

PROFESSIONAL
GUIDE DECEMBER 2023

Cybersecurity – DORA Practical Guide



Digital
Operational
Resilience
Act



AFG

CONTENTS

☰	Introduction	1
☰	1. Governance and organisation	3
☰	2. Risk management framework	5
☰	3. Incident categorisation	9
☰	4. Resilience testing	12
☰	5. Third party management	14
☰	6. A final word on sharing	17



AFG wishes to thank the members of the Cybersecurity Working Group who contributed to the drafting of this Guide, and particularly its chairman, Wilfried Lauber (Amundi).

The Cybersecurity Working Group is affiliated with the Ethics and Compliance Committee chaired by Monique Diaz (AXA Investment Managers Paris).

Valentine Bonnet, head of Corporate Governance and Compliance (AFG), coordinated this work.



Introduction

The DORA Regulation (*Digital Operational Resilience Act*) defines a detailed, comprehensive framework on digital operational resilience for financial entities, and therefore applies to asset management companies (AMC).

The regulation, which will come **into force on 17th January 2025**, imposes obligations on financial entities, but also on their digital service providers, which must review their procedures, contracts, mechanisms and tools on a regular basis to ensure information systems security.

■ What is operational resilience?

→ The ability of a financial entity to rebuild, reassure and review its operational capability, integrity and reliability (...) including through disruption.¹

DORA aims to steer the financial sector towards a real maturity that goes beyond each participant's individual operational resilience to strengthen the resilience of the sector as a whole. In addition to the financial actors that will be designated as systemic for the European financial system and other players involved in its implementation, DORA applies to ICT service providers, which will be subject to stringent requirements and a high level of oversight, for the long-term benefit of the sector.

■ What is an ICT service provider?

→ An ICT service provider is an entity that provides an IT service, in the broad sense, whether as a cloud service, a hosted service or internally from your own data centre or infrastructure through software you use inside your organisation/company.. This covers all areas of information technology, including data storage, processing, entry and provision.

This guide aims to be practical and actionable. Each chapter will be divided into four key sections:



Current situation: important points for verifying that you do in fact meet the requirements of DORA, since you have probably already implemented these practices.



What's new: requirements under DORA for which the next steps appear to be within reach.



Challenges: more complex requirements for which AMCs will need to take certain measures.



Keys for the board: these are key points that your board should focus on and which you can use in an elevator pitch.

Note: in this document, the term “board” refers to your management body.

¹) See Art 3.1.

Consideration should be given to five main points:

1. The digital operational resilience strategy,

which defines the AMC's risk management framework, as well as its objectives through its risk appetite.

2. Reporting of cyber incidents and threats,

which entails implementing procedures to detect, classify, manage and report incidents.

3. Digital operational resilience testing,

at least yearly, for systems supporting critical or important functions. These tests, which include ICT service providers, must be considered from two angles:

- ▶ resilience of the systems to attacks
- ▶ resilience of the systems following an attack.

4. Management of risks related to ICT digital service providers

requiring that service providers covering critical or important functions be singled out, third parties be mapped to avoid concentrations, and minimum clauses be included in contracts.

5. Cybersecurity information sharing.

To ensure the overall digital operational resilience of the financial sector, AMCs are encouraged to share information related to cybersecurity.

■ Who is DORA for?

All AMCs!

However, the requirements for an asset manager considered a microenterprise will be reduced significantly².

■ How is DORA applied?

→ The principle of proportionality is the subject of a specific article of DORA: Article 4 states that the measures applicable to entities are “proportionate to their size and overall risk profile, and to the nature, scale and complexity of their services, activities and operations.”

At the time this guide was drafted, it appears that no AMC, regardless of its size, is considered a systemic operator.

■ How does this tie in with the NIS 2 directive?

While both texts are similar in terms of a level of maturity to be achieved, such as by strengthening protection measures and reporting in case of incidents, DORA constitutes *lex specialis*³ for financial entities. Since, in law, a special rule prevails over a general rule, AMCs must focus on applying DORA.

■ Is all information available at this stage?

DORA is scheduled to come into force on 17 January 2025. At this stage, 10 technical standards (RTS/ITS) intended to supplement DORA have not yet been finalised by the European financial supervisory authorities (ESMA, EBA and EIOPA). Additions will be made to this guide as and when they are published.

²) Microenterprises: AMCs with fewer than 10 employees and annual revenue and/or an annual balance sheet total of not more than €2 million will be exempt from certain DORA requirements. ³) Specific rules will prevail over general rules 16.

