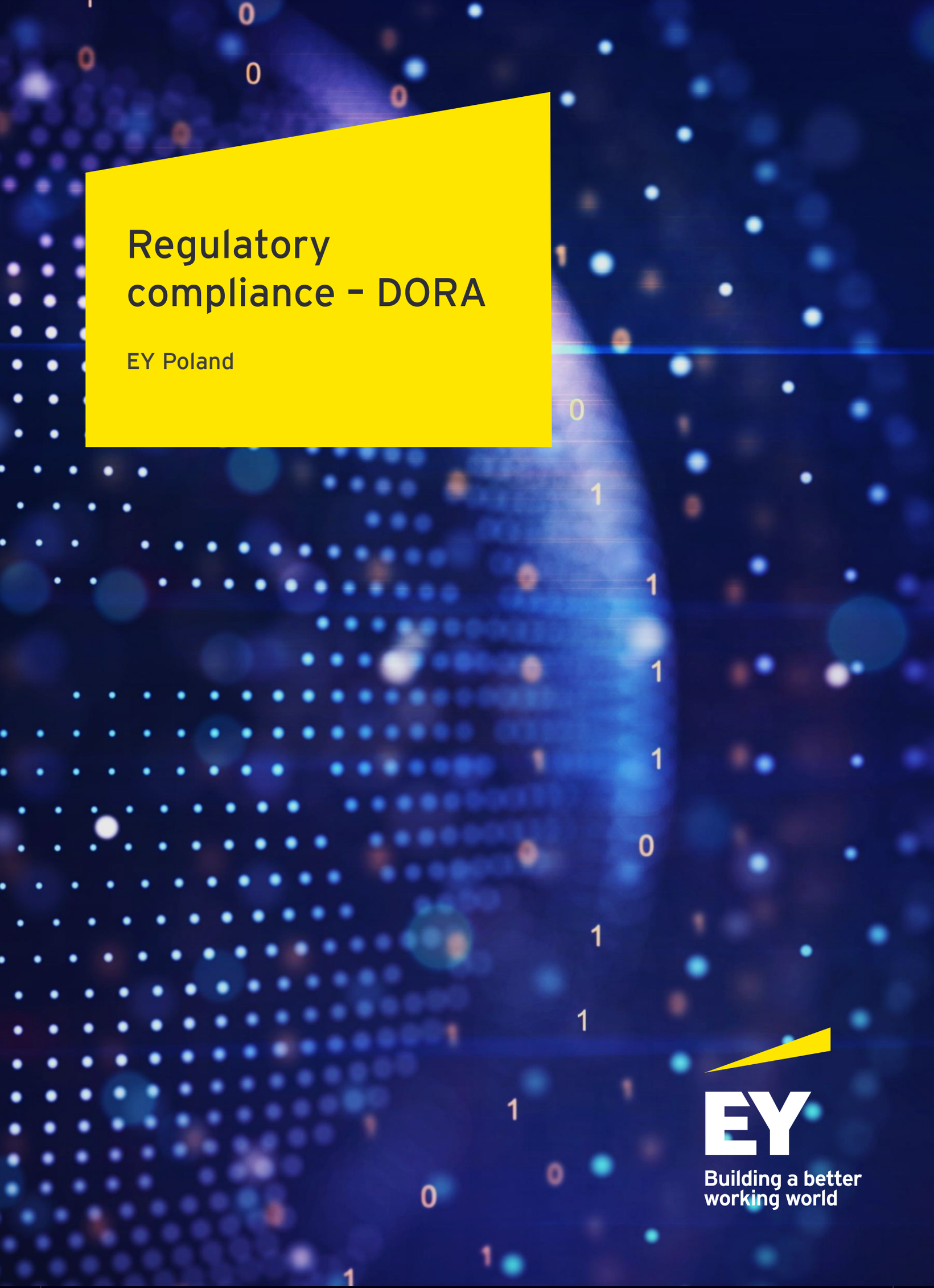
Regulatory compliance – DORA

EY Poland



Building a better working world

Why is DORA compliance important?

- Digital Operational Resilience Act came into force jn January 2023 and is a part of the European Commission Digital Finance Strategy.
- DORA will be passed into law by each EU state. Further technical standards will be developed by the European Supervisory Authorities and compliance will be overseen by the existing National Competent Authority framework.
- The Act will apply across the full financial sector, as well as to additional firms captured within the expanded regulatory perimeter under the term ‘critical ICT third-party service providers, which will include services such as Cloud resources, data analytics and audit.

DORA's focus areas:

- ICT risk management
- ICT-related incident management
- Digital operational resilience testing
- Managing of ICT third-party risk
- Information-sharing arrangements

How to prepare for DORA?

As a first step, we suggest to conduct a gap analysis that identifies existing requirements and provides solutions for adaptation.

The next step is to develop a list of initiatives that will increase the cyber resilience of the organization (if implemented) and at the same time ensure compliance with DORA at organizational, process and technology level.

