European Confederation of
Institutes of
Internal Auditing

AN ECIIA PUBLICATION

DORA

IMPACT OF THE DIGITAL OPERATIONAL RESILIENCE ACT ON THE INTERNAL AUDIT FUNCTION

SEPTEMBER 2024

Table of Contents

Purpose of the paper

The European Union's Digital Operational Resilience Act (DORA) affects Internal Audit in insurance companies, as it sets direct and indirect standards for the internal audit function. The deadline for meeting DORA requirements is 17 January 2025, and both financial institutions and service providers across the industry are feeling the pressure.

The aim of this paper is to provide internal audit functions with an overview of the status approximately six months before the regulation's due date, what activities from internal audit functions are required by DORA directly, as well as what practices companies are adopting to comply with DORA and how internal audit can give assurance.

The views and opinions expressed do not necessarily reflect the official policy or position of any agency or organization on DORA. The information contained in this paper reflects a general informative view on DORA and its potential impact on Internal Audit.

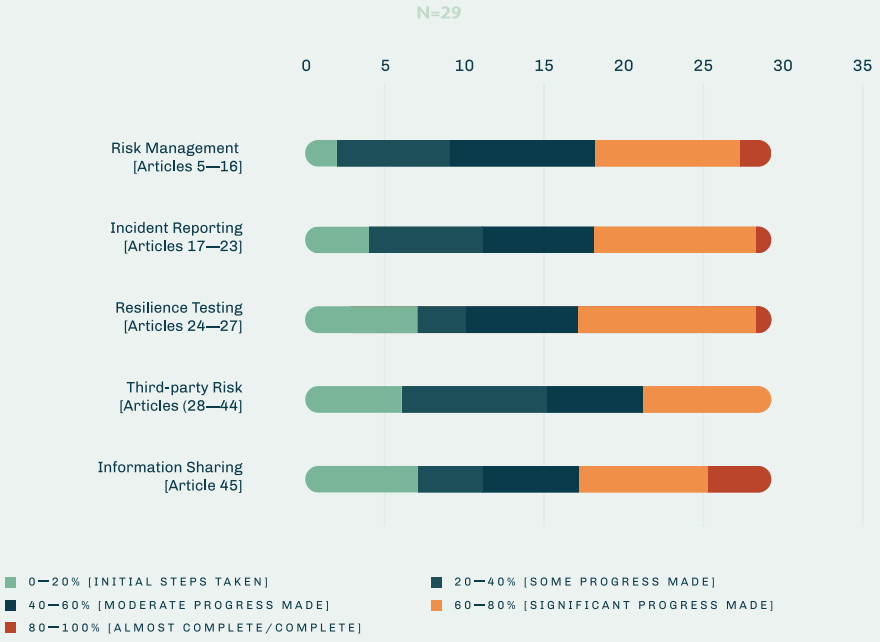
Executive Summary

DORA (Digital Operational Resilience Act) is a regulation by the European Commission aimed at enhancing the digital operational resilience of the financial sector. It includes, but is not limited to, Insurance and Reinsurance Undertakings: firms that do insurance and reinsurance businesses; Insurance Intermediaries, Reinsurance Intermediaries and Ancillary Insurance Intermediaries; Agents and brokers for insurance (DORA - Art. 2 Scope - Digital operational resilience act). The only exceptions for Insurance for DORA are listed in Directive 2009/138/EC (Solvency II) Article 4. These exceptions exclude insurances from DORA under certain conditions, one of which is the gross written premium must not exceed € 5 million.

DORA aims to establish a common framework for ICT risk management, incident reporting, resilience testing, third-party oversight, and information sharing. DORA consists of five pillars that cover different aspects of digital operational resilience. The first pillar is ICT risk management, which requires financial entities to implement a governance and internal control framework for ICT risks. The second pillar is ICT-related incident management, classification and reporting, which requires financial entities to report major ICT incidents to the competent authorities. The third pillar is digital operational resilience testing, which requires financial entities to conduct regular testing of their ICT systems and applications. The fourth pillar is managing of ICT third-party risk, which requires financial entities to assess and monitor the risks posed by ICT service providers. The fifth pillar is information-sharing arrangements, which encourages financial entities to exchange information on cyber threats and best practices. As part of a three lines model (First Line: Business, Second Line: Risk Management and Compliance and Third Line: Internal Audit), internal audit needs to give assurance on all DORA requirements including the first and second lines tasks.

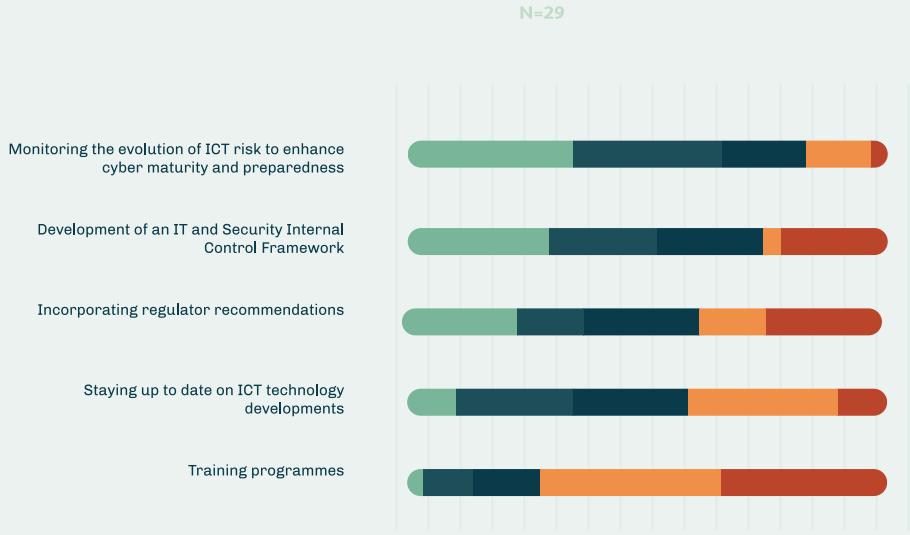
This paper draws on a survey conducted from 16/02/2024 to 27/03/2024 based on 70 respondents, of which 29 were Insurance companies. The survey results show how the Three Lines of Defence of Insurance Companies view and deal with the risks related to DORA. By Q2 2024, most insurance companies are still at early stages of their DORA implementations or have made up to moderate progress, only a few have advanced significantly:

FIGURE 1 — CURRENT PROGRESS ON DORA IMPLEMENTATION OF COMPANIES



The survey results show that ICT Risks and internal controls are the first priority for the participating insurance companies, whereas training is the least important among the mentioned categories:

FIGURE 2 — MEASURES PRIORITIZED BY INSURANCE COMPANIES TO ENHANCE THEIR IT RISK MANAGEMENT. MOST TO LEAST IMPORTANT.



Key takeaways of this paper for internal audit in the insurance industry but also the financial industry overall are:

Internal audit functions must prepare themselves for the direct requirements addressed to them:

- The ICT risk management framework shall be subject to internal audit activities on a regular basis, as part of the audit plan. Auditors shall be appropriately skilled to perform them. A follow-up process on audit findings is necessary, which assures the timely remediation and verification of critical ICT audit findings.
- ICT response and recovery plans shall be subject to internal audit reviews.
- Thread-led penetration tests (TLPT) shall be documented in a qualitative report, even though the tests should not be performed by internal audit and therefore the report might not be authored by internal audit.
- ICT third-party service providers shall be assessed and inspected based on a risked-based approach. These assessments shall be conducted by skilled auditors; also pooled audits are an option, which is an approach possibly very beneficial in the future.
- Contracts with ICT third-party providers shall be checked on all key contractual provisions relevant for internal audit.

Internal audit must train and upskill themselves to catch up on DORA requirements, but also on common IT practices in this context (e.g., ICT risk management, ICT incident management, business continuity management, third-party management).

The DORA is still very young, not all supporting policy products are released by now, and good practices of implementation have to form over time. In any case, the efforts of enhancing the financial industries' cyber defence and preparedness as well as developing a robust ICT and security internal control framework is certainly a step in the right direction. Compliance with DORA is not only advised due to potential consequences of administrative fines, public admonishment, postulated remediation plans or compensations to customers and third parties, but also because of the requirements create a *digitally resilient* European financial market, which is an objective that benefits the financial market and consumers as a whole.

1.0 Introduction to DORA regulation

1.1 Context — The EU Digital Finance Package

Constant changes and developments in the financial sector, such as the release of new financial products, digital finance transformation, crypto assets and distributed ledger technology have called for a stronger and more coherent regulation in the European Union (EU).