1. Governance and organisation

In a nutshell

Your board is now fully responsible for implementing the various obligations and deliverables to comply with the act.

DORA gives it a major role in an area where many aspects are already covered by operational and organisational best practices.


It must define, validate and oversee the implementation of the IT risk management framework.

This framework encompasses the IT policies, strategies, procedures and tools related to the AMC's cyber resilience, which we will define in more detail in the various chapters of this document.

Article 5 of DORA defines various obligations, including:

- ▶ explicit validation of security policies,
- ▶ allocation of IT risk management budgets,
- ▶ oversight of the IT control plan,
- ▶ creation of committees and internal reporting channels.

It is essential that your board be regularly informed of the risks related to cybersecurity and their impacts on the AMC's activities.

 **At least once a year, the board must add a presentation by the Information Systems Security Manager to be replaced by Chief Information Security Officer (CISO) to its meeting agenda and provide for additional reporting and monitoring information throughout the year.**



Current situation

AMCs must have security policies as well as human and financial resources allocated to IT risk management.

These resources must be clearly identifiable and even listed separately in the IT budget.

For comparative purposes, the average expenditure on cybersecurity in the financial sector is 5.4% of the IT budget⁴.

It is important to check and, where applicable, supplement the content of your current procedures related to security policies. The board must be informed of risks faced by the company and the measures taken to minimise them.



We recommend that the board review these risks at least annually.



What's new

- AMCs must establish: a *“role to monitor their arrangements concluded with ICT third-party service providers”* or *“designate a member of senior management as responsible for overseeing the related risk exposure and documentation”*.
- **Boards of AMCs bear the “ultimate responsibility”⁶ for managing IT risks** and must define the roles and responsibilities related to cyber resilience; in particular, your board must:
 - ▶ **Approve and periodically review the IT internal audit plans** and material modifications to them⁷.
 - ▶ **Review and approve the digital operational resilience policy⁸ and the IT business continuity policy⁹.**
 - ▶ Put in place reporting **channels enabling it to be informed of arrangements concluded with ICT service providers, planned material changes regarding such service providers, and the resulting risks¹⁰.**

4) Wavestone - Cybersecurity Benchmark 2023. 5) Art 5.3. 6) Art 5.2 (a). 7) Art 5.2 (f). 8) Art 5.2 (d). 9) Art 5.2 (e).



AFG recommends that your board regularly validate all the aforementioned points, including the list of critical or important service providers.

- ▶ **“Regularly follow”¹⁰ specific training** to better understand and assess IT risks and their impacts on the AMC's operations.



AFG recommends that such awareness be provided at least annually.



Challenges

Supporting the board's understanding of cyber risk and IT resilience poses several challenges, such as the minimum annual recurrence of the awareness and regular reporting. Indeed, the right balance must be set in order for the board to get value from the various consultation/reporting it will get through the year in addition of strategy definition and decision making.



In terms of content during presentations at board meetings, AFG recommends that you:

- ▶ **be very specific and use actual examples in line with your board's activity and receptivity**
- ▶ **make the topic a common theme at successive board meetings so that it is reviewed continuously and not sporadically.**



In terms of reporting, the board expects you to be consulted for actions and decisions. Be careful to not fall into “all green” reporting that does not highlight the points on which the board should focus.



Key for the board

Given the risk of large-scale attacks, the board must put in place an efficient organisation responsible for IT risks. As Vincent Strubel, director of the French Cybersecurity Agency (ANSSI), fears: *“We must be prepared for the big event, when whole segments of our society are attacked simultaneously”¹².*

Educating the board, particularly by presenting the measures described in this guide, is an essential first step towards ensuring your gradual compliance with the DORA Regulation.



Key deliverables

Given the requirement that AMCs formalise their operational resilience governance, we recommend that you keep evidence of:

- ▶ reporting of information and meetings with the board where the company's cyber resilience strategy features prominently on the agenda;
- ▶ approval by the board of the policies related to risk management (see chapter 2);
- ▶ training received by the board (which may be included on the agenda).

¹⁰) Art 5.2 (h). ¹¹) Art 5.4. ¹²) Opening address by Vincent Strubel at the Assises de la sécurité des systèmes d'information (information systems security conference) in Monaco, 11 October 2023.

2. Risk management framework

■ In a nutshell

The risk management framework set out in DORA requires detailed documentation as described below.