A wide range of entities

- Electronic money institutions
- Crypto-asset service providers
- Issuers of asset-referenced tokens
- Insurance and reinsurance undertakings
- Crowdfunding service providers
- ICT third-party service providers
- Central securities depositories
- Trade repositories
- Account information service providers
- Investment firms
- Insurance intermediaries and reinsurance intermediaries
- Credit institutions
- Credit rating agencies
- Payment institutions
- Managers of alternative investment funds
- and other entities

New obligations for financial sector

- DORA establishes unified requirements for the security of networks and information systems of financial sector, as well as key third-party providers of ICT-related services.
- The regulation introduces a wide range of responsibilities, which include, e.g., drafting procedures, developing a testing framework or classifying risks and incidents.
- At the same time, DORA indicates a relatively short time for implementation in an organization, while there are high penalties for non-compliance.
- Therefore, it is important to check your readiness for DORA today.

Financial Institutions should assess if their current state meets the expanded regulation and plan accordingly to respond.

Suggested considerations

ICT risk framework

Assess existing ICT risk strategy, policies, procedures and tools. Consider roles and responsibilities skills in IT and Risk.

Testing – 'basic'

Review the scope and coverage of what would constitute 'digital operational resilience testing' program against DORA articles.

Testing – 'advanced'

Continue to assess the scope of threat-led penetration testing (akin to CBEST and TIBER), which contributes to DORA testing expectations.

'Critical' ICT third party status

Assess the services received from third party service providers to identify any that would an additional level of governance and oversight

Governance

Assess existing ICT risk governance (for regulated entities and inter-entity) to identify gaps in direction, evaluation or monitoring of ICT risk topics.

Incident reporting

Review incident identification, classification and reporting protocols against leading practice (including existing PSD2 expectations) to identify if investment in process/tooling is needed.

When you should remember about DORA?

- ✓ When implementing IT solutions (e.g. software, cloud) - DORA regulates the key elements of relationships with ICT service providers at all stages of contractual arrangements
- ✓ When implementing new critical IT systems, service platforms or network elements – new Act is focused on information security and service continuity/ Security by design
- ✓ When establishing new or modifying existing critical process – due to already mentioned focusing on a business and service continuity – avoiding single point of failure
- ✓ All the time – whenever you provide financial services to your clients – you have to be able to ensure continuity, protect from threats, identify them, make sure that they are managed and if the incidents will occur, being able not only to recover, but also to avoid them in the future, and report them to authorities

DORA compliance assessment by EY

As a part of the DORA compliance check, EY has developed a proprietary questionnaire that allows to assess the level of compliance with DORA. The result of the compliance check is a report indicating potential gaps:

Questionnaire

We work on a questionnaire we have prepared in advance. It contains detailed questions created on the basis of DORA.

Check yourself out! Just answer the indicated questions and we will do the rest.

Compliance report

A compliance report is essentially the identification of gaps in DORA compliance. You will find out in a transparent way what needs improvement in your organization.

Additional support*

However, that's not all! According to your needs, we can offer additional support:

- In-depth analysis in the identified scope (report, opinion);
- Drafting of specific documents (policy, agreement, procedure);
- Consultation with EY experts.

Deadline for meeting requirements

On January 16, 2023 DORA went into effect. From that moment on, entities in the financial sector have only two years to comply and avoid hefty fines.

16 January 2023

Start of the effectiveness of the regulation

17 January 2025

Deadline for implementing DORA-compliant solutions in the organization

Entrepreneurs in the financial sector have 2 years to comply with DORA requirements

Who are we?

We are a team of experts dedicated to helping organizations ensure their products and services are compliant with cybersecurity regulations. We can help identify gaps and issues and guide your organization through the compliance process.

30+ experts

Cooperating with the Cybersecurity team, we combine regulatory and technical expertise. As a result, we are able to prepare a comprehensive offer for you that addresses all aspects of compliance.

Key contacts

Justyna Wilczyńska-Baraniak

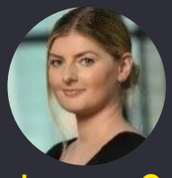
Partner/Principal, Digital Law Leader
EY Law Poland

E-mail: Justyna.Wilczynska-Baraniak@pl.ey.com
Tel: +48 519 098 119

Wojciech Dańczyszyn

Senior Manager, Technology Consulting, Cybersecurity

E-mail: Wojciech.Danczyszyn@pl.ey.com
Tel: +48 502 782 692



Joanna Gałajda, LL.M.

Manager, Cybersecurity & Cloud Expert

E-mail: Joanna.Galajda@pl.ey.com
Tel: +48 789 407 638

Join us for Deep Dive Session!

Based on the case you present, we will prepare a dedicated Deep Dive Session workshop to show what requirements are most likely to be applicable. If you would like to learn more - we remain at your disposal!

Ernst & Young LLP

EY | Building a better working world

EY exists to build a better working world, helping to create long-term value for clients, people and society and build trust in the capital markets.

Enabled by data and technology, diverse EY teams in over 150 countries provide trust through assurance and help clients grow, transform and operate.

Working across assurance, consulting, law, strategy, tax and transactions, EY teams ask better questions to find new answers for the complex issues facing our world today.

EY refers to the global organization, and may refer to one or more, of the member firms of Ernst & Young Global Limited, each of which is a separate legal entity. Ernst & Young Global Limited, a UK company limited by guarantee, does not provide services to clients. Information about how EY collects and uses personal data and a description of the rights individuals have under data protection legislation are available via ey.com/privacy. EYG member firms do not practice law where prohibited by local laws. For more information about our organization, please visit ey.com.

Ey.com