ICTRECHT

Cheat Sheet

DORA

Learn everything about the new rules in just 1 minute.

Read more

Scope

Objective van DORA

To ensure that the financial sector becomes more resilient to cyber threats.

For whom?

- **Financial entities**

  DORA primarily applies to organisations in the financial sector (“financial entities”). This includes credit institutions, payment institutions, account information service providers, electronic money institutions, investment firms, crypto-asset service providers, central securities depositories, central counterparties, trading venues, trade repositories, managers of alternative investment funds, management companies, data reporting service providers, insurance and reinsurance undertakings, (re) insurance and ancillary insurance intermediaries, institutions for occupational retirement provision, credit rating agencies, administrators of critical benchmarks, crowdfunding service providers and securitisation repositories.

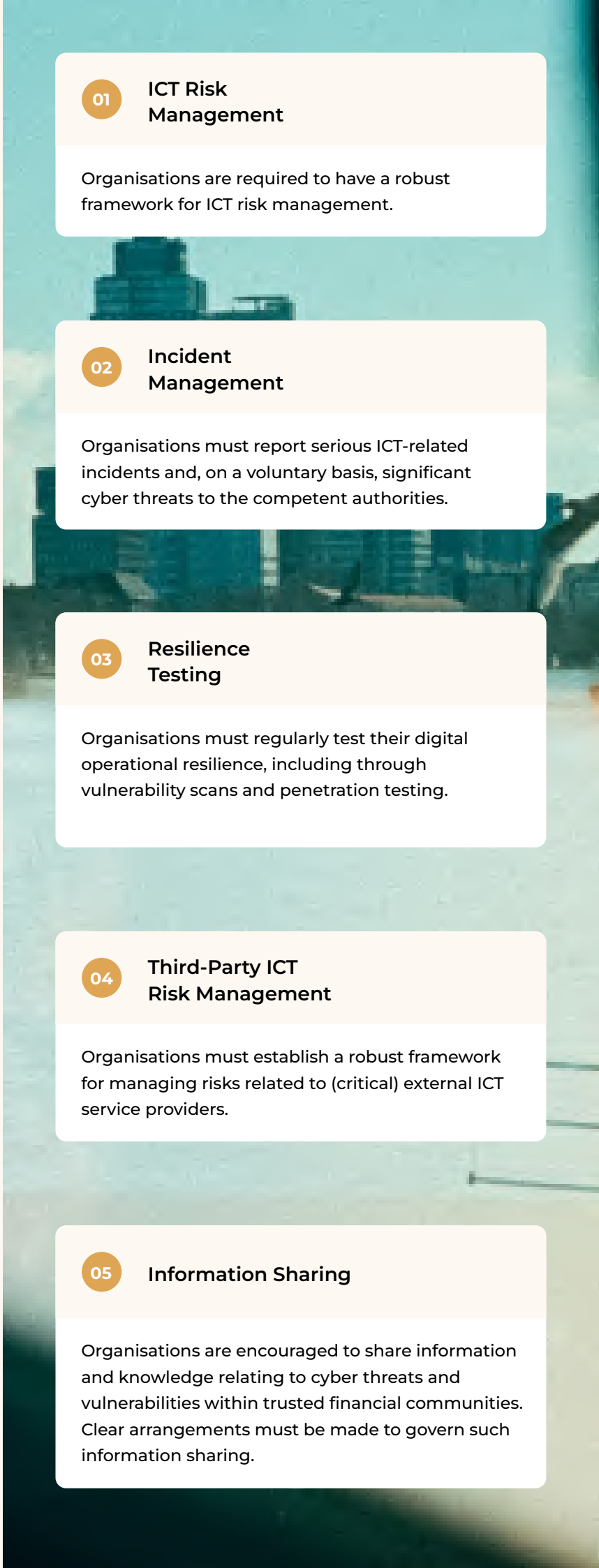
- **Providers of critical ICT services**

  In addition to financial entities, DORA applies to ICT service providers that supply services to financial entities. (with a distinction between providers of critical and non-critical ICT services).

  ICT providers that are of crucial importance to financial institutions (critical ICT service providers) will be subject to direct supervision: this means, among other things, that they must comply with specific standards for ICT risk management and cyber resilience. This represents a significant shift, placing them under a supervisory regime comparable to that

Five pillars

DORA is structured around five pillars. Each pillar is essential to creating a secure and reliable digital financial environment.



01 ICT Risk Management

Organisations are required to have a robust framework for ICT risk management.

02 Incident Management

Organisations must report serious ICT-related incidents and, on a voluntary basis, significant cyber threats to the competent authorities.

03 Resilience Testing

Organisations must regularly test their digital operational resilience, including through vulnerability scans and penetration testing.