This framework, which is based on an overall digital operational resilience strategy, encompasses the various policies, strategies and measures that you implement to ensure the security of your information systems.



Many areas have long been the subject of various frameworks and best practice guides, such as those published by AFG. Up to now, however, they have been applied in varying degrees; what is new in DORA is that it integrates them to ensure regulatory compliance.



Current situation

- AMCs must ensure **appropriate segregation of IT** management functions, control functions and internal audit functions¹³.
- Your AMC must have a **digital resilience strategy**¹⁴ that describes how the **IT risk management framework is implemented**¹⁵.
- Also required are procedures for producing various deliverables (strategies, policies, protocols) and the formalisation of IT tools used to secure the IT infrastructure and minimise risks.

Note: this risk management framework must be reviewed at least once a year, and upon the occurrence of major IT-related incidents¹⁶.

¹³⁾ Art 6.4. ¹⁴⁾ Art 6.9. ¹⁵⁾ Art 6.1. ¹⁶⁾ Art 6.5.



What's new

DORA incorporates all the requirements to be formalised. Your IT risk management framework must determine¹⁷:

- ▶ your **IT risk tolerance level**, in other words your risk appetite which, depending on the size and complexity of your AMC, will be used to determine a strategy for staying below this risk appetite;
- ▶ **clear cybersecurity objectives**, to be shared with your board;
- ▶ the mechanisms put in place to **prevent incidents** and **protect against their impact**;
- ▶ a **holistic multi-vendor strategy**;
- ▶ **oversight of major IT-related incidents**: volume, objective, improvement plan and effectiveness of preventive measures;
- ▶ the procedure for implementing:
 - **digital operational resilience testing**
 - ability to react to a cyber incident
 - penetration testing: ability to withstand a cyber incident
- ▶ a **communication strategy in case of incidents**.

¹⁷) Art 6.8.

DORA stipulates that your risk management must be built on five components:

1. RISK IDENTIFICATION

Identify, classify, document and review, at least yearly, all IT-related business functions, **information assets**¹⁸ and **ICT assets**¹⁹: hidden behind this terminology are your data and the computer systems, applications and software and resources that support them. DORA requires a mapping of interconnections that is different from the traditional mapping currently produced by team or by topic. The mapping must be comprehensive and needs to involve multiple teams, for example between IT teams, purchasing teams and the DPO for third party management.

2. PROTECTION AND PREVENTION

The risk management framework must be proportionate to the size and risk profile of the AMC and contain²⁰:

- ▶ an information security policy covering the AMC's resilience;
- ▶ policies, procedures and controls on network and infrastructure management, access, strong authentication, IT change management, and patch and update management;
- ▶ awareness training and campaigns for the board and employees.

3. DETECTION

AMCs must have in place regularly tested mechanisms²¹ to promptly detect anomalous activities²².

4. RESPONSE

The AMC must set up a “crisis management function” to manage internal and external²³ communications according to a defined and documented crisis communication plan²⁴ “which enables responsible disclosure”.

Tests must be performed at least once a year²⁵ and include cyber-attack scenarios. DORA places special emphasis on tests relating to outsourced or contracted critical or important functions²⁶.

AMCs must maintain an easily accessible register of activities²⁷, including an IT business continuity policy²⁸ that is part of the operational business continuity policy.

5. RECOVERY

In addition, entities must develop a post-IT incident recovery plan that is also subject to an independent audit review and tested at least yearly.



Challenges



For the risk identification component, AFG recommends that you prioritise mapping of the IS.

What was simply a best practice until now (analysed by AFG via questionnaires carried out between 2018 and 2022 which showed little change in IS mapping) is now a requirement.

Its existence and completeness will no doubt be subject to controls by the authorities.

