
Ali Alam RE CISA
is a manager working in the IT Assurance & Advisory branch of KPMG Netherlands.


Arno Kroese MSc RE RA
is a director working in the IT Assurance & Advisory branch of KPMG Netherlands.


Mourad Fakirou MSc RE
is a manager working in the Digital Transformation branch of KPMG Netherlands.


Ishan Chandra
is a manager working in the Cyber department of KPMG Netherlands.

DORA: an impact assessment

Due to the rapid use of digitization within the European financial sector, the European Commission introduces the Digital Operational Resilience Act (DORA) to set the basis for digital resilience at financial entities. Financial entities will be required to improve their digital resilience through enhancing their IT risk management processes, incident handling, management of third parties, while also sharing cyber-related information and their experiences with their peer organizations, to strengthen the sector as a whole. One distinct feature of DORA is that it also brings new financial segments in its regulatory scope under the supervision of the European Commission.

Please note that updates have been made to this article after the initial publication, to make this article correctly reflect the latest developments on the DORA legislation and its timelines.

INTRODUCTION

In the past few years, IT regulatory requirements on a European level have increased, due to increased use of IT and the risks it poses. In 2017, the European Banking Authority (EBA) announced its "Guidelines on ICT Risk Assessment under the Supervisory Review and Evaluation Process (SREP)", soon to be followed by guidelines on PSD2, cloud service providers and ICT & Security. The European Insurance and Occupational Pensions Authority (EIOPA) published its guidelines on "information and communication technology security and governance" and "outsourcing to cloud service providers" in 2020, approximately around the same timing when the European Securities and Markets Authority (ESMA) published its "Guidelines on outsourcing to cloud service providers" in 2020. Just from the titles the overlap between these guidelines stemming from the European Supervision Authorities (ESA) is apparent. This triggers the question why each segment authority is operating in silos and reinventing the wheel instead of working together on a European scale. Apart from supervisory benefits, the financial institutions under supervision that operate in different segments of the financial sector would benefit in terms of time, costs and efforts from reporting on one single set of guidelines.

The European Commission (EC) seems to understand this notion and – in line with this – proposed a new regulation in 2020 that is directed at uniformity of the network and information security and operational resilience of the financial sector as a whole called the "Digital Operational Resilience Act" (DORA).

DORA aims to improve the alignment of financial institutions' business strategies and the conduct for ICT risk management

WHAT DOES DORA ENTAIL?

DORA as a proposed regulation is part of the larger Digital Finance package of the European Commission. Its goal is to propagate, drive and support innovation and competition in the realm of digital finance, while effectively managing the ICT risks associated with it. Without a doubt, use of ICT in the financial sector has increased to the extent that ICT risks cannot be addressed indirectly as a subset of business processes. Moreover, it has seeped through to the different financial services ranging from payments to clearing and settlement and algorithmic trading.

On top of that, ICT risks form a consistent challenge to the operational resilience and stability of the European financial system. Since the financial crisis of 2008, ICT risks have only been addressed indirectly as part of operational risks and did not fully address digital operational resilience. Existing legislation by European Supervision Authorities overlaps too much as each of these authorities have their own IT framework for their segments, poses operational challenges and increases the costs of risk management for certain financial institutions that operate in different segments and therefore create a level playing field.

DORA aims to improve the alignment of financial institutions' business strategies and the conduct for ICT risk management. Therefore, it is required that the management body maintains an active role in managing and steering ICT risk management and pursue a level of cyber hygiene.

This article will dive into the five pillars of DORA and explain these in further detail and provide a comparative analysis of the different types of entities and the extent of existing ICT control frameworks that cover the contents of the DORA regulation and the corresponding gaps. The article concludes with a general roadmap of what actions financial entities can take to fulfill the requirements out by DORA.

PILLARS OF DORA

The Digital Operational Resilience Act (DORA) consists of the following five pillars:

- **ICT risk management requirements**. In order to stay up to date with the quickly evolving cyber threat landscape, financial institutions should set up processes and systems that minimize the impact of ICT risk. ICT risks should be identified on a continuous basis from a wide range of sources and addressed through internal control measures, disaster and recovery plans to safeguard the integrity, safety and resilience of ICT systems as well as physical infrastructures that support the ICT processes within the business.

- **ICT-related incident reporting.** DORA prescribes to set up appropriate processes to ensure a consistent and integrated monitoring, handling and follow-up of ICT-related incidents, including the identification and eradication of root causes to prevent the occurrence of such incidents.
- **Digital operational resilience testing (DORT)**. Capabilities and functions within the ICT risk management framework require periodical assessment to identify weaknesses, deficiencies and gaps and implementation of corrective measures to solve these. Specific attention has been given to "Threat-Led Pen Testing" (TLPT) which enables financial entities to perform penetration testing based on the threats they are exposed to.
- **ICT third-party risk**. Due to increasing use of ICT third-party providers, financial entities are required to manage ICT third-party throughout the lifecycle (from contracting until termination and post-contractual stages) based on the minimum requirements prescribed in DORA.
- **Information sharing agreements**. In order to raise awareness and grow, the regulation gives room to financial entities to exchange cyber threat information and intelligence.