In September 2020, the European Commission initiated its first actions by embracing the "EU Digital Finance Package"[1] , setting out general lines on how the EU can support the digital transformation of Finance in the next five years.

The main goals are (i) to enable and support the potential of digital finance in terms of innovation and competition, while mitigating the risks for consumers, businesses and, in general, EU financial stability and (ii) to ensure that fintech companies can deal with cyber-attacks and operational disruptions through the implementation of governance measures, cybersecurity and ICT risk management and incident reporting.

The package addresses the strategy for the next five years and includes three legislative proposals:

I. Markets in Crypto-Assets Regulation «MICA»,

II. Digital Ledger Technology Regulation «DLT»,

III. Digital Operational Resilience Regulation «DORA».

1.2 Goals and timeline of DORA

This paper is focusing on DORA as the first piece of legislation at European level to address digital operational resilience for financial services, where the term resilience means the ability to continue operating in the event of incidents or disruptive events caused by the digital domain. DORA establishes a regulatory framework to implement rules that companies will have to comply with to reduce their vulnerabilities and be able to respond to and recover from all types of ICT-related disruptions and threats. The main goals of the regulation are:

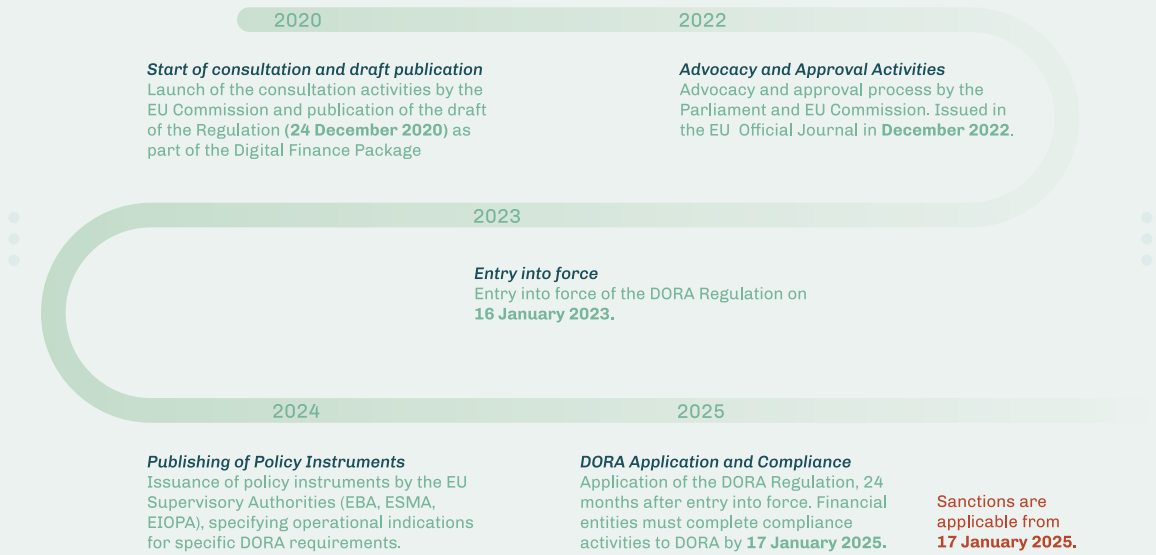
- Effective governance of ICT risks and cyber risks;
- Reinforcing the role of Supervisory Authorities;

1 EU Digital Finance Package: https://finance.ec.europa.eu/publications/digital-finance-package_en

- Raising the European standard on Cyber Security;
- Harmonizing the ICT risk management regulations that already exist in individual EU member states;

DORA application is mandatory starting from January 17, 2025, after a 4-years of continuous publication and consultation period.

FIGURE 3 — DORA TIMELINE



1.3 Consequences for failure to comply with DORA

In case companies do not comply with the DORA regulation, they may face several consequences. Firstly, they may be subject to administrative fines. Additionally, supervisory authorities have the right to publicly admonish financial institutions and to oblige them to implement remediation plans aimed at addressing any weaknesses or failures impacting their operational resilience.

Companies missing regulatory requirements may be obliged to adequately compensate both, direct customers and third parties, in any way impacted by the failure to comply.

Moreover, for severe cases of repeated non-compliance to DORA requirements, supervisory authorities may request capital add-ons and even reserve the option to withdraw the authorization of financial entities.

1.4 The 5 Pillars of DORA

The DORA Regulation consists of 64 Articles, 41 of which are part of the 5 pillars as detailed below. The other 23 articles do not strictly refer to to financial entities' duties, covering structural areas such as: Scope of application, Competent Authorities, Delegated Acts, Transitional and final provisions, Amendments.

FIGURE 4 — THE 5 PILLARS OF DORA

The text below contains a summary of the main points addressed in the 5 pillars.

Pillar I — Governance & ICT risk management (rf. DORA CHAPTER II)

- Strengthening the **top management responsibilities**, requiring the **development of policies** for operational resilience management, and **defining the strategies/models** to minimize the impacts from events arising from the digital world that could undermine the confidentiality, availability or integrity of the critical services and functions.
- Top management should no longer focus only on the **financial sustainability, but also on resilience.**
- Improvement of **risk management models and tools** for an effective response to the ever-changing environment and to minimize the impact of ICT risks:
    - *Set up a governance and internal control framework for ICT risks.*
    - *Require adequate resources to meet operational resiliency needs.*
    - *Identify and classify, based on criticality, ICT support functions and assets and their inter-dependencies with third parties.*
    - *Identify risk sources on a continuous basis.*
    - *Perform the annual risk assessment specific for legacy systems.*
    - *Develop specific awareness and training programs on digital resilience.*
    - *Define and implement the Business Continuity Policy with the Disaster Recovery Plan as an integral part.*

Pillar II — ICT-related incident management, classification and reporting (rf. DORA CHAPTER III)

- Improved **management, classification and reporting of major ICT incidents**. The ESAs[2] will develop **criteria** for major incidents' identification and common/standard **reporting templates**. The ESAs will analyze the possibility of further **harmonization** and **centralization**, by evaluating the establishment of a single EU Hub for major ICT-related incident reporting by financial entities. The classification and reporting criteria are based on the (i) Number of impacted users, (ii) Duration of the incident, (iii) Geographical area/areas and (iv) Importance of services.
- Definition and implementation of an **ICT incident management process.**
- Adoption of **early warning indicators** and definition of **specific criteria** for incidents **classification**.
- **Monitoring of** incidents and implementation of **follow-up mechanisms** until the root cause is eliminated.
- **Reporting of major ICT incidents** to the national regulator.

Pillar III — Digital operational resilience testing (rf. DORA CHAPTER IV)

- Verifying the effectiveness of predictive, incident detection, response and recovery capabilities through **periodic testing.**
- Conducting digital operational resilience testing **proportionate to the size, business and risk profiles** of financial entities, through **Basic tests** (for all financial entities) and **Advanced tests** (e.g., TLPT – Threat Leading Penetration Testing) for significant entities with an appropriate level of cyber maturity (*Note: the competent Authorities evaluate the level of cyber maturity based on elements such as the criticality or importance of the functions in relation to the services provided and the activities carried out by the financial entity, as well as the specific ICT risk profile).*
- **Testing periodically** all **critical ICT systems and applications** (vulnerability, code analysis, performance, capability, etc.).
- Dedicating **sufficient resources** and ensuring that **conflicts of interest are avoided** (e.g., between test design and test execution).

Pillar IV — Managing of ICT third-party risk (rf. DORA CHAPTER V)

- Application of a **strategic approach** to third-party risk management to also monitor **interdependencies** and **risk concentration.** DORA introduces a Union **oversight framework** for providers deemed critical (**ICT Critical Third-Party Provider** or **CTPP**), to address potential systemic and concentration risks posed by the financial sectors' reliance on a small number of ICT third-party service providers. **Lead Overseers** have the power to **monitor** the **activities of CTPPs** on a European scale in relation to the ICT services they provide to the financial sector.
- Development of an **information register** containing a comprehensive overview of all ICT third parties. **Reporting the changes** to the register **to the Regulator** on an annual basis.
- **Extension of the supervisory perimeter** to critical ICT third parties (considering all high-risk ven-

2 The ESAs are the European Supervisory Authorities: EBA (European Banking Authority), ESMA (European Securities and Markets Authority) and EIOPA (European Insurance and Occupational Pensions Authority).

dors, not just those considered as outsourcing).

- **Harmonization of contractual aspects** to allow full monitoring by the financial entity at all stages of the relationship with the third-party provider.
- Performing the **ICT concentration risk assessment** (cost / benefit analysis of alternative solutions).
- **Exit strategy** in case of outsourcing of critical or important functions.

