

ICT recovery in the asset management sector

In short – The risk of ICT disruptions and failures is increasing. Therefore, it is important that financial institutions can restore their ICT quickly and effectively. This ability to get systems, data, and processes operational again after a disruption or failure is known as ICT recovery. The AFM has investigated how five large institutional asset managers have set up their ICT recovery and how well they are prepared to restore ICT after a disruption or failure. The AFM asks all asset managers to study the points of attention in the report and address them where necessary.

Summary

Financial institutions are increasingly reliant on ICT for their service delivery. At the same time, risks are rising due to factors such as cyberattacks, geopolitical tensions, and evolving artificial intelligence (AI) threats. AI can, for instance, be used to detect and exploit system vulnerabilities more quickly. To address these risks consistently across the European Union, the Digital Operational Resilience Act (DORA) came into full effect in January 2025. DORA imposes requirements on financial institutions—including asset managers—to strengthen their digital resilience.

Digital resilience has long been a key supervisory priority. Financial institutions must not only take measures to prevent ICT disruptions but also be capable of rapidly restoring ICT services if systems fail. The set of processes, measures, and arrangements designed to bring systems, data, and services back into operation following a disruption or failure is known as ICT recovery. To gain greater insight into how ICT recovery is structured, an exploratory review was conducted among several large institutional asset managers.

The review reveals that, broadly speaking, these asset managers are prepared for ICT failure. However, the AFM has identified some points of attention that could lead to more effective ICT recovery arrangements:

- Ensure consistent identification and classification of (critical) functions;
- Establish recovery objectives at business function level;
- Align your ICT service provider contracts with your own recovery requirements;
- Test recovery objectives against various extreme scenarios.

Asset managers are asked to review these points and implement improvements where necessary.

Table of Contents

Summary	2
Table of Contents	3
1. DORA and components of ICT recovery	4
2. Background of the exploratory review	5
3. Points of attention for ICT recovery	6
Point of attention 1: Ensure consistent identification and classification of (critical) functions	6
Point of attention 2: Define recovery objectives for functions	6
Point of attention 3: Align your recovery requirements with ICT service providers contracts	6
Point of attention 4: Take various extreme scenarios into account when testing recovery objectives	7
4. Conclusion	8
Appendix 1 Relevant articles	9
Appendix 2 Definitions	10

1. DORA and components of ICT recovery

DORA aims to strengthen the digital resilience of financial institutions. It focuses primarily on measures to minimise risks associated with ICT disruptions and failures at financial institutions. This may include failures caused by cyberattacks, major incidents and human error. Key elements include requirements regarding business continuity, incident response, and ICT recovery following disruptions and failures such as system outages.

DORA requires financial institutions to establish and document various components of their ICT recovery processes. The most important components are outlined below:

- **Business Impact Analysis (BIA):** An analysis must be conducted to assess the impact of business disruptions on the financial institution. The BIA takes into account the critical nature of identified and mapped functions, support processes, third-party dependencies, and information assets, as well as their interdependencies;
- **Recovery objectives:** Under DORA, these refer to the Recovery Time Objective (RTO—the maximum acceptable recovery time) and the Recovery Point Objective (RPO—the maximum acceptable data loss, expressed in terms of time) for specific functions. Financial institutions determine these recovery objectives for each function. In doing so, they take into account the consequences of disruptions and the relevant dependencies identified in the BIA;
- **ICT response and recovery plan (ICT recovery plan):** In this document, a financial institution outlines, for each relevant function or ICT asset, the measures required to restore the situation following an ICT failure. This includes, identifying which processes must be restored, the order of recovery, measures such as redundancy arrangements, alternative sites and backups, as well as governance. The ICT recovery plan must be structured in such a way that the established recovery objectives can be met;
- **(ICT) business continuity plan (BCP):** In this document, the financial institution describes the measures that enable it to continue operations during ICT disruptions or failures. Examples include alternative working methods;
- **Communication plan:** In the event of disruptions or failure, it is essential to have a strategy for communication with both internal and external stakeholders. This must be documented in a plan specifying clear roles, responsibilities, and procedures and the approach should depend on the severity of the disruption or failure;
- **Testing:** Periodic testing provides insight into whether the ICT systems supporting specific functions can actually be restored within the established recovery objectives and whether employees are familiar with their tasks. The results of these tests are used to further improve the ICT recovery arrangements.