DORA applies to the following financial entities. It can be noted that certain types of entities are the more mature and traditional entities that have been in scope of previous European ICT-related regulations. These concern the DNB Good Practice Information Security for banks, insurers and pension funds and EBA guidelines on Outsourcing and ICT & Security Risk Management for banks. At the same time, DORA introduces new types of entities that come into scope of an ICT regulation and are subject to it for the first time, due to their (in) direct involvement in the European financial processes. These include administrators of critical benchmarks like

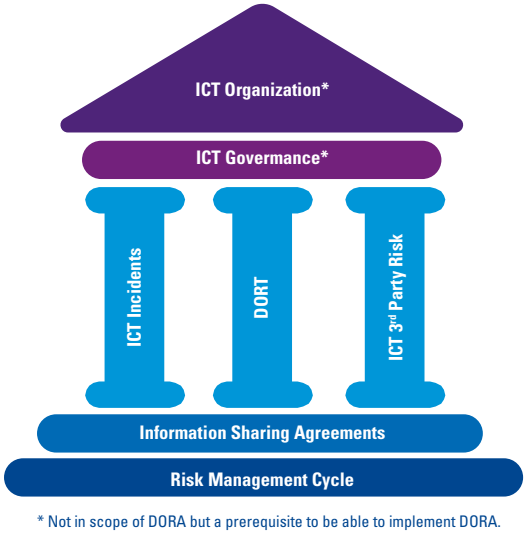


Figure 1. House of DORA.

Moody's, insurance intermediaries and ancillary insurance intermediaries (e.g., telecom companies that sell insurances on cell phones as by-product; see Table 1).

DORA has passed the proposal phase on July 13 this year, when the Economic and Monetary Affairs Committee gave its approval for implementation of DORA. On November 9, the European Parliament will vote on this legislation. The expected planning is that per ultimo 2022, DORA will be finalized, which kicks off the two-year implementation period during which financial institutions are expected to take measures to implement DORA. Per ultimo 2024, compliance with DORA is required. One exception to this timeline is the implementation of "Threat-Led Pen Testing" (the "Digital operational resilience testing (DORT)" pillar in Figure 1), as this has a deadline per ultimo 2025 as the requirements are a bit technical in nature.

Table 1. Scope of applicability.

Credit institutions	Management companies[1]
Payment institutions	Data reporting service providers
Electronic money institutions	Insurance and reinsurance undertakings
Investment firms	Insurance intermediaries, reinsurance intermediaries and ancillary insurance intermediaries
Crypto-asset service providers, issuers of crypto-assets, issuers of asset-referenced tokens and issuers of significant asset-referenced tokens	Institutions for occupational retirement pensions
Central securities depositories,	Credit rating agencies
Central counterparties	
Trading venues	Administrators of critical benchmarks
Trade repositories	Crowdfunding service providers
Management companies of alternative investment funds	Securitization repositories
ICT third-party service providers	

1 Financial Management companies that offer a range of financial services.

Figure 2. Timelines DORA.

Following the introduction of DORA, including the scope and timelines of implementation, as shown above, the next sections contain more details. We will start with an explanation of the requirements for ICT risk management.

ICT RISK MANAGEMENT

The ICT organization is subject to fundamental ICT risk management. The aim of DORA is to establish ICT risk management to realize (permanent) identification of risks and their sources, performance of proper follow-up and the setup of protection mechanisms to minimize the impact of ICT risks. Realizing this is subject to ICT governance and establishing a risk management framework which the EC describes as principle and risk based ([ECFC20]).

ICT governance & standards

The overall responsibility for ICT risk management lies with the management body, who is also required to receive regular ICT training. Management is required to play a critical and active role in directing the guardrails for ICT risk management.

DORA does not propose specific standards to meet the requirements as part of the ICT risk management. However, DORA does aim for a harmonized guideline subject to a European supervisory system. ICT Governance lies at the base of realizing this.

The ICT Governance's function's purpose is to design the accountability and process for the development and maintenance of an ICT risk management framework as well as the approvals, controls and reviews to complement, for example, ICT audit plans. Most important is the definition of clear roles and responsibilities for all ICT-related functions including their risk tolerance levels.

Also subject to the governance is the periodicity of testing and identification of weaknesses or gaps and potential mitigating measures. It is not determined yet which standard or which controls should be tested, besides that incident handling and ICT third-party risk management require explicit follow-up. Hence, the scoping and implementation of the right controls requires attention.

Scoping and applying ICT risk management with DORA

For the scoping and implementation of an ICT risk management framework we will elaborate on the scope of assets and the proportionality in relation to existing controls.

For scoping, DORA refers to the management of ICT risk management in a broad sense, covering aspects such as business functions and system accounts. However, also supporting information assets should be taken into consideration. This means that IT support tooling for the execution of a control should be marked as applicable for ICT risk management. The scope therefore extends beyond core business applications. An example is an identity access management (IAM) tool used for the automatic granting of authorizations to users. In this case, the IAM tool should be subject to ICT risk management to ensure that the risk of unauthorized access to the core business application is mitigated.

Besides the scoping of assets, there are requirements which the regulation emphasizes. This concerns subjects such as ICT incident handling and ICT third-party risk management. Besides the emphasis on these areas, there are already many other regulations to comply with. This triggers the proportionality discussion.