Pillar V — Information-sharing arrangements (rf. DORA CHAPTER VI)

- DORA encourages the **exchange between financial entities of information** on cyber threats, intelligence, techniques, procedures, warnings, and tools to **strengthen digital resilience** and to tackle next-generation threats. **The financial ecosystem** is highly interconnected, which can spread incidents from one operator to another. It also relies on common infrastructures and technologies, and faces threats that often affect the entire sector, not just individual financial operators.

To increase awareness of ICT risks, minimize their spread, support the defensive capabilities of financial institutions and threat detection techniques, DORA aims **to define agreements for the exchange of information on cyber threats**. It should be noted that the implementation of such requirements is not mandatory, financial entities can decide whether or not to exchange such information with other financial entities.

1.5 DORA and its Policy Instruments

Besides DORA as the main act, the **Policy Instruments** specify further operational requirements on DORA pillars to ensure a consistent and harmonized legal framework in the different areas.

The ESAs were requested to jointly prepare this set of **13 Policy Instruments**, through the Joint Committee (JC). More precisely they produced 7 Regulatory Technical Standards (RTS), 2 Implementing Technical Standards (ITS), 2 Guidelines, 1 Feasibility Report and 1 Call for advice.

The Policy Instruments have been divided into two main batches, both subject to a **Public Consultation** lasting approximately three months to gather feedback and comments. Based on these consultations, the ESAs submitted to the European Commission the whole set of documents by two different deadlines: **17th January 2024** (first batch) and **17th July 2024** (second batch).

The European Commission already published the first batch documentation on the 25th of June 2024 and will now start reviewing the second one, aiming to adopt these policy products in the subsequent months.

The picture below represents a mapping between the whole set of policy instruments and the DORA Pillars[3].

3 Source: https://www.eiopa.europa.eu/digital-operational-resilience-act-dora_en

FIGURE 5 — MAPPING OF THE POLICY INSTRUMENTS WITH THE 5 PILLARS

Governance & ICT Risk Management	*Incident Management & Reporting*	*Digital Operational Resilience Testing*	*ICT Third-Party Risk*	*Information Sharing*
RTS on ICT Risk Management framework (Art. 15) and on Simplified Risk Management framework (Art. 16)	**RTS** on criteria for the classification of ICT related incidents (Art. 18.3)	**RTS** to specify threat-led penetration testing (Art. 26.1)	**ITS** to establish the templates of register of information (Art. 28.9)	No Technical Standards have been foreseen for this pillar
Guidelines on the estimation of aggregated costs/losses caused by major ICT related incidents (Art. 11.1)	**RTS** to specify the reporting of major ICT related incidents (Art. 20.a)		**RTS** to specify the policy on ICT services performed by third-party (Art. 28.10)	
	ITS to establish the reporting details for major ICT related incidents (Art. 20.b)		**RTS** to specify the elements to determine and assess when sub-contracting ICT services supporting a critical or important function (Art. 30.5)	
	Feasability report on further centralisation of incident reporting through establishment of a single EU hub for major ICT-related incident reporting (Art. 21)		**Call for advice** on criticality criteria (Art. 31.8) and fees (Art. 43.2) DL: 30 September 2023	
			Guidelines on cooperation ESAs — CAs (Competent Authorities) regarding DORA oversight of critical ICT third-party service providers (Art. 32.7)	
			RTS on harmonisation of oversight conditions (Art. 41)	

Source: DORA public consultation overview document (europa.eu)

2.0 Impact of DORA on Internal Audit

2.1 DORA direct requirements for Internal Audit

DORA is designed to enhance the ability of the financial sector to withstand digital operational, ICT, and cybersecurity risks. DORA imposes several new obligations that financial institutions will have to meet and has significant implications for the Internal Audit function, as it imposes direct expectations towards the function, such as those in Articles 5, 6 and 11.

Article 5 — Governance and organization

The management body of the financial entity shall define, approve, oversee and be responsible for the implementation of all arrangements related to the ICT risk management framework referred to in the following Article 6. The management body should moreover approve and periodically review the **financial entity's ICT internal audit plans**, ICT audits and material modifications to them.

Article 6 — ICT risk management framework

Financial entities shall ensure appropriate segregation and independence of ICT risk management functions, control functions, and **internal audit functions** according to the Three Lines of Defence Model, or an internal risk management and control model. Further, the ICT risk management framework of financial entities, other than microenterprises, shall be subject to **internal audit activities on a regular basis in line with the financial entities' audit plan**. The involved auditors shall possess sufficient knowledge, skills and expertise in ICT risk, as well as appropriate independence. The frequency and focus of **ICT audits** shall be commensurate to the ICT risk of the financial entity. Based on the conclusions from the internal audit review, financial entities shall establish a formal follow-up process, including rules for the timely verification and **remediation of critical ICT audit findings.**

Article 11 — Response and recovery

As part of the ICT risk management framework referred to in Article 6, financial entities shall implement associated ICT response and recovery plans which, in the case of financial entities other than microenterprises, shall be subject to **independent internal audit reviews.**

Based on the survey performed in the first quarter of 2024 within the financial industry, it was found that management bodies of 72% of companies already approve and periodically review the financial entities' ICT Internal Audit plans, ICT audits and material modifications to them. Only 24% of the respondents are still working on implementing this procedure while 4% had no plans yet how to implement it (see figure 6). This indicates that ICT risk management framework audits are already carried out on a regular basis or will be in the future according to the approved ICT audit plan. This also holds for the audit on the ICT response and recovery plans. The survey showed as well that a follow-up procedure on remediation actions of critical ICT audit findings is to a high percentage (79%) already established (see figure 7).

FIGURE 6 — PERCENTAGE OF INSURANCE COMPANIES WHERE MANAGEMENT BODY APPROVES AND PERIODICALLY REVIEWS ENTITIES ICT INTERNAL AUDIT PLANS, ICT AUDITS, AND MATERIAL MODIFICATIONS TO THEM

N=29

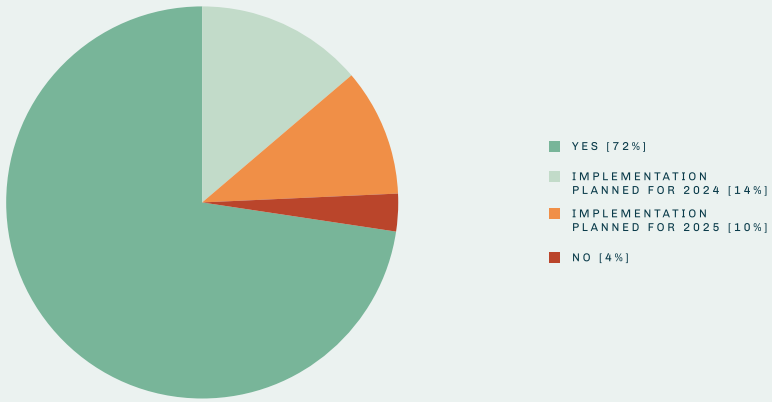
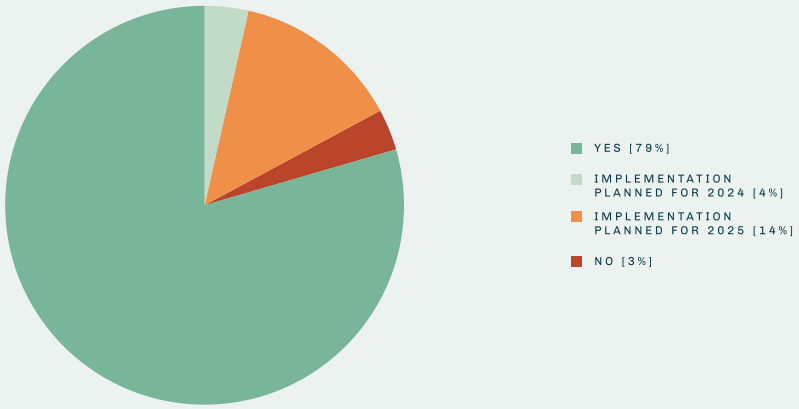


FIGURE 7 — INSURANCE COMPANIES WITH AN ESTABLISHED FOLLOW-UP PROCESS, INCLUDING RULES FOR REMEDIATION AND VERIFICATION OF CRITICAL ICT FINDINGS

N=29



2.2 Other DORA implications for Internal Audit

DORA has several sections which define independent reviews and assurance. Even if such sections are not directly addressing Internal Audit, related requirements should be taken into consideration by Internal Audit for the execution of the audit risk assessment and the definition of the audit plan. Here in particular Articles 6, 11, 27, 28 and 30 are of interest. While parts of Articles 6 and 11 impose direct requirements on Internal Audit, other parts address first and second line reviews and activities of which Internal Audit should be informed. Articles 27, 28 and 30 instead address activities which can be carried out by Internal Audit if not allocated to other resourcing options.