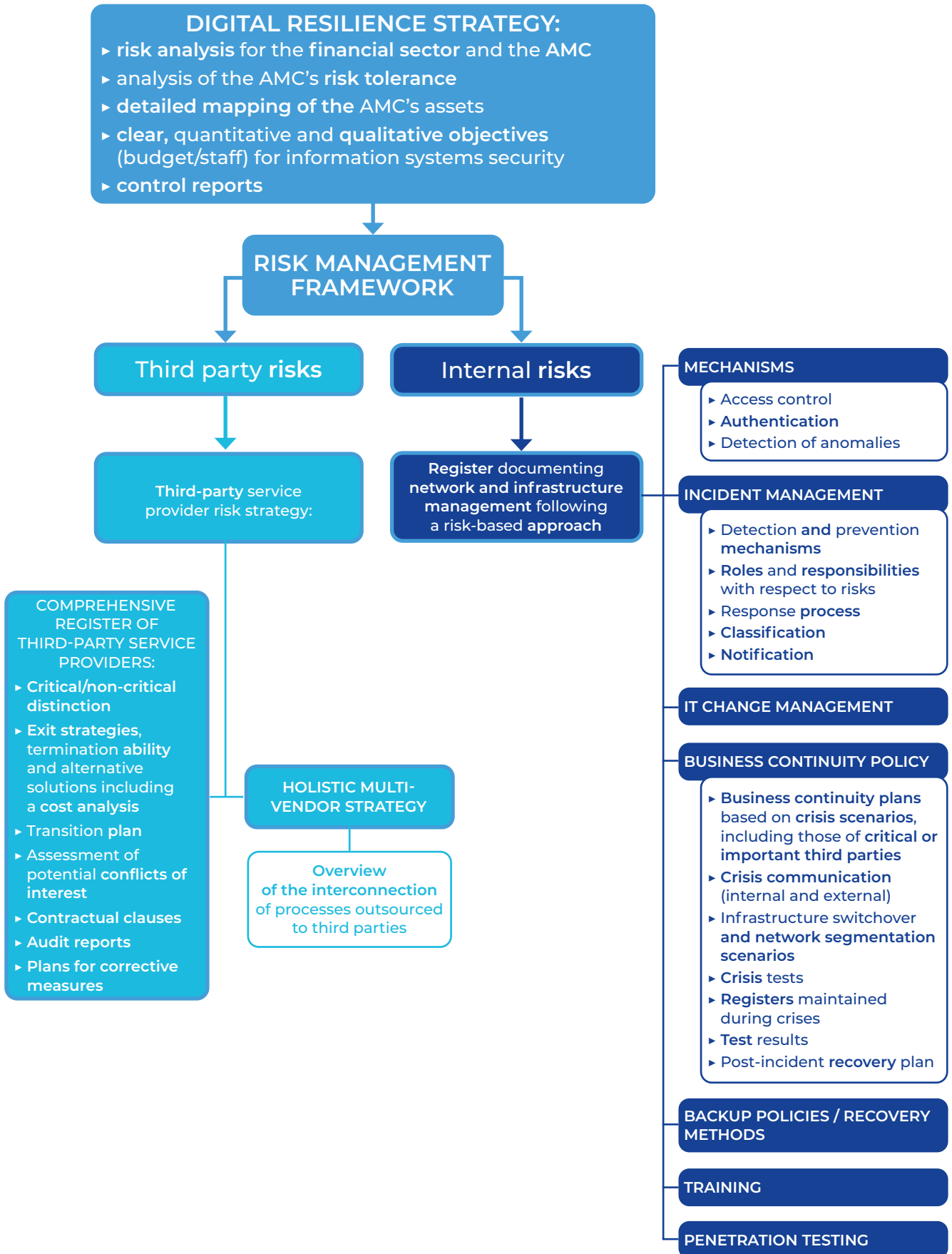
The aim is to have an overview of the business services linking the infrastructure component, applications, software, data and ICT service providers.

¹⁸) Art 3.6: collection of information, either tangible or intangible, that is worth protecting. ¹⁹) Art 3.7: a software or hardware asset in the network and information systems used by the financial entity. ²⁰) Art 9.4. ²¹) Art 10.1 and Art 25. ²²) Art 17. ²³) Art 11.7. ²⁴) Art 11.1. ²⁵) Art 11.7. ²⁶) Art 14. ²⁷) Art 11.6. ²⁸) Art 11.4.



Key deliverables

Mapping of expected deliverables under DORA:



3. Incident categorisation

In a nutshell

DORA strengthens the requirements relating to incident management through:

- ▶ the introduction of a unified and consolidated format at European level. This consolidation should allow a comprehensive view of incidents and the detection of systemic risks at European level;
- ▶ prompt notifications to the board, the AMC's clients and the competent authorities;
- ▶ incident categorisation based on a DORA-specific classification will be key and must be put in place as part of a procedure that includes, where applicable, critical and important subcontractors.



To achieve this objective, incident classification and monitoring will need to be enhanced. This can be made easier by using tools that include specific criteria.