With regards to proportionality, the Dutch Central Bank (DNB) already noted in earlier publications that regulation and supervision require alignment of the size and complexity, but foremost the risks of financial institutions ([DCB18a], [DCB18b]). With DORA, micro-enterprises already benefit from more flexibility. Also, DORA's proposal describes that tailored risks and needs depend on the size and business profile of the respective financial institution ([EuC020]). Based on our experience, we already see many supervisory requirements for the Dutch financial services sector. This may result in not redoing the work for certain areas. Financial institutions that already implement DNB's good practice for information protection might already have the correct measures in place. DNB's good practice for information protection

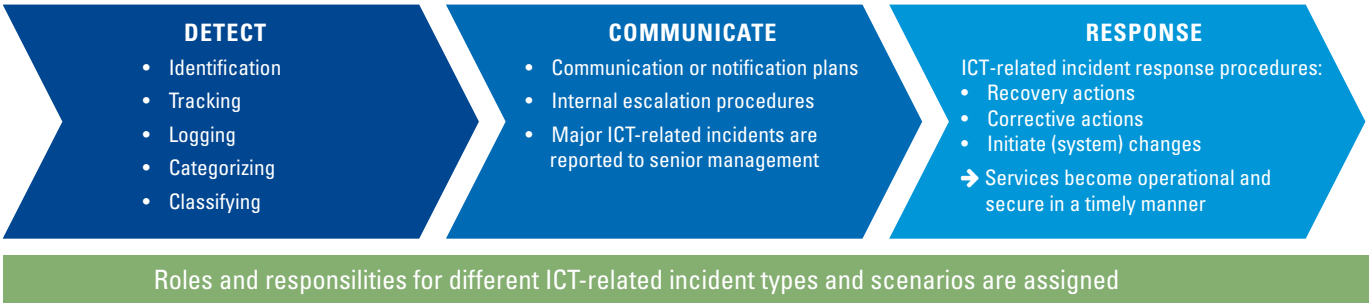


Figure 3. ICT-related incident management process.

is not a marked standard by the EC, however, we see that relevant aspects in relation to DORA have been covered. The only remark is that the good practice is principle-based rather than risk-based ([DCB19]).

We therefore propose the following steps to establish proper ICT risk management in relation to DORA:

1. Determine your scope of IT assets
2. Identify the risks related to DORA
3. Identify the impact based on confidentiality, integrity and availability
4. Identify the source of the risk based on whether the risk is driven by human, process, technology or compliance
5. Determine the likelihood and impact based on low, medium or high for each risk
6. Link the risk to existing/implemented controls and determine your residual risk for follow-up

The incident handling process can facilitate adequate identification of risks on a continuous basis. Having the right data and reporting structure in place enables the organization to perform analyses and identify which new possible risks arise from IT.

ICT-RELATED INCIDENTS

ICT-related incident management process

Many organizations are used to having an incident management process in place. The goal of this reactive process is to mitigate (remove or reduce) the impact of ICT-related disruptions and to ensure that ICT services become operational and secure in a timely manner.

With DORA, financial entities will establish appropriate processes to ensure a consistent and integrated monitoring, handling and follow-up of ICT-related incidents. This includes the identification and eradication of root causes to prevent the occurrence of such incidents. Potentially, financial entities need to enhance their incident management process to align with the minimum requirements.

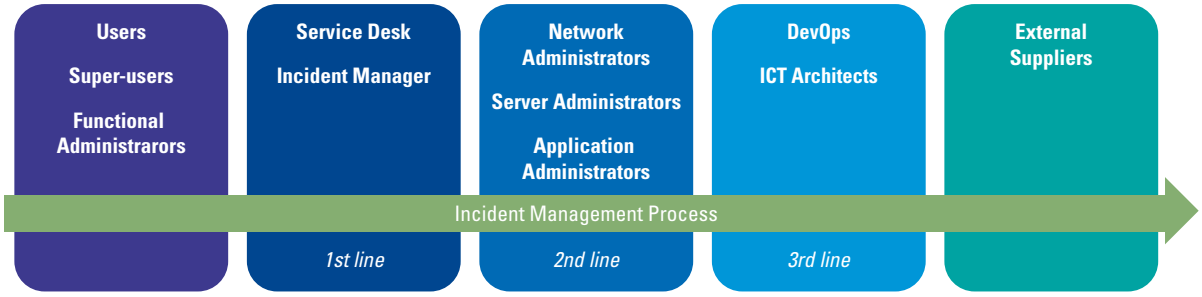
The incident management process should at least consist of elements shown in Figure 3.

The level of formalization of the ICT-related incident management process is different per financial entity. The more the process is formalized, the more likely an incident ticketing system is in place. Using an incident ticketing system facilitates the organization to record and track incidents as well as monitor the timely response by authorized staff.

Figure 4 gives an example of roles and responsibilities involved in the incident management process. It can be noted that the roles involved in the incident management process cover the full range of the organization, as incidents originate at different points in the organization and the resolution takes place at different points.

Based on our experience, we see that most of the financial entities already have a similar incident management

Figure 4. Roles in the incident management process.



a.	The number of users or financial counterparts affected and whether the incident has caused reputational impact.
b.	The duration of the ICT-related incident, including service downtime.
c.	The geographical spread with regard to the areas affected, particularly if it affects more than Member States.
d.	The data losses that the ICT-related incident entails, such as integrity loss, confidentiality loss or availability loss.
e.	The severity of the impact of the ICT-related incident on the financial entity's ICT systems.
f.	The criticality of the services affected, including the financial entity's transactions and operations.
g.	The economic impact of the ICT-related incident in both absolute and relative terms.

Figure 5. Impact assessment criteria.

process in place. As such, we expect the efforts to adjust to the DORA requirements for this part will be limited, as financial entities in general already have an incident management process in place.

Classification of ICT-related incidents

In case there are multiple ICT-related incidents, priorities must be determined. The priority is based on the impact the incident might have on the operations and on the urgency (to what extent is the incident acceptable to users or the organization). Many organizations already use criteria to prioritize incidents.

DORA describes that financial entities will classify ICT-related incidents and determine their impact based on the criteria in Figure 5.

The above-mentioned criteria will be further specified by the Joint Committee of the European Supervisory Authorities, including materiality thresholds for determining major ICT-related incidents which will be subject to the reporting obligation (see Figure 6). Additionally, this committee will develop criteria to be applied by competent authorities for the purpose of assessing the relevance of major ICT-related incidents to other Member States' jurisdictions.