Article 6 - ICT risk management framework

The ICT risk management framework shall be documented and reviewed at least once a year as well as upon the occurrence of major ICT-related incidents, and **following** supervisory instructions or **conclusions derived from relevant digital operational resilience testing or audit processes.** It shall be continuously improved on the basis of lessons derived from implementation and monitoring. A report on the review of the ICT risk management framework shall be submitted to the competent authority upon its request.

Article 11 — Response and recovery

Financial entities shall regularly review their ICT Business Continuity Policy and ICT response and recovery plans, taking into account the results of tests carried out annually by the first and second lines of defense as well as recommendations **stemming from audit checks** or supervisory reviews.

Article 27 — Requirements for testers for the carrying out of Threat-led penetration tests (TLPT)

Independent assurance, or an audit report, in relation to the sound management of risks associated with the carrying out of TLPT, including the due protection of the financial entity's confidential information and redress for the business risks of the financial entity, shall be provided. With this article the law maker emphasizes that the carried out TLPTs shall particularly focus on risks related to the protection of information and potential negatives effects on business operations.

Article 28 — Key principles for a sound management of ICT third-party risk

In exercising **access, inspection and audit rights** over the ICT third-party service provider, financial entities shall, on the basis of a **risk-based approach,** pre-determine the frequency of audits and inspections as well as the areas to be audited through adhering to commonly accepted audit standards in line with any supervisory instruction on the use and incorporation of such audit standards. Where contractual arrangements concluded with ICT third-party service providers on the use of ICT services entail high technical complexity, the financial entity shall verify that **auditors, whether internal or external, or a pool of auditors**, possess appropriate skills and knowledge to effectively perform the relevant audits and assessments.

In addition to the above-mentioned requirements, Article 30 points out the key contractual provisions for ICT providers. While ensuring contractual agreements is not in the responsibility of Internal Audit, Internal Audit should verify during audit engagements that the indicated clauses are present.

Article 30 — Key contractual provisions

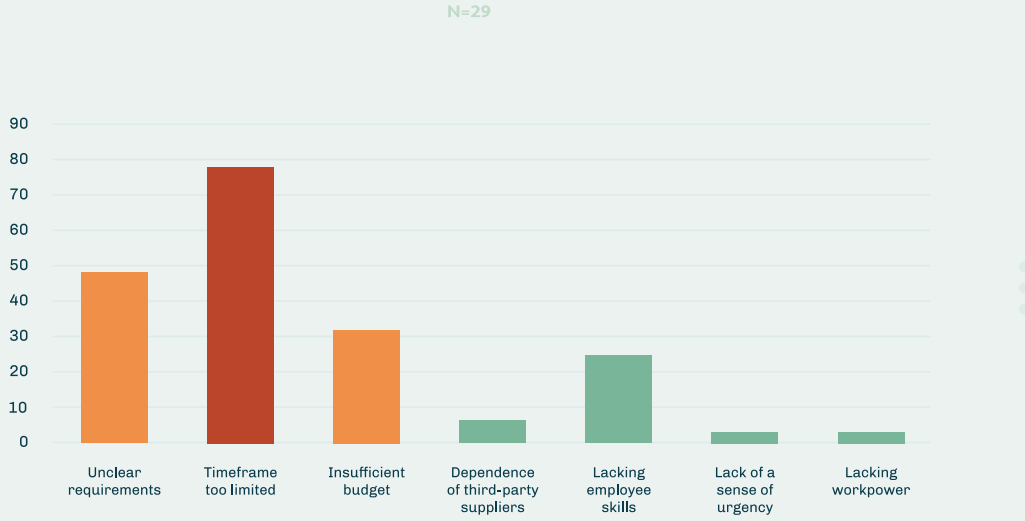
The contractual arrangements on the use of ICT services shall include the following elements: the right to monitor, on an ongoing basis, the ICT third-party service provider's performance, which entails the following:

- **unrestricted rights of access, inspection and audit by the financial entity**, or an appointed third party, and by the competent authority, and the right to take copies of relevant documentation on-site if they are critical to the operations of the ICT third-party service provider, the effective exercise of which is not impeded or limited by other contractual arrangements or implementation policies;
- the right to agree on alternative assurance levels if other clients' rights are affected;
- **the obligation of the ICT third-party service provider to fully cooperate during the on-site inspections and audits performed** by the competent authorities, the Lead Overseer, financial entity or an appointed third party; and
- **the obligation for the provider to provide to the financial entity details on the scope, procedures to be followed and frequency of such inspections and audits.**

2.3 Training and upskilling of internal auditors

To train internal auditors on DORA, a comprehensive and structured approach is needed to ensure they understand the regulatory requirements and can effectively evaluate compliance. Companies face challenges in implementation, particularly with time, budget, skills, and expectations. For an internal audit function, it is essential to help internal auditors understand the requirements and enhance

FIGURE 8 — ANTICIPATED LARGEST ISSUES PREVENTING SUCCESSFUL DORA COMPLIANCE



their skills. This is also reflected in the survey conducted for this paper, where lacking employee skills were found to be the fourth most significant issue preventing DORA compliance (see figure 8).

Trainings could possibly include the following key topics:

- **Introduction to DORA:** Overview of DORA, its purpose, scope, and key requirements.
- **ICT Risk Management:** Understanding ICT risk assessment, identification, and mitigation strategies.
- **Incident Reporting and Management:** Procedures for reporting, managing, and analyzing ICT-related incidents.
- **Operational Resilience Testing:** Methods for conducting resilience testing, including tabletop exercises, simulations, and live testing.
- **Third-Party Risk Management:** Assessing and managing risks associated with third-party ICT service providers.
- **Compliance and Reporting:** Detailed requirements for compliance reporting, documentation, and audit trails.

And moreover:

- **On the job training:** Training for new joiners with more experienced team members.
- **Audit Methodology:** Audit methodologies for evaluating conformance with DORA requirements should be developed and continuously improved based on feedback and continuous learning.

3.0 Detailed audit program for DORA

This section includes recommendations for internal audit functions to plan audits, considerations for audit testing of DORA and a proposed audit program. The views and opinions expressed in this chapter do not necessarily reflect the official policy or position of any agency or organization. The information contained in this paper is for general information purposes only.

1 — Audit planning for DORA: Internal Audit should consider the regulatory deadlines in management actions relevant to DORA and align the audit plan to potential regulatory inspections, if any, to avoid overlaps or coverage gaps. Internal Audit should also consider different focus areas and scopes during a multi-year cyclic plan, such as operational resilience, cyber, critical or important functions (CIFs), and recovery testing. Internal Audit should consider conducting audit activities already in 2024 (e.g., verifying the Company approach for the DORA requirements implementation, such as the execution of an adequate and complete gap analysis, the set-up of a proper program/project with the involvement of all affected functions and the implementation of the related operational activities), and should conduct operational effectiveness audits in the subsequent years.

2 — Audit testing for DORA: Internal Audit needs the means to verify the process of identifying concentration risks with ICT service providers, including downstream dependencies on 4th parties, derived from process maps identifying the most critical resources, technologies, and third parties. Internal Audit also needs to understand the implications of the Union-wide Oversight Framework on critical ICT third-party providers, as designated by the ESAs. Internal Audit should evaluate how assurance for ICT providers can be performed and used, and what it means for the audit approach, such as the right to audit, certifications, ISAE 3402, SOC1 and SOC2.

3 — DORA audit program: This content is not meant to be a comprehensive audit guide for the DORA regulation. It aims to highlight the main controls to customize the review process based on the specific features of each audited entity. By taking into consideration the distinctive attributes of these entities, auditors can efficiently evaluate compliance and pinpoint areas for enhancement.

3.1 Audit Planning for DORA

Auditors should keep challenging the first- and second-line functions to build and maintain proper controls and oversight, while preserving independence. Internal Audit must create a plan to assure sufficient coverage of DORA requirements over the years, consider a first audit in 2024 on design and implementation, and enhance it by auditing operational effectiveness in the following years. Internal Audit may benefit from altering the focus and scope of its cyclic plan (operational resilience, cyber, key functions, recovery tests), opting for in-depth audits rather than auditing the entire scope annually. Plan alignment is required with potential regulatory inspections to prevent overlaps or coverage gaps.

To comply with DORA and improve the operational resilience of financial entities, Internal Audit should prepare and update their audit plans for DORA compliance. Audit planning usually follows the internal audit planning approach and includes these steps:

1 — Assessment of Regulatory Developments: Auditors should learn about DORA and the related policy instruments, including their scope and objectives for improving digital operational resilience.