The progress made in implementing DORA at each AMC will depend in particular on:

- ▶ the company's maturity in terms of its incident management system;
- ▶ the implementation of a response plan (communication, risk scenario);
- ▶ the desired level of detail;
- ▶ its ability to monitor alerts and oversee action plans;
- ▶ the implementation of cyber threat monitoring (optional).



Current situation

Incident management, a process that already exists at AMCs, entails:

- ▶ verifying that your incident management organisation is operational;
- ▶ implementing a reference list of critical processes and key subcontractors: basic response plans, at a minimum, must be put in place;
- ▶ implementing an IT incident management process to detect, manage and report incidents²⁹. Incidents must be tracked, logged, categorised, prioritised and classified according to their priority and severity and to the criticality of the services impacted³⁰.



What's new

DORA introduces criteria to determine which incidents should be classified as critical.

These criteria will be further clarified in RTS published by the ESAs. There will also be technical standards regarding the harmonisation of reporting content and formal templates.

- **Incident classification** criteria include³¹:
 - ▶ the impact on the operational continuity of financial services;
 - ▶ the duration of the incident;
 - ▶ the change and geographical distribution of the areas affected by the incident;
 - ▶ data security, particularly sensitive data;
 - ▶ the criticality of the services affected;
 - ▶ the financial stability or continuity of the financial system.

²⁹) Art 17.1. ³⁰) Art 17.3. ³¹) Art 17.1 (Article 18 defines incident classification criteria, which will be clarified by regulatory technical standards).



- **Major incidents** must be reported to:
 - ▶ the board³², including post-incident reviews and measures to be implemented;
 - ▶ service users and clients if the incident may have an impact on their financial or operational interests³³;
 - ▶ **the authorities, in three phases:**
 - **an immediate initial notification**
 - **an intermediate report within not more than one week**
 - **a final report when the root cause analysis has been completed³⁴.**



Challenges



- DORA requires that major incidents be reported to your clients, board and authorities with full transparency and a high level of detail.

AMCs must inform their authority as to whether the incident was reported to other competent national authorities or relevant bodies, and provide information about possible cooperation with such entities.

After the initial notification, made **as quickly as possible**, regular reports must be sent throughout the incident.

The level of information to be provided includes:

- ▶ a description of its impact;
- ▶ the presumed causes;
- ▶ the corrective measures taken or planned to mitigate the effects of the incident and prevent its recurrence in the future;
- ▶ relevant data regarding the affected systems and services;
- ▶ the status of the incident, including the estimated time needed to fully resolve it.



- AMCs must consider how their communication and response plan is organised in case of an incident.

You should begin to think about your incident management organisation.

Your procedures must include ways in which information about major incidents is classified, collected and centralised.

In addition, RTS will provide clarifications on the information to be provided in terms of:

- ▶ the level of detail, deadlines, reporting threshold and reporting format;
- ▶ incident management system requirements;
- ▶ alert management requirements.

These clarifications should allow harmonisation of the criteria and reporting with other existing requirements (CNIL, ECB, etc.).

Note: threats can also be reported on a voluntary basis by implementing technology and cyber watch (as do large groups via Computer Emergency Response Teams – CERT).

³²⁾ Art 18.1. ³³⁾ Art 19.3. ³⁴⁾ Art 19.4.



Key for the board



Key performance indicators (KPI) should be used to monitor incidents along with a classification of their severity.

Be specific! Your board will be able to take action based on the reporting of major incidents brought to its attention.

By being fully involved in incident management, your board will have greater visibility.