04 Third-Party ICT Risk Management

Organisations must establish a robust framework for managing risks related to (critical) external ICT service providers.

05 Information Sharing

Organisations are encouraged to share information and knowledge relating to cyber threats and vulnerabilities within trusted financial communities. Clear arrangements must be made to govern such information sharing.

Sanctions

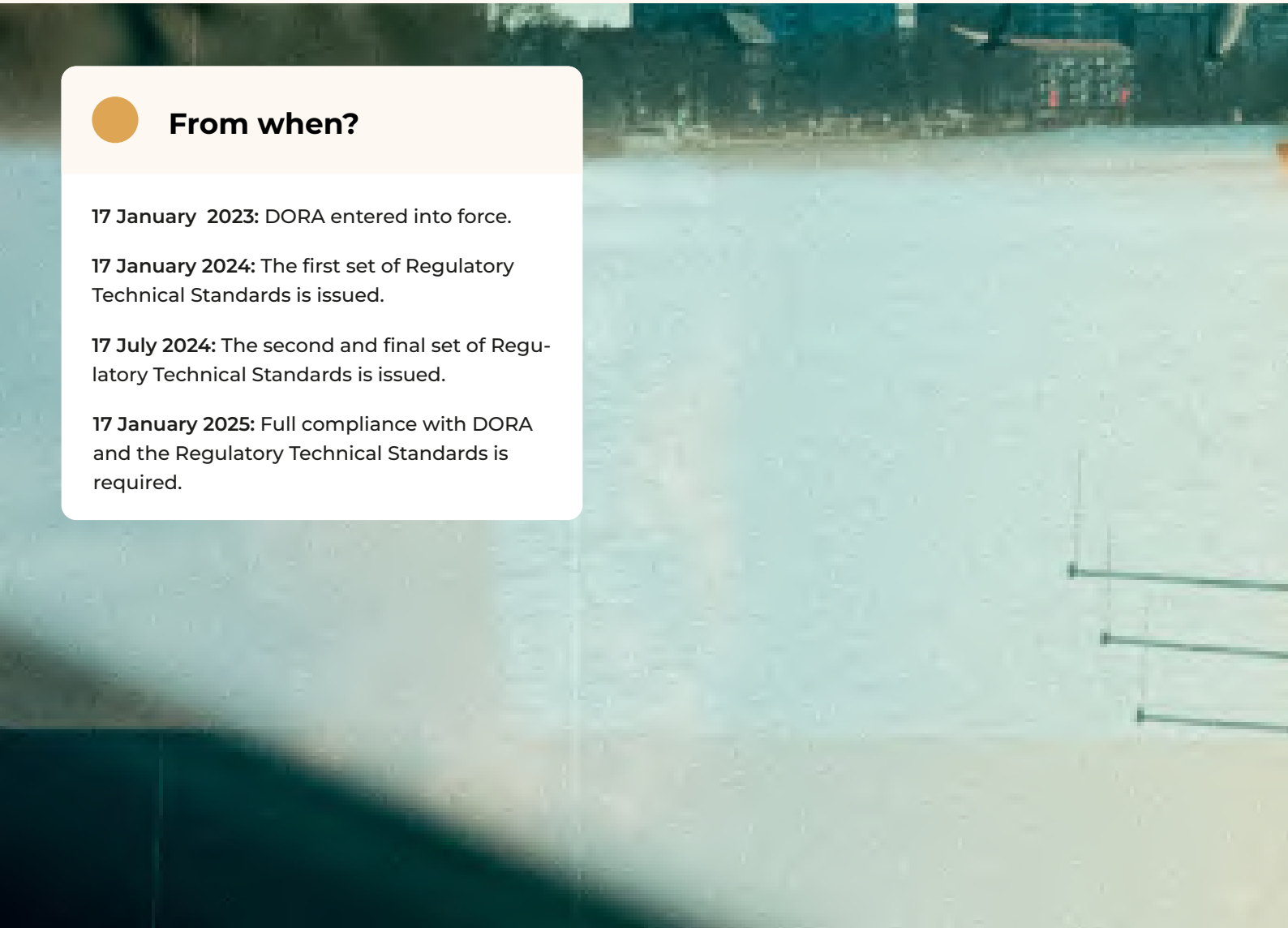
There are significant fines for non-compliance with the obligations arising from DORA. Financial institutions that fail to comply may face various administrative penalties and corrective measures.

For example, De Nederlandsche Bank (DNB) may, among other things:

- Obtain access to documents and data (for example through inspections or investigations)
- Require financial institutions to temporarily or permanently cease certain conduct
- Issue public statements or notifications about the infringement, including the identity of the organisation that committed the infringement
- Impose fines on financial institutions; and
- Require telecommunications services to submit specific overviews of data traffic.