2 — Audit Risk Assessment: Auditors should evaluate the ICT-related risks that could affect the entity's operations, such as cyberattacks, data leaks, system breakdowns, and other incidents. Analysis of the probability and impact of these risks helps prioritize what to examine in detail.

3 — Audit Scope and Objectives: Auditors should decide what processes, systems, and controls to review, and adapt them to cover all aspects of DORA over a cycle. They must define clear objectives, such as checking compliance with DORA, testing ICT controls, and finding areas for improvement.

4 — Resource Allocation: Auditors should form a team with expertise in ICT, cybersecurity, and regulatory compliance. This may include internal and/or external specialists. They must allocate enough resources, such as budget and time, for a thorough audit. They should align the timeframe with regulatory and internal deadlines. For guidance on how to train auditors on DORA, see section Training and upskilling of Auditors.

5 — Audit Testing: Auditors should choose the methods for collecting data, such as interviews, document reviews, system testing, and data analytics. They should use different audit techniques, such as control testing, substantive testing, and walkthroughs, to gather evidence and assess controls. They should select sampling methods for testing controls and transactions to ensure coverage and reliability of audit results. Regarding regulatory requirements, auditors should compare the entity's practices with DORA requirements to find any gaps or non-compliance issues. They should ensure that all required documentation and evidence of compliance are available and well kept. They should pay special attention to the evaluation of scenario testing (incl. threat-led penetration testing) and whether their results lead to lessons learned and remediation plans. They should also focus on preparing for critical cyber incidents, including training and exercises (drills) with senior management, security operation teams, and business functions.

- **Reporting and Follow-Up:** Auditors should write a comprehensive audit report with findings, conclusions, and recommendations. They should highlight areas of non-compliance and improvement. They should get management's response to audit findings and recommendations. They should ensure that there is a commitment to fix identified issues. They should plan for follow-up actions to check the implementation of recommendations and verify that corrective measures work.

3.2 Audit Testing for DORA

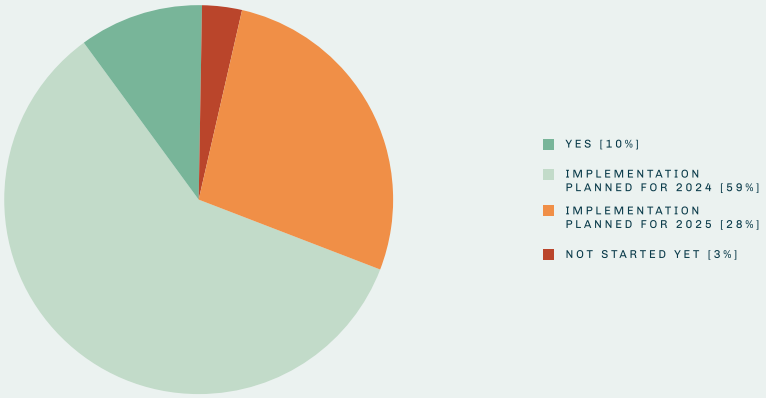
Below are the key elements that should be tested by the Internal Audit function to provide assurance on the main DORA requirements, with evidence of the detailed results of the survey for each specific element.

3.2.1 Resilience

Resilience is crucial and needs testing. As the survey results show, only 25% of the companies have already developed a digital resilience strategy as required by DORA. Internal Audit should plan ahead and consider the evaluation of the audited entity's operational resilience by DORA standards in 2025 at the latest. In 2024, Internal Audit could take various steps, such as checking requirements before implementation and reviewing the methods used by the entities

FIGURE 9 — INSURANCE COMPANIES THAT HAVEN'T DETERMINED A DIGITAL RESILIENCE STRATEGY

N=29

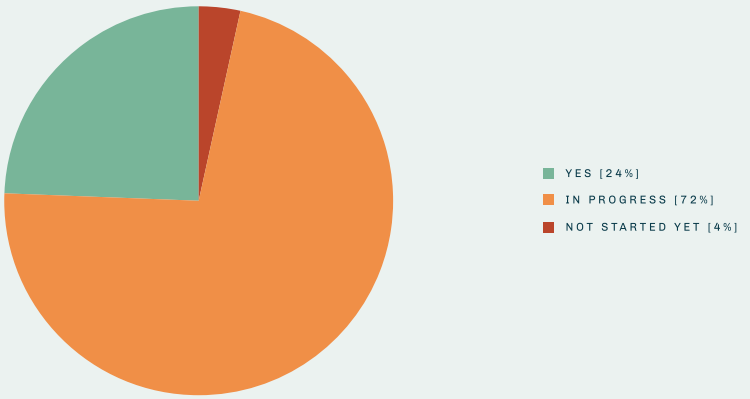


3.2.2 Critical and Important Functions (CIF)

One of the key governance elements of DORA is the identification of Critical and Important Functions (CIF) as outlined in Article 3. As of the first quarter of 2024, only 17% of companies report having implemented CIF identification.

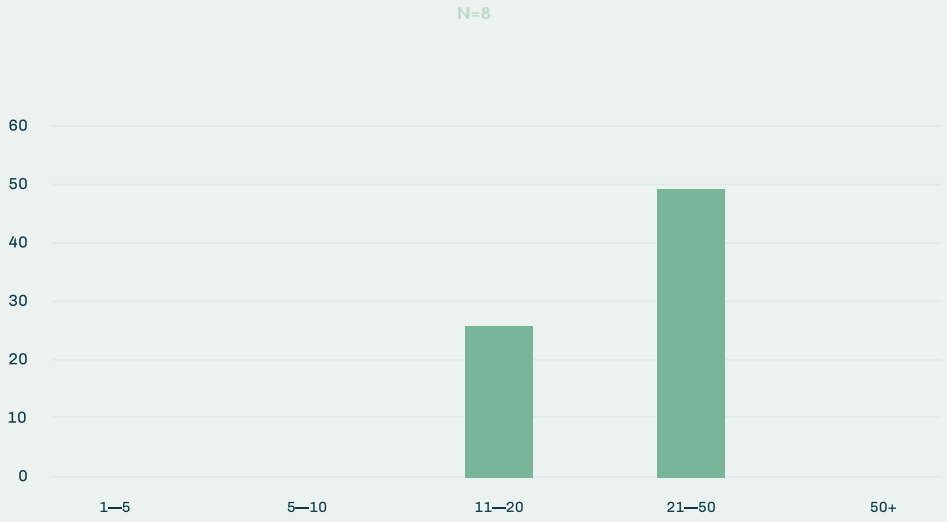
FIGURE 10 — INSURANCE COMPANIES THAT HAVE IDENTIFIED THEIR CIFS

N=29



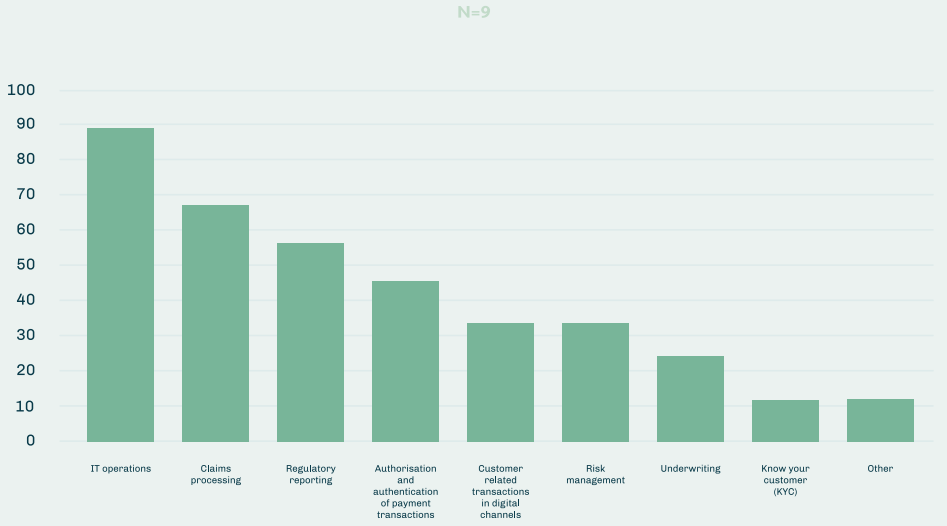
About 16% of companies have more than 50 CIFs, and the figures vary a lot. The more CIFs, the harder it is to implement and provide assurance on them. Internal Audit should use a risk-based approach to select and review CIFs for the audit plan – by rotating or scenario-based assessments. Internal Audit should also test the process for the identification of the concentration risks with ICT service providers that affect CIF (incl. downstream dependencies on 4th parties), based on process maps that show the most critical resources, technologies and third parties.