Based on our experience, we see that most of the financial entities already apply a base of criteria to prioritize ICT-related incidents. We expect that all financial entities need to enhance this base of criteria to align the DORA requirements for this part, however this is something that is doable.

Reporting of major ICT-related incidents

When a major ICT-related incident occurs, financial entities will be subject to report these to the relevant competent authority within the time-limits shown in Figure 6.

The major ICT-related incidents may also have an impact on the financial interests of service users and clients of the financial entity. In that case, the financial entity will, without undue delay, inform their service users and clients about the incident and inform them as soon as possible of all measures which have been taken to mitigate the adverse effects of such incident.

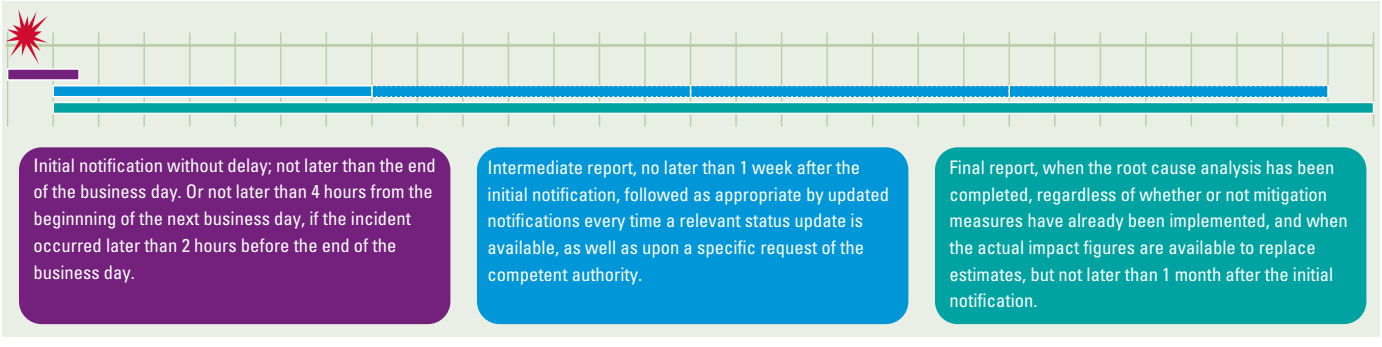
At this moment, we note that reporting of major ICT-related incidents to relevant competent authorities and to service users and clients is not formalized. As such, KPMG expects that implementing a formalized reporting process on major ICT-related incidents will take effort for every financial entity. The next section explains about the requirements on Threat-Led Pen Testing.

THREAT-LED PEN TESTING

One of the key pillars of DORA is to perform digital operational resilience testing on a periodic basis. The requirements stated in the Act support and compliment the overall digital resilience framework and provides guidelines to financial institutions for scoping, testing, and tracking of ICT risks. The requirements of this testing can be classified and is explained below.

The financial entities should follow a risk-based approach to establish, maintain and review a comprehensive digital operational resilience testing program, as per

Figure 6. Reporting timeline incidents.



the business and risk profiles. The resilience tests of the digital operational resilience testing program can be conducted by a third-party or an internal function and should at least contain the following and at least on a yearly basis:

- Vulnerability assessments
- Open-source analysis
- Network security assessments
- Physical security reviews
- Source code reviews
- Penetration testing

Apart from the testing program, the entities also have to perform vulnerability assessments before any new deployment or redeployment (or major changes) of critical functions, applications and infrastructure components.

In addition to the general tests mentioned above, DORA also states that advanced penetration tests, such as Threat-Led Penetration Tests (TLPT) meaning penetration testing adjusted to the threats the financial entity faces (i.e., a payment organization should perform penetration testing on their payment platform as threats on there are high), should also be performed at least every three years on the critical functions and services of a financial entity. The following points should be considered while performing these tests:

- The scope of the TLPT will be determined by the financial entity itself and validated with the competent authority. The scope will contain all critical functions and services – including a third party.
- TLPT performed should be proportionate to the size, scale, activity and overall risk profile of the financial entity.
- EBA, ESMA and EIOPA will develop draft regulatory technical standards after consulting the ECB and taking into account relevant frameworks in the Union which apply to intelligence-based penetration tests.
- Financial entities should apply effective risk management controls to reduce any type of disruptive risks which affect the confidentiality, integrity or availability of data and assets.
- Reports and remediation plans should be submitted to the competent authority, which shall verify and issue an attestation.

DORA also places specific demands with regard to the testers performing the Threat-Led Pen Testing. Reputation and suitability are key combined with the required expertise and level of skill. Moreover, testers are certified by an accreditation board (e.g., ISACA) valid in the member states. If testers from external parties are included, the same requirements apply. However, when using external parties, professional indemnity insurances should be in place to manage risks of misconduct and indemnity and an audit or independent assurance is needed on the sound management of protection of confidential information used as part of the testing.

Apart from internal control, emphasis is placed on managing third parties too. This will be explained in the next section.

DORA's approach towards ICT third-party risk is based on the perspective of financial entities managing ICT third-party providers throughout the entire lifecycle

ICT THIRD-PARTY RISK

The use of ICT third-party providers is prevalent in the financial sector. This ranges from limited outsourcing for data hosting services at external data centers to the more extensive outsourcing where use of IT systems and software is cloud-based or based on the Software-as-a-Service (SaaS) model, with different types of outsourcing between the two extremes.

