DUFAS

Dutch Fund and
Asset Management
Association

info@dufas.nl
www.dufas.nl

Digital Fitness Check: testing the cumulative impact of the EU's digital rules

To	European Commission
From	Dutch Fund and Asset Management Association (DUFAS)
Date	11 March 2026
Subject	Call for Evidence – Digital Fitness Check
Contact details	Manouk Fles, manager regulatory affairs, mf@dufas.nl

Introduction

The Dutch Fund and Asset Management Association (DUFAS) welcomes the European Commission's initiative to conduct a Digital Fitness Check aimed at assessing the cumulative impact of the EU's digital regulatory framework. The asset management sector strongly supports the Union's objectives of enhancing digital resilience, safeguarding market integrity, protecting investors and consumers, and reducing strategic dependencies in an increasingly digital and geopolitically complex environment. At the same time, DUFAS considers this fitness check both timely and necessary, given the rapid expansion of horizontal and sector-specific digital legislation adopted over recent years.

From the perspective of asset managers, the cumulative application of these instruments risks undermining core Better Regulation principles, notably proportionality, legal certainty, coherence and subsidiarity. While each individual legislative act may be justified in isolation, their combined effect has resulted in regulatory layering, overlapping obligations and unclear scoping, particularly where horizontal digital rules interact with lex specialis financial services legislation. This not only increases compliance costs but also diverts resources away from substantive risk management and innovation, without necessarily delivering commensurate gains in resilience or consumer protection.

The Digital Fitness Check therefore provides an important opportunity to identify overlaps, harmonise definitions and improve the overall operability of the EU digital regulatory framework, so that any inconsistencies or inefficiencies can be effectively addressed.

At the same time, regulatory stability and predictability are essential. A rapid succession of new rules or additional obligations makes it difficult for firms to implement legislation effectively and efficiently. It also limits the ability to assess whether the adopted measures achieve their intended objectives and whether the regulatory burden remains proportionate to the expected outcomes. This should be taken into account when introducing new legislation and when amending existing (or yet-to-be implemented) regulatory frameworks.

In light of these considerations, DUFAS calls on the European Commission to place stronger emphasis on harmonisation, proportionality, clear regulatory scoping, regulatory stability and the principle of "report once, use many".

Why the digital fitness check is necessary for asset managers

Asset managers operate in highly digitalised and internationally integrated value chains. Their activities depend on a broad ecosystem of ICT service providers, cloud providers, data vendors and fund administrators.

At the same time, they are subject to multiple sectoral regulatory frameworks, including AIFMD, UCITS and MiFID II. These frameworks are built on the overarching requirement that firms maintain a sound and controlled business operation. This core principle requires firms to adequately manage operational risks and ensure the integrity, reliability and resilience of their operations. In practice, this already encompasses elements such as operational resilience, ICT risk management and the responsible use of technologies such as artificial intelligence.

Alongside these sectoral requirements, asset managers must also comply with a growing number of horizontal digital regulations. In recent years the number of digital regulatory initiatives has increased significantly. Regulations such as DORA and the AI Act have a direct impact on the asset management sector. This creates cumulative effects alongside existing sectoral regulation.

This cumulative effect results in:
- overlapping governance and risk management requirements
- different definitions and classifications for comparable risks
- multiple reporting obligations to different supervisory authorities
- parallel regulatory implementation programs within firms.

Without better coordination across the EU regulatory framework, including between horizontal legislation, between sectoral frameworks, and between horizontal and sector-specific rules, there is a risk that firms will primarily devote resources to managing regulatory complexity rather than to strengthening digital resilience itself.

Sectoral application of horizontal legislation

DUFAS observes that the interaction between horizontal legislation and sector-specific regulation can in practice create uncertainty for financial institutions.

Many horizontal digital regulatory initiatives are not primarily designed for the financial sector and may only apply indirectly to financial institutions, for example in their role as users of digital services or data-driven technologies. In practice, however, firms may still need to consider how such legislation interacts with their applicable regulatory obligations and supervisory expectations.