FIGURE 11 — NUMBER OF CIFS FOUND BY INSURANCE COMPANIES THAT HAVE COMPLETED CIF IDENTIFICATION



Typical functions identified as CIF include IT operations, claims processing, regulatory reporting, and payment authorization.

FIGURE 12 — CIFS THAT COMPANIES ARE PRIORITIZING FOR COMPLIANCE



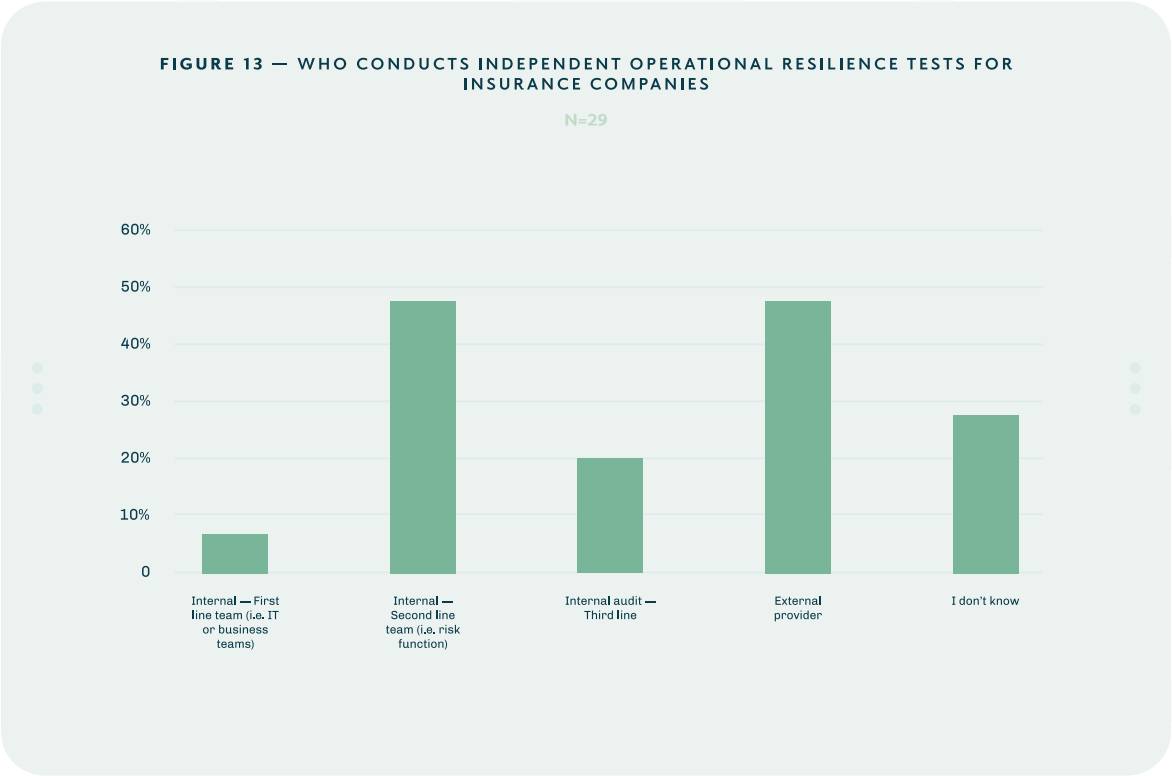
3.2.3 Testing recovery plans

The goal of testing recovery plans is to ensure that they are effective and can be executed successfully in the event of a failure or disaster. It is important to involve all stakeholders, including developers, operations personnel, and other relevant parties responsible for the recovery process..

DORA requires that at least once a year, tests are performed on all ICT systems and applications that are critical or important for the functions they support.

Internal Audit is not typically responsible for performing independent operational resilience tests; only 15% of survey respondents said that Internal Audit conducts these tests themselves. Independent testing can be carried out by an independent function within the first line, the second line, the third line, or by external providers.Internal auditors can review the strategy and performance of the business for recovery tests through different approaches (not exhaustive):

FIGURE 13 — WHO CONDUCTS INDEPENDENT OPERATIONAL RESILIENCE TESTS FOR INSURANCE COMPANIES



- **Tabletop Exercises:** participants walk through the disaster recovery scenarios in a discussion-based format. This helps in identifying gaps in plans and procedures.
- **Simulation disaster recovery tests:** participants perform simulation tests that mimic real-life IT disruptions in a dedicated environment without impacting actual operations. This can include running backup systems or switching to alternative sites.
- **Live disaster recovery testing:** where feasible and safe, live tests involve actual disruptions and may require executing Business Continuity Plans. This can be carried out during planned maintenance windows or in controlled environments.

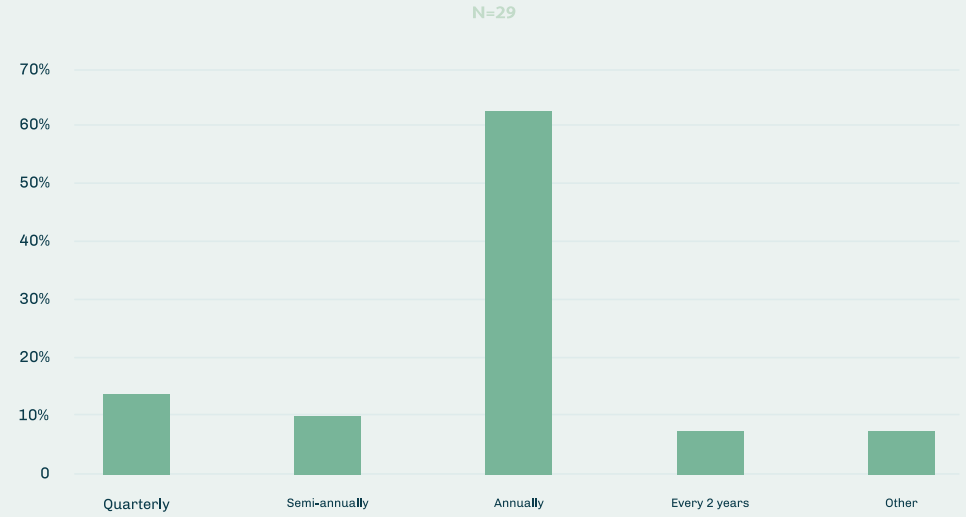
Moreover, different approaches can also be used depending on the scope of the testing activities:

- **Disaster Recovery Tests:** tests can involve only IT systems, such as verifying the adequacy of the Disaster Recovery Plan for recovering IT applications and infrastructure. In this case the business owners of the applications are usually involved to verify Recovery Time Objective and Recovery Point Objective requirements and functionalities of the applications.
- **Business Continuity Test:** tests involve both IT systems and the associated business processes to ensure these processes are effectively recovered. This typically includes relocating personnel from one business site to another or testing remote work capabilities.

DORA requires financial entities to have redundant ICT capacities to support business needs during disruptions. This can include backup systems, such as extra servers or cloud-based infrastructure, that can switch over quickly and smoothly if the main systems fail. The survey collected data on the frequency of backup, restoration, and recovery testing for insurance companies.

The frequency of recovery plan testing can vary depending on the specific organization and the criticality of the systems being tested. However, it is generally recommended to test recovery plans on a regular basis, at least once a year or whenever there are significant changes to the infrastructure, applications, or business processes. Most surveyed companies test their recovery plans annually. There are a few companies which test more frequently and only a minority test less often than the required annual frequency.