DORA's approach towards ICT third-party risk is based on the perspective of financial entities managing ICT third-party providers throughout the entire lifecycle from the contracting to post-termination stage. This means a more holistic process than just monitoring the achievement of service level agreements and assurance reports received

Figure 7. Spectrum of outsourcing.

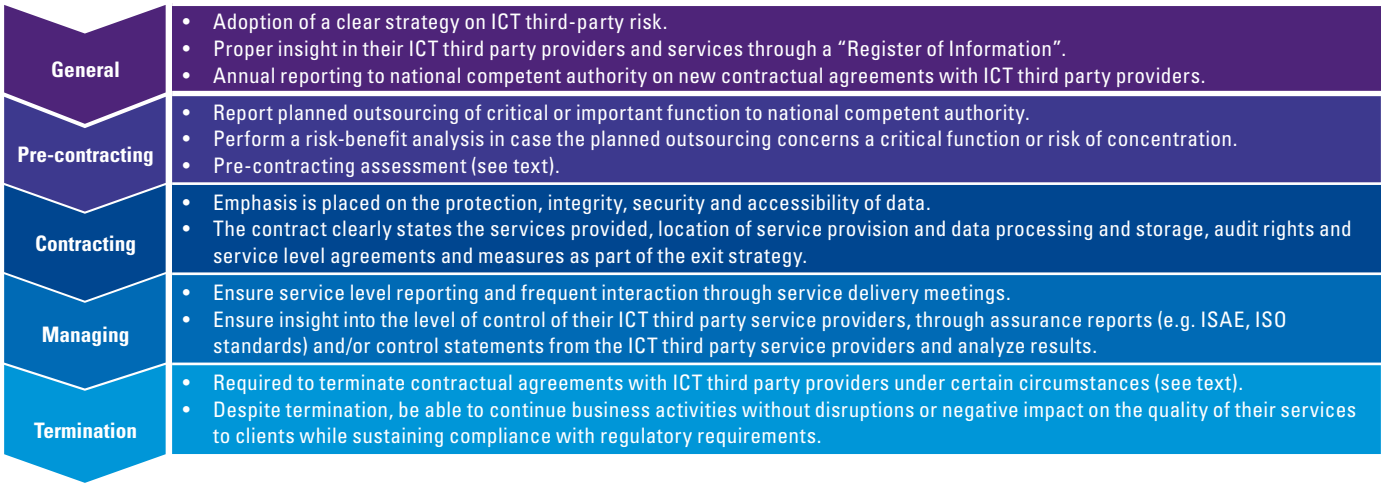


Figure 8. Lifecycle ICT third-party service provider management.

from the ICT third-party providers. This perspective is similar to that of the Outsourcing Guidelines of the European Banking Authority (EBA) ([EBA19b]).

At the same time, DORA does propagate the principle of proportionality when implementing measures to comply with DORA.

DORA defines proportionality for outsourcing as follows ([EuC020]):

1. "scale, complexity and importance of ICT-related dependencies" and;
2. "the risks arising from contractual arrangements on the use of ICT services concluded with ICT third-party service providers, taking into account the criticality or importance of the respective service, process or function, and to the potential impact on the continuity and quality of financial services and activities, at individual and at group level."

The main changes lie in the processes around pre-contracting, contracting and termination.

General requirements

Just like other regulations on outsourcing, DORA places responsibility for the results from the business process (impacted or not) by outsourcing at the financial entity, regardless of the extent of outsourcing. Financial entities are also expected to have proper insight in their ICT third-party providers and delivered services by properly maintaining this information in a so-called "Register of Information". The level of detail of this register should explain the difference between ICT third-party providers that deliver services that cover critical or important functions and those that do not. Where needed, the national competent authority (e.g., AFM and DNB) may request (parts of) the register of information to fulfill their supervisory role.

(Pre-)contracting requirements

In the context of DORA, the requirements that need to be taken into account when selecting an ICT third-party provider increase significantly compared to the situation now (see Figure 8).

The reporting process as mentioned in Figure 8 is the same as the existing policy of the Dutch Central Bank (DNB) that requires financial entities to notify DNB in case the entity is planning to enter a contractual agreement with a third-party service provider for any critical activities or with a cloud-provider ([DCB18a], [DCB18b]).

In addition to the list in Figure 8, to guide the financial entities, the European Supervision Authorities (ESAs) together will also designate and annually update the list the ICT third-party service providers that they view as critical for financial entities. The designation of "critical ICT third-party service providers" is among others based on:

- the systemic impact on the financial entities in case of failure of the ICT third-party service provider;
- number of financial entities (globally or other systemically important institutions) relying on a certain ICT third-party service provider;
- the degree of the substitutability of the ICT third-party service provider;
- number of countries the ICT third-party service provider provides service to financial entities;
- the number of countries of which the financial entities are operating using a specific ICT third-party provider.

As part of the pre-contracting, the following assessments and checks need to be made with regard to the ICT third-party provider in order to enter the contractual agreement:

- Whether the contractual agreement concerns the outsourcing of a critical or important function;
- Supervisory conditions for contracting are met;
- Proper risk assessment is performed, with attention to ICT concentration risk;
- Proper due diligence as part of the selection and assessment process;
- Potential conflicts of interest the contractual agreement may cause;
- The ICT third-party service provider that complies with the appropriate and the latest information security standards;
- Audit rights and frequency of audits at ICT third-party provider needs to be determined based on the financial entity's risk approach;
- For contractual agreements entailing a service with a high level of technological complexity (for instance software using algorithms), the financial entity should make sure it has auditors (internal or external) available that have the appropriate skills and knowledge to perform relevant audits and assessments;
- In case a financial entity is planning to outsource to a third-party service provider that is located in a third country, the entity needs to make sure that the third country has sufficient laws in place regarding data protection and insolvency and that these are properly enforced.

