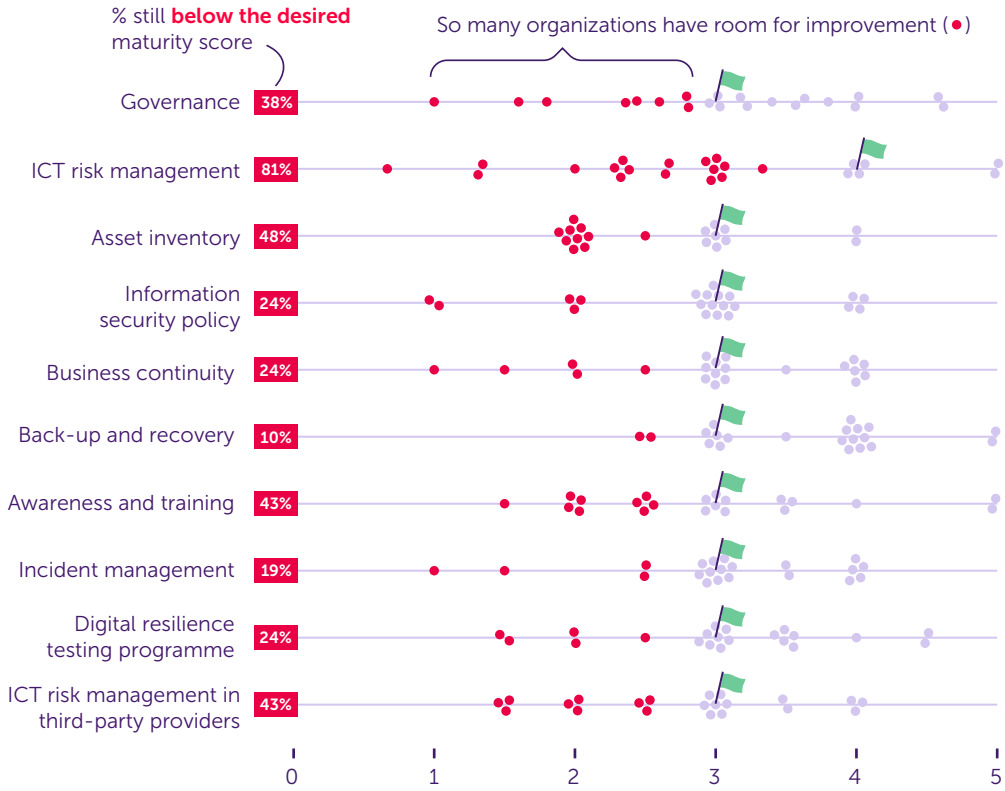
ANALYSIS FACTSHEET

Information security in financial service providers

Summary This factsheet shows the maturity scores for ICT control measures implemented by 21 financial service providers. These scores are based on a self-assessment conducted in 2023 and are linked to ten key DORA-related themes. They show that in many cases the control measures were still below the expected maturity level and that considerable effort is still required before DORA is applicable. The AFM calls on financial service providers to assess their information security in the light of these findings and to improve it where necessary. In addition to these improvements, they should also focus attention on the additional DORA requirements that must be implemented.



Key

Each data point represents one organization.
A total of 21 organizations completed the questionnaire.

- Organizations achieving the maturity score
- Organizations **not** achieving the maturity score

Minimal expectation score

The questionnaire

The questionnaire took the form of a self-assessment. The organizations awarded themselves a maturity score for each control in DNB's Good Practices for Information Security. The AFM then linked the relevant controls in the questionnaire to the legislative articles in DORA. This link reflects our own interpretation and does not cover all requirements set by DORA.

The response scale used runs from 0 to 5:

The control measure ...

0 ... is **non-existent.**
1 ... exists (at least in part), but is **not consistently** implemented.
2 ... exists, but is **not demonstrably** implemented in an effective manner.
3 ... is **demonstrably effective** and is assessed.
4 ... is **demonstrably effective** and is **periodically evaluated** together with the entire system of control measures.
5 ... is **demonstrably effective** and is **continuously improved**.

AFM

ANALYSIS FACTSHEET

Are financial service providers ready for DORA?