This can create uncertainty regarding the extent to which horizontal rules should be reflected in sector-specific governance, risk management or outsourcing frameworks. Greater clarity on these interactions would help ensure that firms can assess their obligations in a predictable and proportionate manner.

A related example concerns the Data Act. While the regulation has a horizontal character and asset managers are generally not directly within scope as regulated entities, it forms part of a broader policy discussion on data access and data mobility in the financial sector. National supervisory authorities, including DNB and the AFM, have referred to the Data Act in discussions on improving access to and governance of data, as well as addressing risks related to digital dependencies and concentration in technology providers.

Irrespective of the precise applicability of the Data Act to individual asset managers, the underlying policy questions extend beyond individual firms. Issues such as concentration in cloud infrastructure, data access and broader digital dependencies arise at the level of the financial system as a whole and cannot be effectively addressed by individual institutions alone. Addressing these challenges may therefore require sector-wide or European-level policy approaches.

Greater clarity on how horizontal legislation interacts with sector-specific financial regulation would enhance legal certainty, reduce unintended regulatory overlap and support the effective and proportionate achievement of policy objectives.

Overlapping regulation

Several areas of EU financial and digital regulation contain overlapping requirements that create practical implementation challenges for firms.

A first example concerns incident reporting under DORA, GDPR and NIS2. DORA introduces ICT incident reporting obligations for financial entities, GDPR requires notifications of personal data breaches, and NIS2 establishes reporting duties for significant security incidents. Although these frameworks address related risks, they rely on different definitions of incidents, different reporting thresholds and different reporting deadlines. In practice, a single ICT disruption — for instance involving a cloud service provider — may simultaneously qualify as an ICT incident, a security incident and potentially a personal data breach. Firms must therefore conduct several internal assessments and submit separate notifications to different authorities. A possible improvement would be to harmonise definitions and enable a single incident reporting process that can be shared across relevant supervisory authorities. The proposal to designate ENISA as a single entry point for meeting the incident reporting requirements of multiple legislative acts could help address overlapping reporting obligations. However, such centralisation would only be effective if accompanied by greater alignment of definitions, thresholds and reporting templates across frameworks, enabling firms to submit a single report that can be shared among the relevant supervisory authorities.

A second example relates to DORA ICT registers and existing outsourcing registers. DORA requires financial entities to maintain a register of information on ICT third-party providers, while outsourcing registers already exist under frameworks such as MiFID II, AIFMD and UCITS. Much of the underlying information contained in these registers is similar, yet the reporting fields and formats differ. As a result, asset managers often maintain multiple registers for the same service providers, creating unnecessary administrative burdens and additional reconciliation processes. A harmonised EU register model with standardised data fields could significantly reduce duplication.

A third area of overlap arises between DORA resilience testing and existing IT assurance frameworks. DORA requires financial entities to conduct digital operational resilience testing, while institutions and ICT providers are already subject to various IT audit and assurance frameworks and frequently rely on third-party assurance reports, such as SOC reports. These mechanisms largely aim to demonstrate similar outcomes — namely the resilience and security of ICT systems.
In practice, however, ICT providers and financial institutions are often confronted with multiple audit requests covering the same systems. Different financial entities may request similar information or testing activities, creating a high volume of overlapping assurance requests for ICT providers. At the same time, individual financial institutions are not always in a position to obtain bespoke audits or testing from large ICT providers that operate shared infrastructure and services at global scale. In these cases, assurance is typically organised through standardised third-party assurance mechanisms that can be relied upon by multiple clients. Recognising and appropriately relying on such existing assurance mechanisms could help reduce unnecessary duplication while reflecting the practical realities of the ICT services market. This would support effective oversight of ICT risks without creating disproportionate audit and testing burdens for either financial institutions or ICT providers..

Another example concerns outsourcing frameworks and DORA third-party risk management requirements. Existing outsourcing regimes under MiFID II, AIFMD and UCITS already require risk assessments, contractual safeguards and monitoring arrangements. DORA introduces additional requirements for the management of ICT third-party risks that overlap with these existing frameworks. Consequently, firms frequently need(ed) to renegotiate existing outsourcing contracts in order to incorporate additional DORA clauses, even where similar safeguards are/were already present. The development of harmonised contractual clauses that apply across regulatory frameworks could reduce this duplication.