DORA places significant emphasis on ICT concentration risk and defines it as follows ([EuCo20]):

- Contracting with an ICT third-party service provider that is not easy to substitute for another provider, or;
- Having multiple contractual agreements with the same ICT third-party service provider or a tightly knit group of ICT third-party service providers.

Termination requirements

DORA requires financial entities to terminate contractual agreements with ICT third-party providers under certain circumstances:

- The ICT third-party provider breaches applicable laws, regulations or contractual terms;
- Circumstances or material changes arise that can potentially impact the delivered services to the extent that performance alters and impacts the financial entity;
- Weaknesses in the overall ICT risk management of the ICT third-party provider are identified that can impact the security and integrity of confidential, personal, or sensitive data;
- Circumstances arise that result in the national competent authority not being able to effectively supervise the financial entity as a result of the contractual agreement.

Proper analysis of alternative solutions in the pre-contracting stage and development of transition plans are needed to be able to sustain business operations after terminating the contract with the ICT third-party provider.

Future outlook

Overall, DORA results in a significant increase of requirements for managing ICT third-party providers, as it requires management of ICT third-party service providers throughout the lifecycle from pre-contracting till post-exiting.

The current state of management of ICT third-party service providers at financial entities is focused on due diligence procedures, service level management and analysis of assurance reports received from these ICT third-party providers (the traditional way of "managing ICT third-party providers"). Moreover, financial entities also experience difficulties in providing insight into all the relevant ICT third-party service providers with the level of detail that DORA requires. Most of the time, recording information of ICT third-party service providers is limited to the larger and more critical ICT third-party service providers. KPMG's view is that of all the DORA pillars, it is expected that compliance with the requirements to manage ICT third-party providers will require the most effort from financial entities due to the widest gap between the current and future required states. Financial entities have to review their processes per lifecycle phase and expand current or implement new procedures and controls to ensure the inclusion of the DORA requirements. Large efforts lie in the creation of the "Register of Information" as within most financial entities contracts with ICT third-party providers are dispersed over the organization and management of these contracts takes place in a decentralized manner. Getting all this information together in one overview is an ardent task.

INFORMATION SHARING AGREEMENTS

All operating financial entities experience information- and cybersecurity threats one way or another. Most of the time, the threats are also similar in form and nature, like common network and system vulnerabilities, hacks and malware. Overall, each financial entity battles the same threats, some quicker or more adequate than the other because of differences in size, experience or other factors.

Reasoning from this situation, DORA prescribes financial entities to form communities and exchange information amongst themselves on cyber threat information. This includes indicators of identification, compromise, tactics, techniques and procedures on how to prevent and/or recover from the threat.

However, there are certain conditions to forming such information sharing agreements. Forming such groups should be focused on enhancing the digital operational resilience and increasing awareness of the cyber threats and how these can be identified and resolved. At the same time, conditions for participation should be set, and data and information exchanged should be protected. Lastly, the national competent authorities should be notified when such information agreements are formed.

In the current landscape, we note that there are working groups between financial entities in the banking and insurance segments, but these are broader in nature and directed at exchanging information and not specifically at cyber threat information.