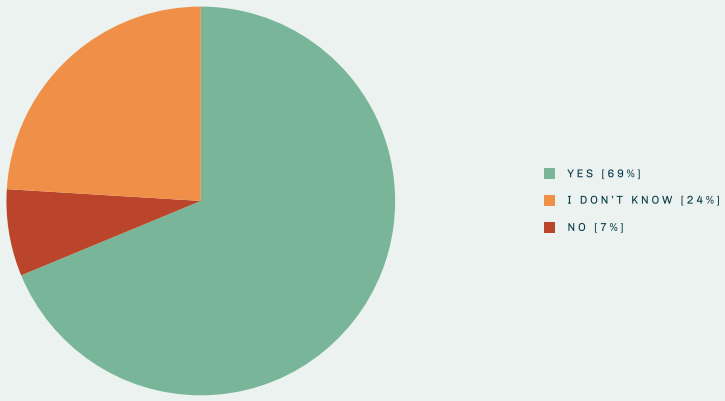
FIGURE 14 — FREQUENCY OF BACKUP-, RESTORATION-, AND RECOVERY PROCEDURE TESTING FOR INSURANCE COMPANIES



It can be beneficial for the internal audit function to be involved in disaster recovery tests and observe the actual exercises, rather than just reviewing test documents during desk reviews. According to the survey, 69% of companies test the recovery of applications as part of their Disaster Recovery Plan (DRP) testing

FIGURE 15 — COMPANIES THAT TEST THE RECOVERY OF APPLICATIONS AS PART OF THE DISASTER RECOVERY PLAN TESTING (END-TO-END TEST)

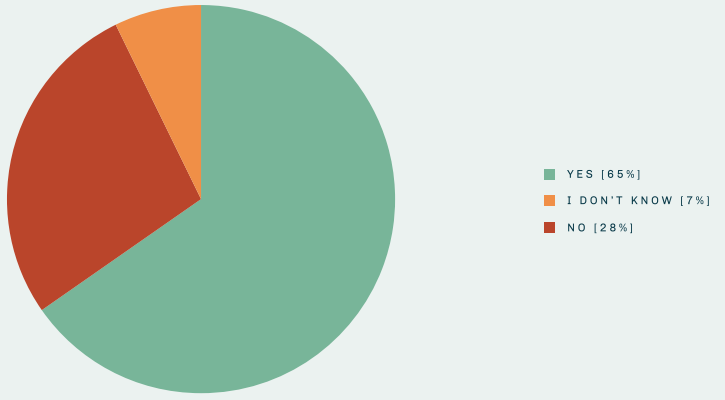
N=29



During internal audits, auditors check the ICT response and recovery plans, which include the ICT business continuity plans and the ICT response and recovery plans. 65% of companies reported full compliance with these requirements.

FIGURE 16 — ICT RESPONSE AND RECOVERY PLANS SUBJECT TO INDEPENDENT INTERNAL AUDIT REVIEWS, INCLUDING THE ICT BUSINESS CONTINUITY PLANS AND THE ICT RESPONSE AND RECOVERY PLANS IN RELATION TO ICT SYSTEMS SUPPORTING ALL FUNCTIONS

N=29

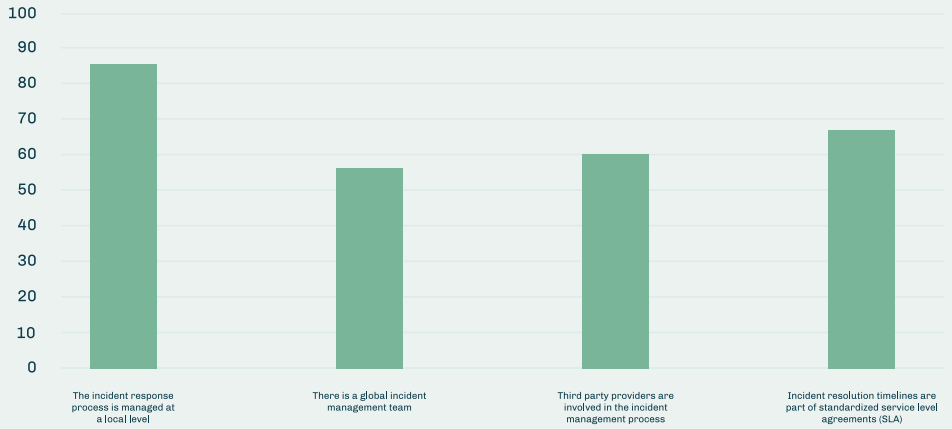


3.2.4 Incident response

Companies use different approaches to organize incident management and response – the majority of companies rely on a local process, the larger ones have a global team including third party providers. Internal auditors need to define their tests according to the organisational approach. In any case it is important that reporting within the organisation, and also to regulators, is handled effectively by the financial entity.

FIGURE 17 — INSURANCE COMPANIES' STANDARDIZED INCIDENT RESPONSE PROCESS

N=27

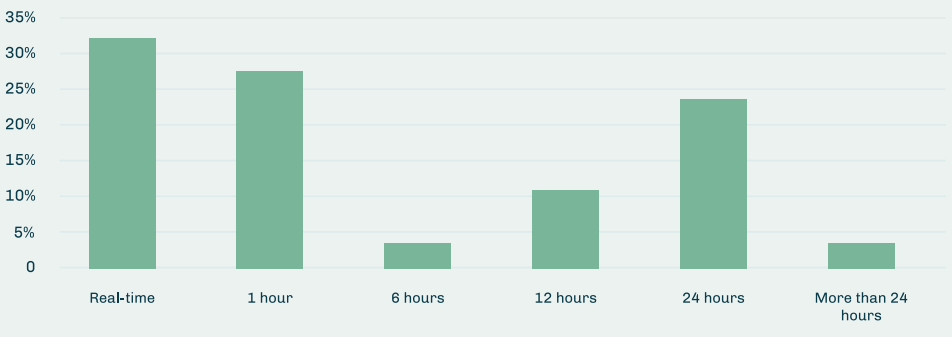


3.2.5 Notification to the regulator

Best practice is a real time detection of ICT issues; only a few companies stated in the survey to require more than 24 hours. Overall, the survey results give the impression that many companies still need to invest to achieve the DORA requirements of 4 hours for the initial notification.

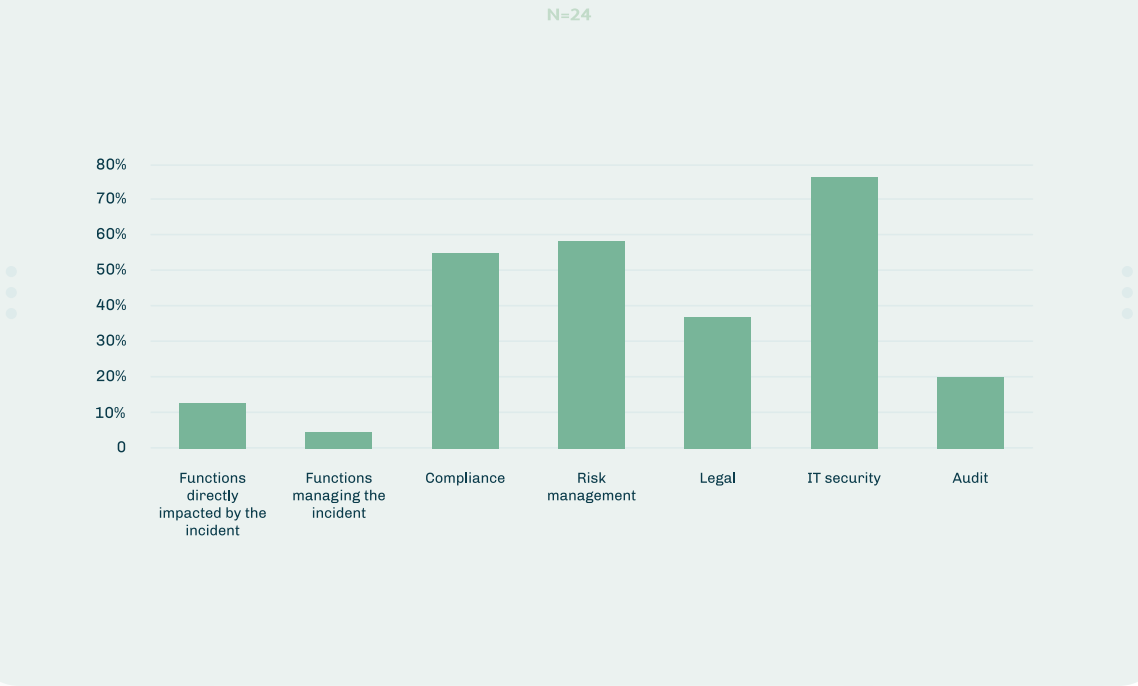
FIGURE 18 — WHAT INSURANCE COMPANIES CONSIDER TO BE "PROMPT DETECTION" OF IT ISSUES AS DETERMINED BY ARTICLE 10(1)

N=29



Functions involved in incident notification are typically IT Security, Risk Management. According to the survey results, Internal Audit is involved in only a minority of companies.

FIGURE 19 — FUNCTIONS INVOLVED IN THE ICT INCIDENT NOTIFICATION PROCESS IN INSURANCE COMPANIES



3.2.6 ICT audits

The DORA regulation has ICT specific implications for Internal Audit and the audit approach. Internal Audit needs to include specific tests for the relevant DORA requirements in their audit plan. IT auditors should have the knowledge and expertise to test DORA ICT requirements, which are specific and usually define key IT security requirements. They cover all aspects of IT security, from managing IT assets, to encryption and cryptographic controls, vulnerability and patch management, data and system security, network security, ICT project and change management, human resources policy and access control, ICT-related incident detection and response and ICT business continuity management (see the RTS risk management framework for details). It is not possible to test all these controls in one audit engagement, even for big organisations, that's why it is strongly recommended that Internal Audit should test them based on a risk-based approach over a multi-year audit plan. As many of the DORA concepts are already in place, first, second and third lines often use existing standards and polices to handle regulatory requirements in large organizations. Often, a mapping of policies and regulatory requirements to existing standards can support risk assessment, control definitions and the audit approach and coverage. In any case, it is essential that specific DORA principles and requirements are clearly communicated, documented and tested.