A further example involves the interaction between the AI Act and existing financial governance frameworks. The AI Act introduces governance and risk management requirements for AI systems, while ICT risk management obligations already exist under DORA and sectoral governance rules under MiFID II, AIFMD and UCITS. Many AI systems used in financial services are therefore already covered by existing IT governance and model risk management frameworks. Without further clarification, firms may be required to establish additional governance structures and documentation layers on top of existing arrangements. To mitigate this risk, the implementation of the AI Act should be aligned more closely with existing financial regulation. In particular, Recital 158 of the AI Act could be clarified and expanded to ensure better coordination with sector-specific rules across a broader range of financial entities, including asset managers.

Finally, DORA and NIS2 may overlap within group structures. DORA applies directly to financial entities, while certain entities within the same corporate group may fall under NIS2. This can lead to situations where different parts of the same group are subject to different regulatory regimes addressing similar risks. In practice, many groups implement DORA requirements across the entire organisation to ensure consistency, while NIS2 may still impose additional obligations on specific entities. Improved coordination and clearer scoping between DORA and NIS2 could help reduce these complexities.

Compliance burden and ongoing reporting requirements
Asset managers are currently required to comply with several digital regulatory frameworks simultaneously. This includes both the implementation of new regulatory requirements and the ongoing compliance with existing obligations, which together create a significant operational and administrative burden.

In particular under DORA firms face substantial ongoing compliance requirements related to:

- incident reporting obligations
- the maintenance of ICT asset registers
- oversight and monitoring of third-party ICT service providers.

While these requirements play an important role in strengthening the digital resilience of the financial sector, firms report that the associated reporting processes and governance requirements can be resource-intensive on a continuous basis.
Certain adjustments could help reduce unnecessary administrative burden while preserving supervisory effectiveness. In particular, consideration could be given to:

- reducing the number of reporting fields where possible;
- extending reporting deadlines where operationally feasible;
- ensuring that reporting obligations are triggered only for incidents of genuine critical relevance.

In addition, asset managers in the Netherlands currently report similar information to multiple supervisory authorities through different reporting channels. For example, incident reporting, outsourcing information and ICT risk data are often submitted through separate templates and systems.

A “one-stop-shop” reporting approach, where information is submitted once and subsequently shared between relevant authorities, could significantly improve reporting efficiency and reduce duplication for firms without reducing supervisory insight.

Implementation and timing of regulatory measures

Effective implementation of digital resilience requirements depends to a large extent on the timely availability of implementing measures and supervisory guidance.

Where regulatory technical standards (RTS/ITS), Level 2 measures or interpretative guidance become available late in the implementation process, or even after the applicable date, firms may need to redesign internal

systems, adjust governance frameworks and renegotiate contracts with service providers. This can result in additional implementation costs and increased operational complexity.

Ensuring the timely publication of implementing rules and providing consistent supervisory guidance would therefore significantly facilitate implementation efforts and allow firms to plan regulatory changes in a more efficient and predictable manner.

Conclusion

DUFAS welcomes the European Commission's initiative to assess the cumulative impact of EU digital legislation. A well-aligned, proportionate and operationally workable regulatory framework is essential to support both the resilience and the competitiveness of the European financial sector.

In particular, greater coordination across EU digital rules, including clearer scoping between horizontal and sector-specific legislation, improved alignment between initiatives, and greater harmonisation of definitions, reporting requirements and operational obligations, would help reduce unnecessary complexity while maintaining strong safeguards for digital resilience.

At the same time, proportionality, regulatory stability and sufficient implementation timelines remain important to ensure that firms can implement new requirements effectively. Timely publication of level-2 measures, technical standards and supervisory guidance is equally critical to avoid unnecessary implementation costs, including those arising from re-work or duplicated implementation efforts, and to reduce regulatory uncertainty.

Overall, a coherent and predictable regulatory framework will enable firms to focus resources on strengthening digital resilience, innovation and the safe use of new technologies, thereby supporting the broader objectives of the EU's digital and financial policy agenda.