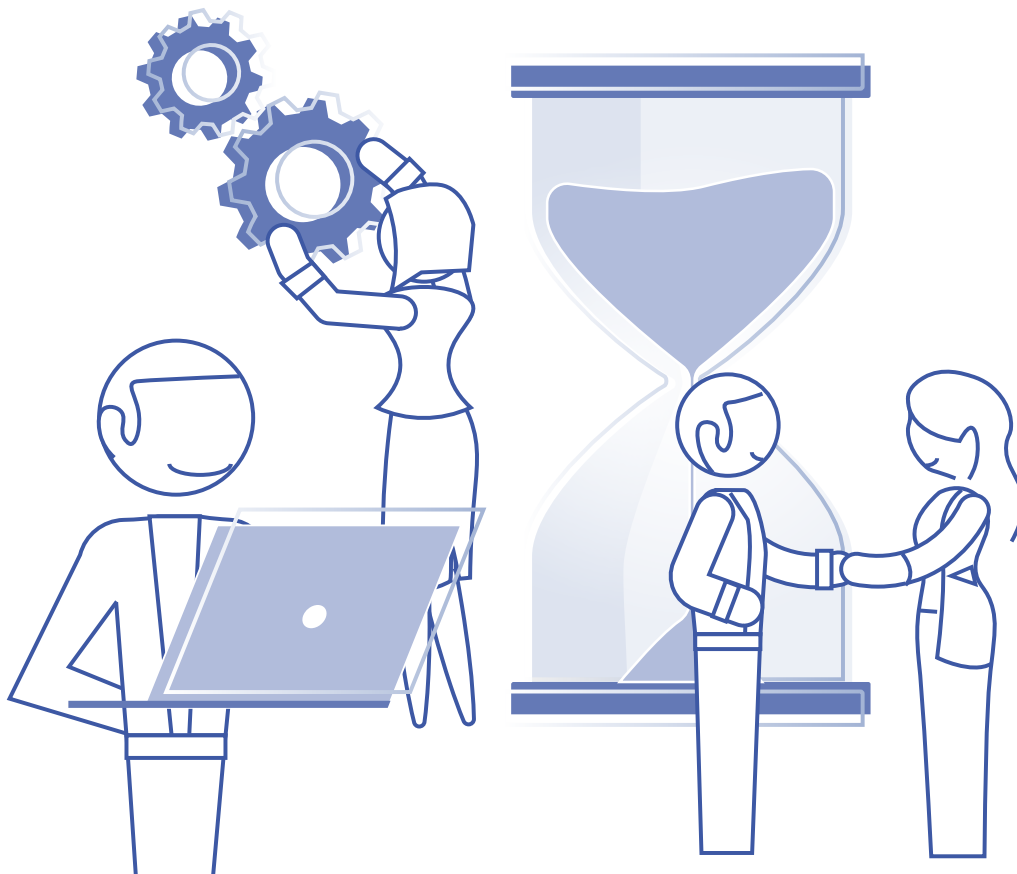
It is crucial that they be aware of the existence and effectiveness (testing) of response plans to deal with critical situations and, if necessary, be able to react in a timely manner and implement action plans.

Your board's knowledge and validation of your AMC's critical processes and subcontractors are also important.



Key deliverables

- An IT incident management process that must include³⁵:
 - ▶ a register of incidents;
 - ▶ the roles and responsibilities to be assumed for the different incident types and scenarios;
 - ▶ response (reaction) procedures to limit the effects and duration of incidents;
 - ▶ communication plans for employees, external stakeholders and the media.



³⁵) Art 17.3.

4. Resilience testing

■ In a nutshell

In order to “assess preparedness for handling ICT-related incidents” as set out in DORA, the AMC will need to adopt a service view and not limit itself to an individual approach focused on the service provider, the application or the team.

There are two types of operational resilience tests:

- ▶ tests to assess the ability of the services (including service providers) to withstand attacks;
- ▶ tests to assess business continuity following a failure or degradation of the service (regardless of the cause).



Current situation

At this stage, AMCs periodically assess their security by conducting tests (pentesting), security audits and business continuity tests.



What's new

DORA requires that operational resilience and digital security tests³⁶ follow a risk-based approach.

These tests are carried out in a manner proportionate to the size and overall risk profile of the AMC, and the nature, scale and complexity of its services, activities and operations.

They must cover critical functions using currently available tools and methods³⁷ such as vulnerability scans, pentesting, gap analyses, audits, end-to-end testing, etc.

The testing programme includes a range of assessments, tests, methodologies, practices and tools to be applied.

These tests may be carried out internally or externally provided they are performed by independent parties. When tests are conducted internally, conflicts of interest should be avoided during the design and execution phases of the test³⁸.

After pentesting, reports and action plans related to critical vulnerabilities must be produced.



Critical or important IT systems and applications must be tested at least once a year.

Note: it is possible to leverage the results of a security test on an external third party by pooling the audit with other entities.

³⁶⁾ Article 24.1 excludes microenterprises from the required resilience testing programme. ³⁷⁾ Article 25.1 for a complete list. ³⁸⁾ Art 24.4.



AFG recommends sharing with your peers to optimise your testing programmes (scope and frequency).



Challenges

At least yearly, conduct appropriate tests on all ICT systems and applications supporting critical or important functions, as well as service providers that support these functions.