An EU Member State may also decide to impose criminal sanctions for infringements that are subject to criminal penalties under national law.

Critical ICT service providers that do not comply with the rules may be subject to fines in the form of periodic penalty payments of up to 1% of average worldwide daily turnover. These fines may be imposed on a daily basis until compliance is achieved. Due to reputational damage and loss of customer trust, non-compliance may be even more harmful.



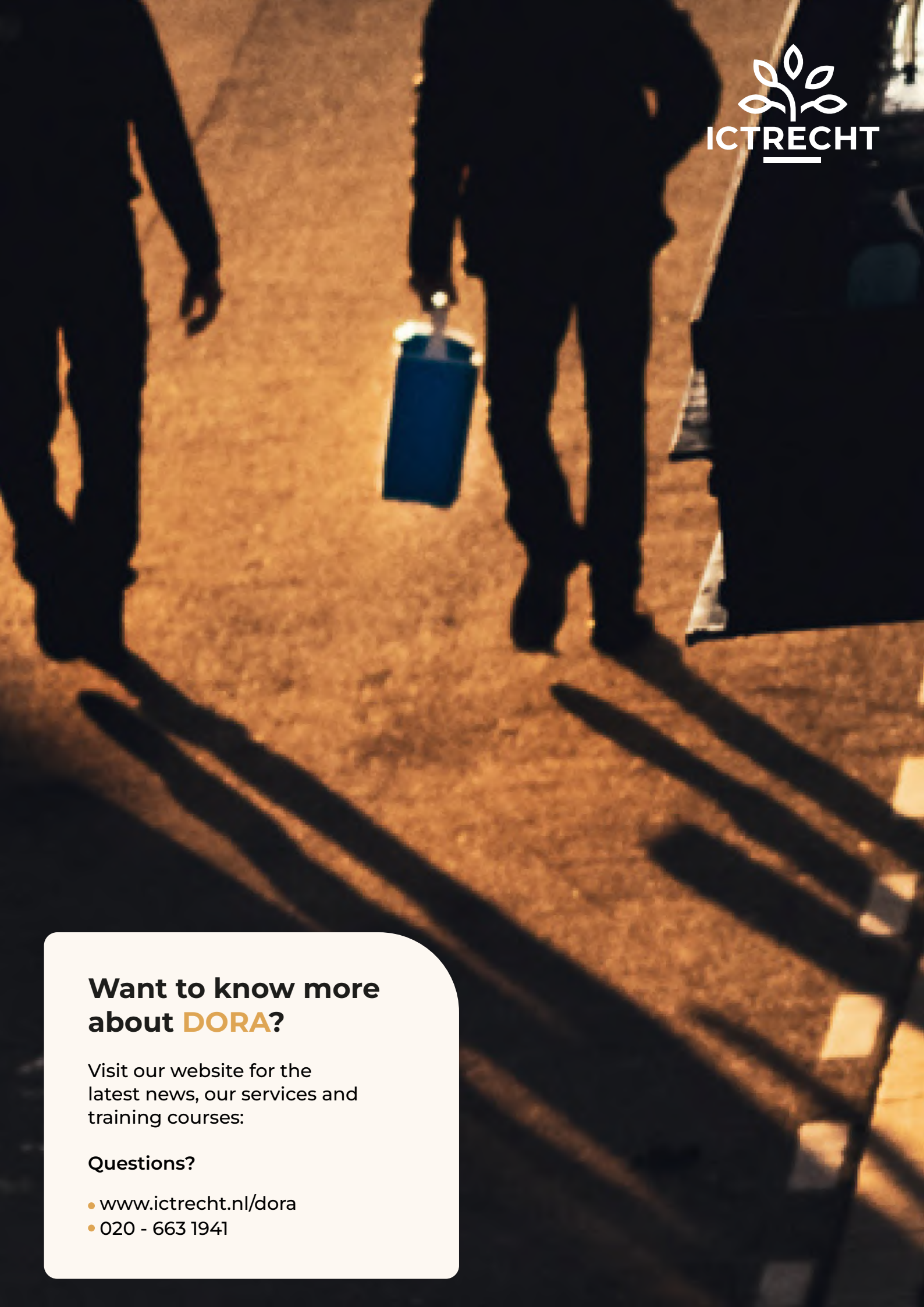
From when?

17 January 2023: DORA entered into force.

17 January 2024: The first set of Regulatory Technical Standards is issued.

17 July 2024: The second and final set of Regulatory Technical Standards is issued.

17 January 2025: Full compliance with DORA and the Regulatory Technical Standards is required.



ICTRECHT

Want to know more about DORA?

Visit our website for the latest news, our services and training courses:

Questions?

- www.ictrecht.nl/dora
- 020 - 663 1941