In Dutch companies, management and supervisory board members carry the responsibility for the general course of affairs of the company they manage or supervise, respectively. While customarily specific tasks and responsibilities are attributed to specific board members, they are ultimately collectively responsible. Consequently, they run the risk of being held liable by the company, creditors and sometimes also shareholders in case of mismanagement to which they can be attributed serious reproach.

With the entry into force of DORA in the financial sector, the responsibility of the 'management body' of financial institutions for the implementation of all arrangements related to ICT risk management is made explicit in an EU regulation. The management body within the meaning of DORA includes the management board and supervisory board or, in a one-tier board, both the executive and non-executive directors. This explicit responsibility has consequences from a regulatory compliance perspective, but may also influence an individual board member's responsibility and potential liability towards other stakeholders.

This blog explores the specific responsibilities of board members under DORA, the implications for board member suitability screening, and how the requirements of DORA may translate into potential board member liability if these are not implemented properly.

With a rapidly evolving digital landscape and a substantial increase in ICT risks threatening the financial sector, it has become critical that board members are aware of the ICT risks that may affect the institution they manage or supervise. These developments have resulted in an increased pressure from legislators and regulators on board members to have sufficient knowledge of ICT risks and their consequences for the institution, and to ensure that appropriate measures are taken to manage these risks within the institution.

In any case, DORA makes absolutely clear that ICT risks should be a board room topic.

DORA is one of the legislative initiatives that has codified the requirements on sound governance and ultimate responsibility of the management body for an institution's ICT risk management. Below, we discuss the specific responsibilities for board members following

from DORA, what consequences DORA may have for the suitability screening of board members, and how the requirements under DORA may translate to a potential liability of board members for a failure to properly manage ICT risks.

Responsibilities of the management body under DORA

As discussed in our blog on the three key aspects of DORA, DORA requires the management body not only to define and approve the ICT risk management framework, but also to oversee its implementation. More specifically, responsibilities of the management body include:

- Implementing and updating the ICT risk management framework
- Setting clear roles and responsibilities for all ICT-related functions
- Being responsible for setting and approving the digital operational resilience strategy, which includes determining appropriate ICT risk tolerance
- Approving, overseeing and periodically reviewing the implementation of the entity's ICT business continuity policy and ICT response and recovery plans
- Approving and periodically reviewing the entity's ICT internal audit plans
- Allocating and periodically reviewing the appropriate budget to fulfil the obligations under DORA
- Approving and periodically reviewing the policy on third-party ICT service providers (at least annually for services supporting critical or important functions)
- Establish reporting lines on a corporate level for ICT services, including third-party services, and major ICT-related incidents
- Regularly review the risks identified in relation to contractual arrangements for the use of ICT services that support critical or important functions
- Actively maintaining sufficient knowledge and skills to understand and assess ICT risks and their impact on the entity's operations, including through regular specific training

In this context, DORA also sets out that financial entities should establish a role to monitor the arrangements entered with third-party ICT service providers for the use of ICT services, or, alternatively, designate a member of senior management to be responsible for overseeing the related risk exposure and relevant documentation.

Suitability screening of board members

In the run-up to DORA, both the ECB and the Dutch regulators (AFM and DNB) have made it clear that sufficient knowledge and skills in ICT risks will be considered as part of the suitability requirements for board members of financial entities. This applies to both prospective and current board members. Although our interpretation of the regulators' expectations is not that every board member should have specific knowledge of ICT risks, every board member should have sufficient knowledge of ICT risks and there should at least be one board member with specific knowledge. Clearly, further knowledge of ICT risk can and, according to DORA, should be obtained through regular training on ICT risks and their impact on the operations of the financial entity.

Ultimately, failure to implement the aforementioned requirements may have consequences for the financial entity from a regulatory compliance perspective. The same applies to individual board members. If individual board members cannot substantiate that they have sufficient

knowledge on ICT risks, there is a risk they will not be deemed to be suitable (anymore) by the competent regulator to perform the function they have been or are envisaged to be appointed to.