For pentesting, AMCs are not required to use certified pentesters. However, it is advisable to use testers that demonstrate expertise or are certified (e.g. PASSI or other European certification) or adhere to codes of conduct and are covered by insurance³⁹.

If you use pentesters, keep in mind clauses relating to personal data protection.



At least every three years, AMCs must conduct advanced tests in the form of threat-led penetration testing (*TLPT: threat-led pentest*). Each TLPT must cover several or all critical or important functions.

AFG recommends using this threat analysis as input for your risk mapping, cyber resilience programme and board training.

These tests must be conducted in production environments with all the precautions that entails.

Under the regulation, the AMC must take all necessary measures and safeguards to ensure the participation of ICT third-party service providers in the test, while remaining responsible for ensuring compliance with the regulation.



Key for the board

The DORA Regulation entails periodically assessing, improving and demonstrating resilience to technology-related risks.

The board must be aware of reports and action plans related to critical vulnerabilities detected during audits.



We recommend that you **contextualise the vulnerabilities** detailed by the **pentesters** so that the measures are actionable by the board: describe the scenario that allowed the attack and the concrete measures to be taken in a language that helps the board understand the risk and the usefulness of the measures.



Key deliverables

- Audit reports.
- Analysis of test results.
- Plan for corrective measures.

³⁹) Art 27.

5. Third party management

■ In a nutshell

AMCs must incorporate ICT service providers into their risk management framework.

Wherever possible, AMCs must apply the same measures to them as they impose on themselves.

The consolidation of information collected at the European level should help to strengthen the stability of the European financial sector.



Current situation

The AMC is **responsible** for ensuring that ICT services provided by service providers are compliant, and must define a **strategy for managing risks** related to ICT service providers, including a **regular annual review** and taking into account the **multi-vendor strategy**⁴⁰.



What's new

The following are required under DORA:

- a. The establishment of governance arrangements to ensure oversight and appropriate monitoring of relations with all service providers.
- b. The definition and formalisation of security and continuity requirements. These requirements must be set out in service agreements that include expected service levels. The levels will be defined in the agreements along with indicators to measure their effectiveness (performance indicators for the service but also for security, such as the number of security incidents, at a minimum).



The risk management strategy must specifically consider and therefore identify the services supporting **critical or important functions**, i.e. the disruption of which would materially impair the financial performance of a financial entity, or the soundness or continuity of its services and activities, or the discontinued, defective or failed performance of those functions would materially impair the continuing compliance of a financial entity with the conditions and obligations of its authorisation, or with its other obligations under applicable financial services law⁴¹.

⁴⁰⁾ Art 6.9. ⁴¹⁾ Art 3.22.

DORA also imposes more stringent requirements regarding procedures to be put in place:

- a. Maintenance of a **register of information on contractual commitments** at the entity level and consolidated at organisation or group level which must contain⁴²:
 - ▶ an analysis of the criticality of the third party, with a breakdown between critical or important and non-critical or important third parties;
 - ▶ a risk analysis and an assessment of whether the conclusion of the contract is compliant under DORA;
 - ▶ if the third party is established in a foreign country, its compliance with various laws (such as GDPR, on which DORA places emphasis, bankruptcy law and data recovery laws)⁴³;
 - ▶ for third parties supporting critical or important functions, exit strategies⁴⁴ that include alternative solutions and documented transition plans.



b. Provision of the register to the competent authorities once a year and prior notification to the competent authorities of planned contracts for ICT services supporting critical or important functions .

- c. A single contract that sets out the rights and obligations of the ICT third-party service provider and the AMC⁴⁵ and includes additional clauses for ICT services supporting critical or important functions⁴⁶.

Note: future technical standards will provide templates for the register of information, the multi-vendor strategy, the contractual arrangement management policy and the elements that an AMC must determine and assess when subcontracting critical functions.



Challenges

Before entering into a contract for a new service, the AMC must be sure to:

- a. Conduct a **preliminary analysis** to assess the concentration risk of ICT services outsourced to service providers. Additionally, the failure of a service provider carrying out a large number of ICT services for an AMC could impact the AMC's business continuity.
- b. **Give consideration to multi-layer subcontracting:** if the arrangements allow a service provider to subcontract an ICT service, the entity includes that factor in its risk analysis and references the use of that subcontractor. The number of subcontracting levels to be overseen will be clarified; be sure to define your minimum requirements in appropriate clauses.
- c. **Review the risk of potential conflicts of interest.**

It is important that AMCs enter into **contractual arrangements** only with ICT third-party **service providers that comply with appropriate information security standards.**

For service providers providing critical and important services, financial entities must, **prior to concluding the arrangements**, take into consideration the use by ICT third-party service providers of the most up-to-date standards.