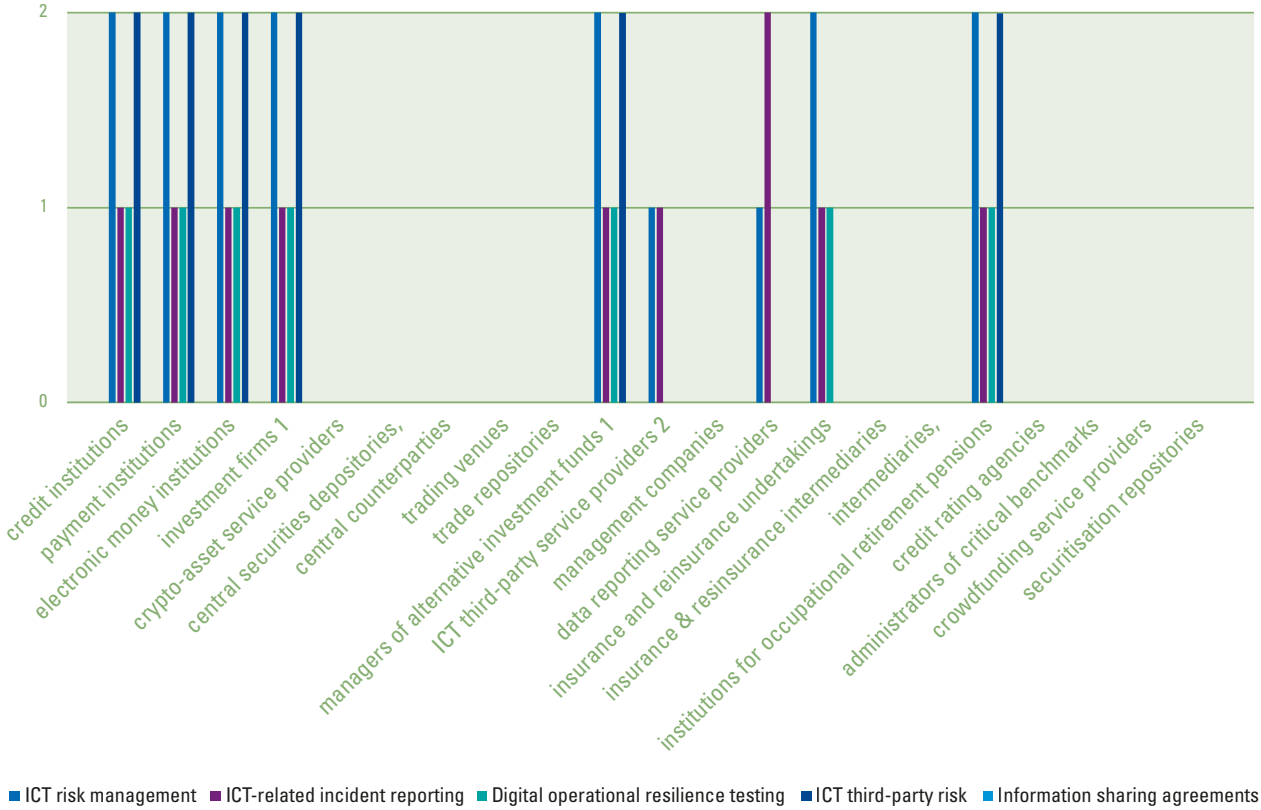
THE CURRENT STATE OF DORA

As mentioned in the introduction, DORA scopes in many segments that are new to any IT regulation and have little to no experience in translating and implementing IT requirements into their organizations. At the same time, there are a number of segments that have had their fair share of experience with IT regulations through the national competent authority (being the Dutch Central Bank ([DCB19]) and European Supervisory Authorities ([EBA19a], [EBA19b], [EIOP20]) and are more mature in governing IT in their respective organizations which include banks, insurers and pension funds.

This dynamic creates a split in terms of the effort needed to comply. More mature organizations have the capabilities to bridge the gap based on past experiences, whereas less mature organizations also have to build on their capabilities to translate IT requirements into their organization.

The analysis in Figure 9 provides a detailed view of what the situation is like. The five pillars of DORA are plotted against the different segments in scope. Per segment it is described whether there are any existing IT regulations/ frameworks in those segments that overlap with DORA to determine an indication of the effort required to comply with DORA. A digit of 1 means that there is one existing IT regulation or framework that overlaps with the requirements in the respective DORA pillar, whereas 2 means there is an overlap with two existing IT regulations or frameworks.

Figure 9. Analysis of mapping of DORA pillars vs. segments.



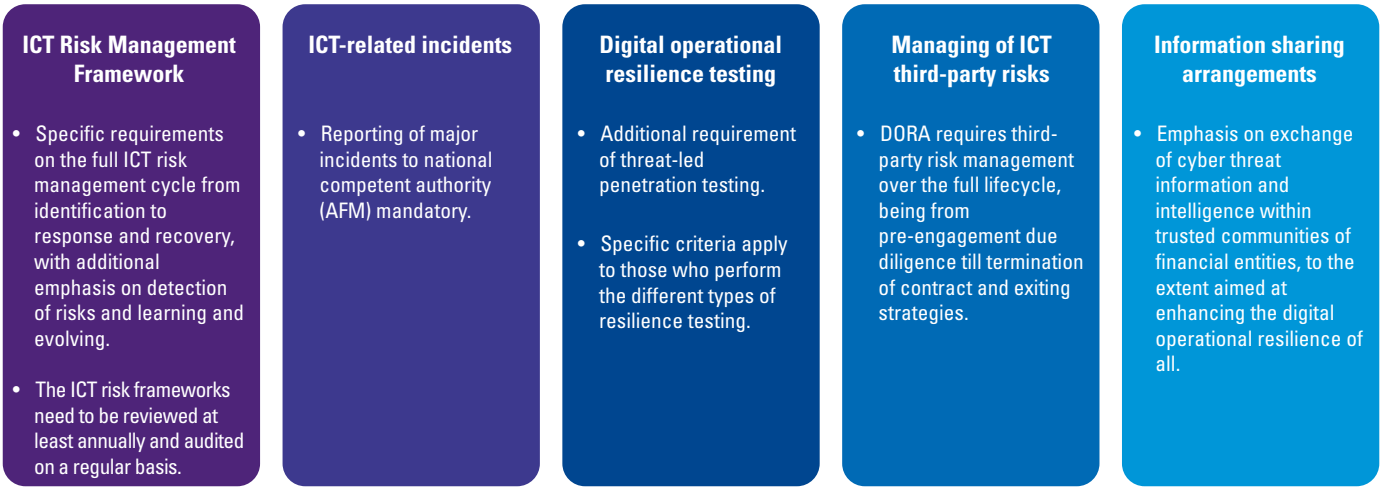


Figure 10. Compliance roadmap.

Based on the analysis above, three specific observations can be made:

1. What becomes immediately apparent from this analysis is that there are certain sectors (e.g., credit rating agencies, benchmark administrators, crowdfunding organizations) that lack IT frameworks to govern IT, which are being subjected to IT regulations for the first time and therefore do not have any experience in translating IT regulations into controls within their organizations. The expectation is that financial entities in this segment will have to undertake considerable efforts to comply with DORA requirements.
2. At the same time we note that all segments across the board do not have any good practices or controls in place through existing regulations that address the information sharing agreements. The requirements for "information sharing agreements" are not the hardest set of requirements within DORA that needs to be complied with. As mentioned earlier, some informal working groups among banks, insurers and pension funds already exist, and adding the requirements from DORA would most probably require little effort.
3. Lastly, segments that already have experience in implementing IT regulatory requirements such as credit institutions, insurers and pension funds did this through frameworks such as the DNB Good Practice Information Security, EBA Guidelines on ICT & Security Risk Management, EBA Guidelines on Outsourcing and EIOPA ICT Guidelines. However, these financial entities still have to undertake some effort to comply with DORA. Like for ICT risk management there are additional requirements not covered by the existing regulations/frameworks and the guidelines of the EIOPA framework for insurers and pension funds limit outsourcing to contract and service level management only. In the same manner, the reporting of ICT-related incidents and Threat-Led Pen Testing is not common practice yet and will therefore also require efforts for proper implementation – although to a lesser extent compared to newly regulated financial entities.