2. Background of the exploratory review

For this exploratory review into ICT recovery, five institutional asset managers have participated in the review. The review is based on document research and interviews with these institutions. The aim was to gain insight into how well prepared they are for ICT failure and the subsequent recovery. For effective ICT recovery, it is important that institutions have a clear picture of their business functions, information assets and ICT assets, including their interdependencies. Recovery objectives must also be established. These form the basis for measures that support the continuity of service delivery and contribute to a rapid recovery following an ICT failure.

The points of attention in this report are largely based on general principles for ICT recovery and are therefore, in principle, relevant to all asset managers. The extent to which institutions must elaborate on these points of attention depends on their nature, scope, and complexity. Proportionality is not discussed further in this report.

3. Points of attention for ICT recovery

The asset managers surveyed are generally prepared for ICT failures. At the same time, the review shows that improvements are possible regarding a number of aspects of ICT recovery. The four points of attention in this report provide guidance for further strengthening digital resilience. Asset managers are asked to address these points where necessary.

Point of attention 1: Ensure consistent identification and classification of (critical) functions

Financial institutions must identify, classify, and document all functions supported by ICT. This also includes classifying functions into critical and non-critical functions. Prolonged failure of a critical function can lead to unacceptable damage for the financial institution itself, counterparties, and/or customers. To prevent such damage, strict control measures must be in place for critical functions that are proportionate to the recovery objectives, including control measures for ICT business continuity. All asset managers in the review did have an overview of critical functions. However, in the documentation assessed by the AFM, the identification and classification of these functions did not in all cases correspond to the classification used by the asset managers in the DORA register of information in 2026.

The AFM points out that consistency in this regard is important. Inconsistencies in defining critical functions can lead to functions unjustly being classified as non-critical. Specifically for ICT business continuity, implemented control measures may prove insufficient in the event of a serious disruption, resulting in insufficient recovery and/or excessive data loss.

Point of attention 2: Define recovery objectives for functions

Financial institutions must establish recovery objectives. Recovery objectives indicate when and under what conditions a function must be able to become operational again. In its review, the AFM often observed that recovery targets are established for individual ICT assets, but not separately for the functions supported by those assets.

It is important to establish recovery targets for functions for several reasons. Firstly, asset managers need to have insight into how quickly functions can be restored following the failure of one or more ICT assets or services, and whether this meets the function's recovery target. Secondly, it is important to be clear which ICT assets contribute to critical functions. Blind spots regarding which ICT assets are critical can result in insufficiently managed risks related to ICT business continuity.

Point of attention 3: Align your recovery requirements with ICT service providers contracts

Financial institutions outsource many ICT services. Examples include specialised software and cloud providers. Due to this outsourcing, there is often a significant dependency on ICT service providers. Due to the complexity of the ICT organization and the increased risk of cyberattacks, sound agreements with third parties are essential for the financial institution's risk management.

Part of this are the institution's requirements for ICT recovery. When selecting and documenting agreements with ICT service providers, it is therefore important for financial institutions to verify whether the outsourcing aligns with their recovery objectives regarding the function or functions supported by the outsourced ICT. Consider, for example, the time a function may be unavailable before unacceptable damage occurs. Financial institutions must verify whether that objective can also be achieved after the outsourcing. In its investigation, the AFM observed that some asset managers did not explicitly record these recovery objectives in an agreement (including a service level agreement).

Negotiating and documenting requirements with ICT service providers regarding factors relevant to restoring the functions of financial institutions within the recovery objectives is important for managing recovery risks. Particularly in the case of critical functions, the AFM expects financial institutions to include specific sections or KPI's in their contracts with ICT service providers that align with the recovery objectives it has established for the relevant function(s).