The digitalisation of the financial sector and the provision of products and services through online platforms are steadily increasing. This also increases ICT risks, such as cyberattacks or other disruptions. These threats can slow down or even halt the provision of financial services. It is important that financial service providers take sufficient measures to be digitally resilient. Cyber incidents and potential domino effects harm both the continuity of and confidence in the financial sector. The European DORA (Digital Operational Resilience Act) regulation sets requirements for ICT risk management, ICT incidents, periodic digital resilience testing and the control of risks in outsourcing to third-party providers. DORA applies to financial service providers having more than 250 FTEs or turnover of more than €50 million.

Maturity scores for information security in Financial Service Providers

The Dutch Authority for the Financial Markets (AFM) continually monitors the quality of information security in the financial sector. This factsheet shows the maturity scores for ICT control measures implemented by 21 financial service providers. These scores are linked to ten key DORA-related themes. The scores resulted from a 2023 self-assessment on information security based on DNB's Good Practices for Information Security. For the factsheet, the AFM has linked the surveyed control measures to the DORA-related themes. This link reflects our own interpretation and does not cover all requirements set by DORA.

Many organizations (81%) failed to meet the expected level in terms of **ICT risk management**. DORA aims to ensure that financial organizations have better control of ICT risks and are thus more resilient to cyber threats and ICT disruptions. High-quality ICT risk management enables organizations to detect and control risks in a timely and effective manner. DORA contains requirements for both the process side of risk management and its implementation in technical measures. These are further detailed in draft RTS[1] 15, while the simplified ICT risk management framework applicable to a number of exempt organizations is described in draft RTS 16(3).

A number of organizations (38%) could also make further improvements to their **governance** of ICT risk management. DORA includes requirements for a risk-based and periodic evaluation of the ICT risk management by the management body. In addition to this control cycle, clear duties and responsibilities should be assigned for ICT risk management, such as an independent function for the control of ICT risks and an internal audit function.

It also emerged that almost half of the organizations (48%) had no or no complete **ICT asset inventory**. Such an inventory is necessary to identify and maintain the ICT assets that support critical or important business functions. Otherwise it is not possible to adequately monitor possible changes and vulnerabilities in ICT assets.

With regard to **ICT risk management in third-party providers**, almost half (43%) rated themselves as inadequate. Important business functions are increasingly being outsourced to third parties, potentially increasing the supply chain risks. The organizations themselves remain responsible for controlling these supply chain risks. Organizations must analyse the risks, enter into approved agreements on services and conduct appropriate monitoring. The various requirements for controlling ICT risks in outsourced services are detailed in draft RTS 28(1) and 30(5). Draft ITS 28(9) explains the requirements for compiling an outsourcing register.

In order to ensure the resilience of an organisation's services, it is important to establish and implement procedures for ICT business continuity. An essential part of this is establishing **back-up and recovery procedures** in case disruptions nevertheless occur. Most organizations achieved adequate scores here (90%), but it should be borne in mind that DORA imposes additional detailed requirements.

1 Regulatory Technical Standards

The AFM expects financial organizations to evaluate their information security in the light of these findings and to improve it where necessary. In addition to these improvements, they should also focus attention on the additional DORA requirements that must be implemented.

Get ready for DORA

Financial organizations must comply with DORA from 17 January 2025. By way of preparation, organizations need to know in good time where they stand in terms of digital resilience and what further steps they need to take to comply with the requirements set by the regulation. Organizations can use the DORA checklist, among other things, as a starting point for such a gap analysis. The identified gap must then be converted into specific activities that enable a organisation to improve its information security organisation and prepare to meet the requirements of DORA. Among other things, this means adjusting internal policies and procedures, improving control measures and evaluating contracts with third-party providers.

The DORA checklist is a useful tool that gives organizations clarity on various aspects of the policies and procedures required to meet the requirements of DORA. The checklist should be seen as a starting point for organizations to gain an idea of the key reference points for carrying out a full gap analysis. Given the scope of DORA, the checklist is not exhaustive. For the full requirements, see the regulation and associated RTS and ITS.
More information on this can be found on our website.