ROADMAP TO COMPLIANCE

If we sum up all the requirements discussed in the previous sections, we note that while some elements are entirely new, there are also elements that represent an add-on to existing practices. The requirements for managing ICT third-party risks and information sharing agreements are entirely new, whereas IT risk management and ICT incidents represent the add-ons to existing topics. All in all, there is quite a lot to comply with for DORA. Figure 10 gives a summary of the requirements for each of the DORA pillars, which are new to financial entities.

CONCLUSION

DORA increases the attention on ICT used by financial institutions . As discussed in this article, DORA focuses on five pillars: ICT risk management, ICT-related incident reporting, Digital operational resilience testing, ICT third-party risk and Information sharing agreements. The scope of financial institutions to whom this applies has been broadened. Besides the traditional financial institutions, such as banks and insurance companies, crypto-asset service providers are also required to comply with the guidelines and require more formalization since no current standards are published yet for crypto-asset service providers. Hence, the current state of maturity may vary between the types of organizations regarding compliance with the five pillars. This also triggers the proportionality discussion and requires revisiting of

DORA will increase the regulatory pressure and will require compliance with new additional requirements

the financial entities' current state to determine to what extent new or extra measures should be taken.

KPMG's view is that DORA will increase the regulatory pressure and require compliance with new additional requirements. This has multiple reasons. First of all, DORA is a European IT regulation that will bring extra pressure and impact as it will apply as a law and brings them under the supervision of the European Commission. Therefore, financial entities will have to comply with a law and not being able to comply will be viewed as Non-Compliance with Laws and Regulations (NOCLAR) with potential legal implications.

Secondly, DORA introduces entirely new requirements, that will require the necessary additional efforts to implement within the organization, including the redefinition of internal processes (ICT third-party management) and formation of new processes (information sharing agreements). For financial entities that do not have much experience with complying with IT regulations this will be an arduous task.

Thirdly, a large part of the financial entities already has to comply with many different IT regulations/guidelines. Financial entities can therefore experience the so-called "regulatory fatigue" which may impact their overall level of compliance.

KPMG is of the opinion that financial entities should start assessing the impact of DORA on their organization as soon as they can, in order to effectively utilize the implementation timeframe of one year and achieve compliance with DORA by the end of 2024.

References

[DCB18a] Dutch Central Bank (2018, June 25). *Good practices beheersing risico's bij uitbesteding.* Retrieved from: https://www.dnb.nl/voor-de-sector/open-boek-toezicht-fasen/lopend-toezicht/prudentieel-toezicht/governance/good-practices-beheersing-risico-s-bij-uitbesteding/

[DCB18b] Dutch Central Bank (2018). *Proportioneel en effectief toezicht.* Retrieved from: https://www.dnb.nl/media/yojpc5a5/dnb-studie-proportioneel-en-effectief-toezicht.pdf

[DCB19] Dutch Central Bank (2019). *Good Practice Informatiebeveiliging.* Amsterdam: DNB.

[EBA19a] European Banking Authority (2019). *EBA Guidelines on ICT and security risk management.* Paris: European Banking Authority.

[EBA19b] European Banking Authority (2019). *EBA Guidelines on outsourcing arrangements.* Paris: European Banking Authority.

[ECFC20] European Commission First Council Working Party (2020, September 30). *Digital Operational Resilience Act.* Retrieved from: https://ec.europa.eu/info/sites/default/files/business_economy_euro/banking_and_finance/200924-presentation-proposal-digital-operational-resilience_en.pdf

[EIOP20] European Insurance and Occupational Pensions Authority (2020). *Guidelines on information and communication technology security and governance.* European Insurance and Occupational Pensions Authority.

[EuC020] European Commission (2020). *REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on digital operational resilience for the financial sector and amending Regulations (EC).* Brussels: European Commission.

[EuPa22] European Parliament (2022, March 24). *Legislative Train Schedule: Digital Operational Resilience for the Financial Sector.* Retrieved from: https://www.europarl.europa.eu/legislative-train/theme-a-europe-fit-for-the-digital-age/file-cross-sectoral-financial-services-act-1

About the authors

Ali Alam RE CISA is a manager at KPMG working in the IT Assurance & Advisory branch of KPMG Netherlands. He has been working in the financial sector for the past 9,5 years in the field of ICT risk and IT audit and has extensive experience in IT risk carrying out IT Maturity and IT Risk Assessments.

Arno Kroese Msc RE RA is a director at KPMG working in the IT Assurance & Advisory branch of KPMG Netherlands. He has been working with a focus on the financial sector for the past 21 years in the areas of financial audit, IT audit and (IT) risk management. He has extensive experience in performing quality assurance and IT risk & IT maturity assessments.

Mourad Fakirou MSc RE is a manager at KPMG working in the Digital Transformation branch of KPMG Netherlands. He has been working in the financial sector and tech for the past 5 years. He combines a strategic business view with IT to optimize ICT risk management and IT audit procedures.

Ishan Chandra is a manager at KPMG Netherlands working for the Cyber Security practice in IT Risk Advisory. He has been working with clients in the financial sector, technology and national critical infrastructure for the past 9.5 years. His expertise focuses on performing penetration testing and red teaming.