DORA also stipulates the conditions that may trigger the termination of the service.

42) Art 28.4 and 28.5. 43) Art 29.2. 44) Art 28.8. 45) Art 30.1. 46) Art 30.3.



For service providers supporting critical or important services: exit strategies must be provided to ensure the continuity of the critical or important functions supported by said ICT services. Since many long-standing contracts do not include this requirement, remember to correct this.



Key for the board

The AMC is **responsible** for ensuring that ICT services provided by service providers are compliant, which now requires an enhanced risk analysis.

It is important that the board be advised that all new contracts must include these new requirements and that it review the current situation in order to be compliant by 2025.

The ESAs will designate the critical or important ICT service providers placed under their supervision and subject to stricter security requirements, which will have a positive impact on the maturity level of those service providers.



Key deliverables

- Register of third parties.
- Policy on the use of IT services that support critical or important functions provided by third parties⁴⁷ and register of information including all contractual arrangements.
- Strategic exit plan.
- Overview of the interconnection with third parties that support critical or important functions.⁴⁸

⁴⁷⁾ Art 28.2. ⁴⁸⁾ Art 8.

6. A final word on sharing

The DORA Regulation

DORA strongly recommends that information be shared among financial entities and among peers.

The goal is to make available to all participants information enabling them to strengthen their cyber resilience.

The fact that security is being organised on a collective basis to address this threat – which has also become organised – is a positive sign.

We will be stronger together.

By relying on ICT service providers that will be subject to increasingly strict requirements, we will be even more resilient in front of new threats.

The pursuit of cyber resilience of the financial sector is a response to the rapid digital transformation seen in recent years. Cybersecurity and resilience have become top priorities for us.

It is also an opportunity for AMCs to create synergies internally around the issues of cybersecurity and business continuity.

AFG and the cybersecurity working group

“Investing in tomorrow together”, AFG’s values are particularly relevant in light of the DORA Regulation.

For many years, the Cybersecurity working group has shared best cybersecurity practices by regularly publishing practical documents that focus on proportionality.

Particularly in asset management, the scale effects from one company to another are very significant and a single model cannot be applied to all of them. Diversity is a source of enrichment for our work.

The various cybersecurity questionnaires carried out by AFG show a real improvement in the cybersecurity maturity level of the asset management sector and the extent to which cyber risk is taken into account.

The DORA Regulation supports this trend.

We hope that this guide will help you implement a plan that is pragmatic and proportionate to your AMC. With this guide, the Cybersecurity working group wished to provide you with an expert analysis of the asset management sector so that you can estimate your maturity level vis-à-vis the DORA Regulation, take the necessary actions to ensure your future compliance and focus on key points that require attention.



AFG wishes to thank René Amirkhanian (DNCA Investments), Clément Civeit (Moneta), Bruno Ducamp (Syquant), Walif El Hitti (Comgest), Mohamed Ghayati (Tikehau), Frederic Gleizer (BNPP AM), Stéphane Graux (Ostrum Asset Management), Alexandre Joachim (LBP AM), Stanislas Perney (BDL Gestion), Tristan Quiles (Amundi) and Olivier Tomatis (Groupama AM), Mamadou Wane (OFI Invest), who played an active role in drafting this guide.

For the past 60 years, AFG has brought together asset management professionals, serving the interests of investment industry participants and economic players.

- It works to promote asset management and **its growth**.
- It defines **common positions**, which it supports and defends vis-à-vis the public authorities.
- It contributes to the emergence of **solutions that benefit all participants** in its ecosystem.
- It **furtheres the industry's standing** in France, Europe and beyond, in the interest of all those concerned.
- It is invested **in the future**.

AFG

Investing in tomorrow together.



AFG

Ensemble, s'investir
pour demain

Publication produced by the Expertises department

- Valentine Bonnet, Head of Corporate Governance and Compliance
v.bonnet@afg.asso.fr | T: +33 (0)1 44 94 94 32

41 rue de la Bienfaisance | 75008 Paris | T: +33 (0)1 44 94 94 00
Avenue des Arts 44 | 1000 Brussels



www.afg.asso.fr