Point of attention 4: Take various extreme scenarios into account when testing recovery objectives

Financial institutions must establish recovery objectives that are also achievable in extreme scenarios. The recovery objectives must be included in the recovery plans. Additionally, the recovery plans must mention relevant scenarios that are considered when determining the measures in the recovery plans. In this regard, financial institutions must in any event consider at least nine scenarios prescribed by DORA.

The testing of these recovery plans must be carried out based on test scenarios that simulate potential failures, including an adequate series of severe but plausible scenarios. The tests also include scenarios for switching from primary ICT infrastructure to redundant capacity, backups, and redundant facilities. The AFM notes that all asset managers in the review have a test program in which various scenarios are tested.

The AFM observes differences in the scope and depth of the tests performed. For instance, the transfer from the primary to the secondary data centre was tested in all cases. For the remaining tests, some asset managers focused on the failure of a specific system, with this test being repeated periodically. Other asset managers tested multiple scenarios in which various systems were unavailable.

The AFM expects financial institutions to test recovery plans, including recovery objectives, over the years using a sufficient variety of scenarios. In doing so, it is important that financial institutions consider the scenarios involved in the design of the recovery plan and the outcomes of the risk analysis. The test program must provide sufficient insight into whether critical or important functions can be restored within the established recovery objectives. It is therefore important not only to test whether various functions can recover after a cyberattack, but also whether recovery is possible for other relevant causes of disruptions.

4. Conclusion

DORA focuses on the digital operational resilience of financial institutions. Digital threats are further increasing due to technological and societal developments. The AFM believes it is very important to gain a better understanding of how institutions can restore their ICT after a failure with as little damage as possible. That is why, in addition to a review into ICT risk management the AFM has now also conducted an exploratory review into ICT recovery¹.

Important points of attention are:

- Ensure consistent identification and classification of the (critical) functions within the institution
- Define recovery objectives on functions
- Align your recovery requirements with ICT service providers contracts
- When testing recovery objectives, take various extreme scenarios into account.

The AFM also considers these points relevant for other asset managers and therefore shares them in this report. The points of attention may also be relevant for other financial companies.

The AFM asks asset managers to study the points of attention in the report and address them where necessary.

¹ Refer to [Handelssystemen vragen om scherpere ICT-risicobeheersing onder DORA](#) , aimed at trading venues which includes recommendations that are useful for other types of financial entities.

Appendix 1 Relevant articles

Subject	DORA	Delegated Regulation Risk Management
Definitions	Article 3	-
Consistent identification and classification	Article 8, section 1,3, 4 and 6	Article 4, section 2, subsection b
Recovery objections based on function	Article 12, section 6	Article 24, section 1, subsection b, part ii, point 2
Requirements recovery in third party agreements	Article 30, sections 3 subsection c	-
Testing different extreme scenarios	Article 11, section 6	Article 24, section 2, subsection b, part iv Article 25, section 2, subsection a Article 26, section 2

Appendix 2 Definitions

What is a critical or important function (critical function)? A function the disruption of which would materially impair the financial performance of a financial institution or the soundness or continuity of its services and activities, or the termination or defective or unsuccessful performance of which would materially impair the continuing compliance by a financial institution with the conditions and obligations under its licence or its other obligations under applicable financial services law.

What are recovery objectives? In DORA these consist of an RTO (Recovery Time Objective) and an RPO (Recovery Point Objective).

What is an RTO? The maximum time within which a system, process or service must be restored after a disruption, before unacceptable consequences for the organisation occur.

What is an RPO? The point in time to which data must be restored after a disruption.

What is an ICT service provider? An undertaking that provides ICT services.

What is an ICT service? A digital and data service provided continuously via ICT systems to one or more internal or external users, including hardware as a service and hardware services, including the provision of technical support via software or firmware updates by the hardware provider, with the exception of traditional analog telephone services. Various types of ICT services are listed in Annex III of Delegated Regulation (EU) 2024/2956 on the Information Register.