Liability for board members for mismanagement of ICT risks

In addition to regulatory compliance concerns, we are seeing an increased focus on the potential liability of board members in the event that ICT risks materialise and cause damages for the institution's stakeholders. While DORA does not specifically address potential liabilities of individual board members, it could be seen that failure to comply with the governance standards set out in DORA in relation to major ICT-related incidents could be a relevant factor under Dutch law in determining whether there has been mismanagement by board members and whether they can be attributed serious reproach for such mismanagement.

It is worth noting that although DORA does not specifically address liability, another EU legislative initiative - NIS2 - does. NIS2 is the EU-wide directive on cybersecurity that applies to various vital sectors. According to Article 20 of NIS2, member states shall ensure that the management bodies of essential and important entities in these sectors approve and oversee the implementation of the prescribed cybersecurity risk management measures, and may be held liable for infringements by these entities of the prescribed risk management requirements. The banking and financial market infrastructures (i.e. trading venues and CCPs) sectors are identified as vital sectors within the scope of NIS2. However, as DORA is a sector-specific act, DORA should prevail over NIS2 and therefore NIS2 does not apply to financial entities that are in scope of DORA (including banks and financial market infrastructures). The European Commission has indicated the same, and more specifically that member states should not apply those provisions of NIS2 to financial entities that are also part of DORA and applicable to those financial entities.

We interpret this statement to cover the provisions on governance and risk management in NIS2. However, NIS2 requires implementation into the laws of member states before it becomes effective and it provides for minimum harmonisation. It therefore remains to be seen how the Dutch legislature will implement NIS2 and whether it will provide a specific ground for liability of board members of banks, trading venues and CCPs for a breach of the risk management requirements in NIS2, notwithstanding the European Commission's statement. If the Dutch legislature would conform to the EC's statement and recognise DORA as prevailing over NIS2, the potential consequences of a failure to implement DORA's governance standards towards stakeholders other than the regulator, would be left to the general principles under Dutch corporate law regarding the responsibility of board members for the general course of affairs of the company they manage or supervise. In any case, board members should not underestimate their responsibility and exposure towards an adequate management of ICT risks.

What this means for you

DORA emphasises the responsibilities of the management body – including the management board and supervisory board for managing ICT risks. Regulators have announced that members of the management body are already being screened on their knowledge of ICT risks. In the slipstream of these developments, we see an increased risk of liability of individual board members if ICT risks are not properly managed.

To address what is expected under DORA and the responsibility imposed on board members, financial institutions should consider the following actions:

- Develop or update digital operational resilience policies, including for business continuity, response and recovery, and internal audit
- Set clear roles and responsibilities within the organisation for implementing the ICT risk management framework
- Determine the entity's ICT risk tolerance and develop a strategy for the use of third-party service providers
- Allocate a budget to meet digital operational resilience needs
- Establish reporting channels to the board to be informed of incidents, critical/important third-party arrangements and material ICT risks, and ensure board discussion and decision-making on these topics
- Set-up a training programme for the board to be regularly informed of ICT risks and their potential impact on the financial entity
- Review and assess the individual and collective 'suitability' of board members in terms of their knowledge of ICT risks

NautaDutilh's Financial Regulatory, Governance and Tech teams would be pleased to discuss these matters further with you.

Contact

Sven Uiterwijk | Financial Law partner
T: +31 6 20 21 05 70
sven.uiterwijk@nautadutilh.com

Anne Fontaine | partner | Brussels
T: +32 496 26 59 75
anne.fontaine@nautadutilh.com

Geert Raaijmakers | Governance partner
T: +31 6 53 68 08 43
geert.raaijmakers@nautadutilh.com

Vincent Wellens | partner | Luxembourg
T: +352 621 15 61 78
vincent.wellens@nautadutilh.com

Joris Willems | Technology partner
T: +31 6 52 05 03 90
joris.willems@nautadutilh.com