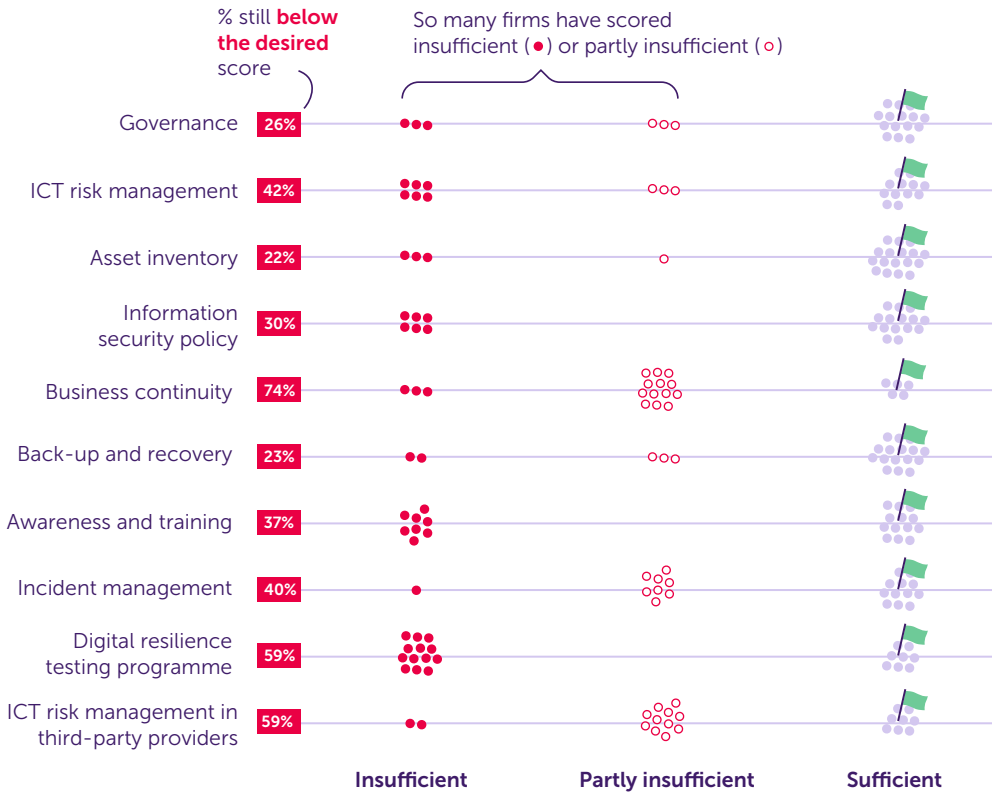
ANALYSIS FACTSHEET

Information security in investment firms

Summary This factsheet shows the scores for ICT control measures in 212 investment firms. These scores are based on the SREP survey conducted in 2023. The relevant questions in this self-assessment are linked to ten key DORA-related themes. The scores show that in many cases the control measures were not yet up to par and that considerable effort is still required before DORA is applicable. The AFM calls on firms 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 ten firms.
A total of 212 firms completed the questionnaire.

- Firms achieving the sufficient score
- Firms partly achieving the sufficient score
- Firms not achieving the sufficient score

Minimal expectation score

The questionnaire

The scores shown are based on the SREP questionnaire. The questionnaire took the form of a self-assessment. AFM subsequently 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.

AFM

ANALYSIS FACTSHEET

Investment firms: 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 investment firms 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 service providers.

Scores for information security in investment firms

The Dutch Authority for the Financial Markets (AFM) continually monitors the quality of information security in the financial sector. This factsheet shows the scores for ICT control measures in 212 investment firms[1]. These scores are linked to ten key DORA-related themes. The scores are based on the SREP (Supervisory Review and Evaluation Process) survey conducted in 2023. For the factsheet, the AFM has linked the relevant SREP questions to the DORA-related themes. This link reflects our own interpretation and does not cover all requirements set by DORA.

Many firms (42%) failed to meet the expected level in terms of **ICT risk management**. DORA aims to ensure that financial firms have better control of ICT risks and are thus more resilient to cyber threats and ICT disruptions. High-quality ICT risk management enables firms 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[2] 15 and 16(3) ICT Risk Management Framework. This also describes the simplified ICT risk management framework that applies, inter alia, to certain investment firms (known as Class 3).

More than half of the firms (59%) did not rate themselves as adequate with regard to **ICT risk management in third-party providers**. More and more firms are outsourcing important business functions to third parties, potentially increasing the supply chain risks. The firms themselves remain responsible for controlling these supply chain risks. Among other things, firms must analyse the ICT risks, enter into contractual agreements on services and conduct appropriate monitoring. Under DORA, the various requirements for the control of ICT risks in outsourced services are further detailed in draft RTS 28(1) and 30(5). Draft ITS[3] 28(9) explains the requirements for compiling an outsourcing register.

Most firms (74%) still have room to improve their **business continuity**. ICT business continuity is important to ensure the stability of a firms services. DORA therefore states that BCM plans must be periodically tested and that the necessary crisis communication arrangements must be in place.

The majority of firms (59%) also failed to achieve adequate scores for their **digital resilience testing programme**. Regular testing gives firms insight into the actual security of their IT environment and enables them to make targeted improvements. DORA therefore requires firms to develop a risk-based programme to test and increase their digital resilience. The content of this programme depends on the identified risk profile of a firm.

In order to ensure the stability of a firm's services, it is important that it establishes and implements procedures for business continuity. An essential part of this is establishing **back-up and recovery procedures** in case disruptions nevertheless occur. Most firms (77%) achieve adequate scores here, but it should be borne in mind that DORA imposes additional detailed requirements.

1 Including firms with an MiFID top up
2 Regulatory Technical Standards
3 Implementing 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 other 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. Entities 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 an activity plan that enables an entity 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.