Specific standards for assurance over third parties can support third party assurance from such an independent tester. This type of assurance requirements can be built into contractual agreement (Right to Audit, requirements for a generic or specific independent audit report (as defined by the standards ISAE 3402, SOC1 and SOC2)). Such standards are, however, general in nature and do not consider specific DORA requirements:

- **SOC 2:** A set of guidelines for service providers who store customer data. It was created by the American Institute of Certified Public Accountants (AICPA) and outlines how to manage customer data based on five "trust service principles"—security, availability, processing integrity, confidentiality and privacy.

- **ISAE 3402:** An international assurance standard that defines Service Organization Control (SOC) engagements, which give confidence to a service organization's customer that the service organization has good internal controls. ISAE 3402 was issued by the International Auditing and Assurance Standards Board (IAASB) and published by the International Federation of Accountants (IFAC) in 2009. It replaces SAS 70 and focuses more on the continuous monitoring and assessment of controls.

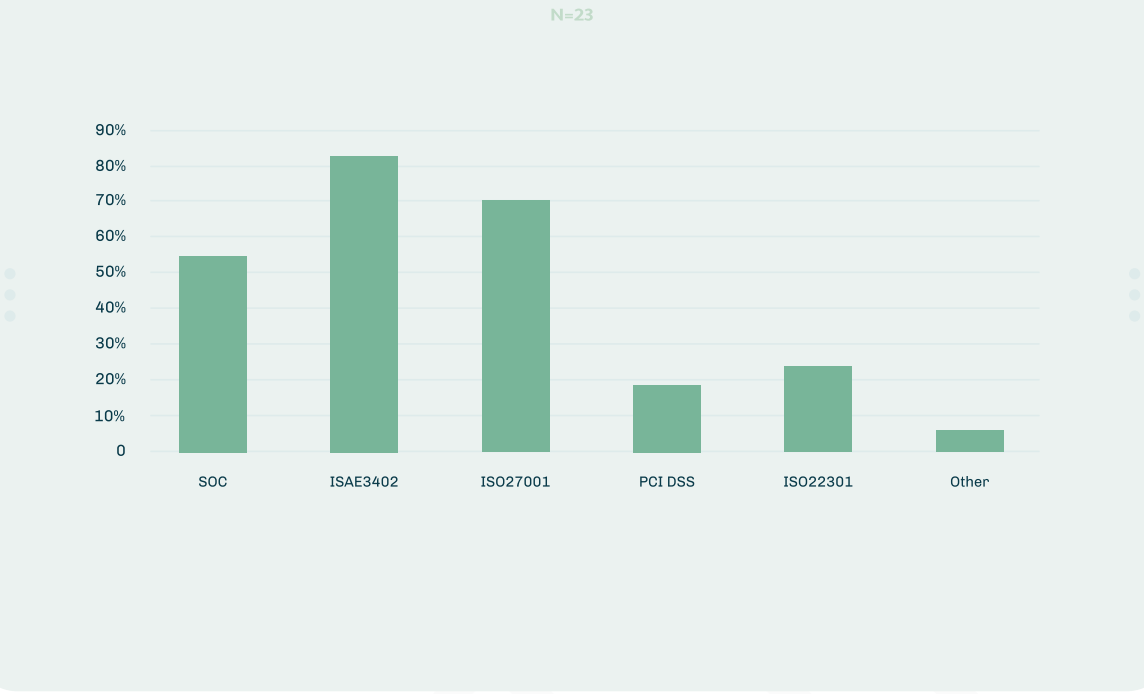
- **PCI DSS:** The Payment Card Industry Data Security Standard is a set of security standards designed to ensure that all companies that accept, process, store, or transmit credit card information maintain a secure environment.

- **ISO 27001:** This is the international standard for Information Security Management Systems (ISMS). It provides a framework for establishing, implementing, maintaining, and continually improving an information security management system

- **Resilience standards ISO 22316:2017 - Security and resilience - ISO 22316:2017** provides guidance to enhance organizational resilience for any size or type of organization. It is not specific to any industry or sector.

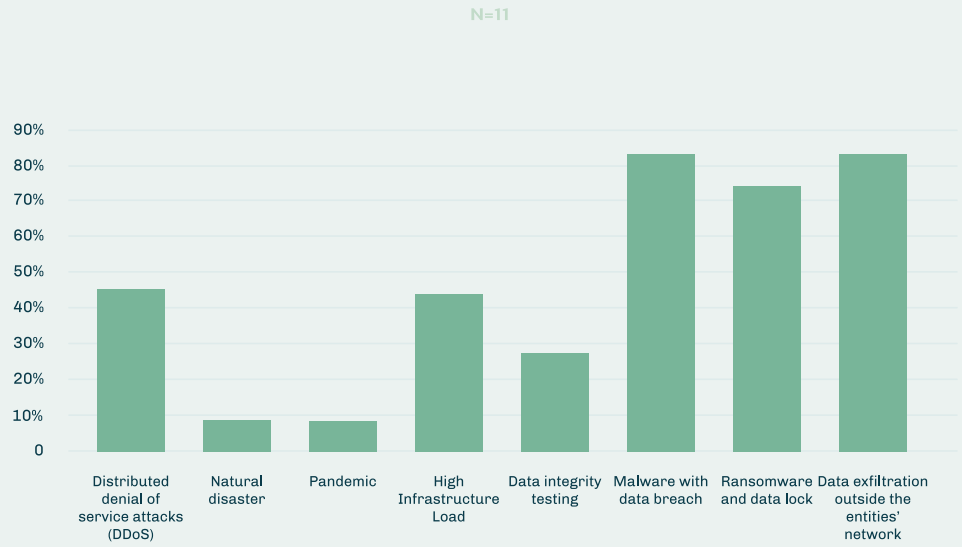
These standards are also supported by certifications that companies rely on for third-party risk assessments, according to survey respondents.

FIGURE 20 — CERTIFICATIONS THAT COMPANIES WOULD RELY ON WHEN PERFORMING THIRD PARTY RISK ASSESSMENTS



It often makes sense to test certain scenarios on a cyclical basis to ensure that the control environment is robust against different types of potential disruptions and/or attacks. Internal auditors should understand typical scenarios, associated risks and advantages/disadvantages of the testing scenarios. Our survey found that cyber scenarios are tested most frequently, while infrastructure-related scenarios, such as natural disasters and physical risks, are tested less often.

FIGURE 21 — SCENARIOS TESTED DURING TLPT AT INSURANCE COMPANIES



Below is a non-exhaustive list of some key elements for simulated attacks.

Attack types:

- *Ransomware Attacks:* In this scenario, a hacker infiltrates a system and locks out users, demanding a ransom to restore access.
- *Phishing Attacks:* testing of this scenario is to understand how hacker sending a seemingly harmless email to an employee, which contains a malicious link or attachment aimed to steal sensitive data or install malware.
- *Malware Infection:* This scenario involves a malicious software infiltrating the organization's network, which can lead to data theft, system damage, or other harmful outcomes.
- *DDoS Attack:* A Distributed Denial of Service attack scenario involves overwhelming a network, service, or server with traffic to make it unavailable to its intended users.
- *Zero Day Exploit:* A vulnerability in software or hardware that is typically unknown to the vendor and for which no patch or other fix is available.
- *Multi-factor Authentication Fatigue Attack (Also known as MFA bombing or MFA spamming):* An attacker sends a flood of login attempts in the hope that a user will click on "accept" at least once.

Attack Origins:

- *Insider Threat:* This scenario involves an employee or other insider maliciously or unintentionally causing a security breach.

- *Advanced Persistent Threat (APT):* A broad term used to describe a campaign in which attackers establish a long-term presence on a network in order to mine highly sensitive data. These attackers are often experienced and may be government-funded.

Attack targets:

- *Supply Chain Attack:* In this scenario, a hacker compromises a trusted vendor or supplier to gain access to your system.
- *Cloud Security Breach:* This scenario involves unauthorized access or manipulation of data stored in the cloud.
- *Web Application Attack:* This involves an attacker exploiting a vulnerability in a web application to gain unauthorized access or disrupt the service.
- *Mobile Device Attack:* In this scenario, a mobile device like a smartphone or tablet is compromised, often through malicious apps or phishing, to gain access to sensitive data or systems.

Attack Consequences:

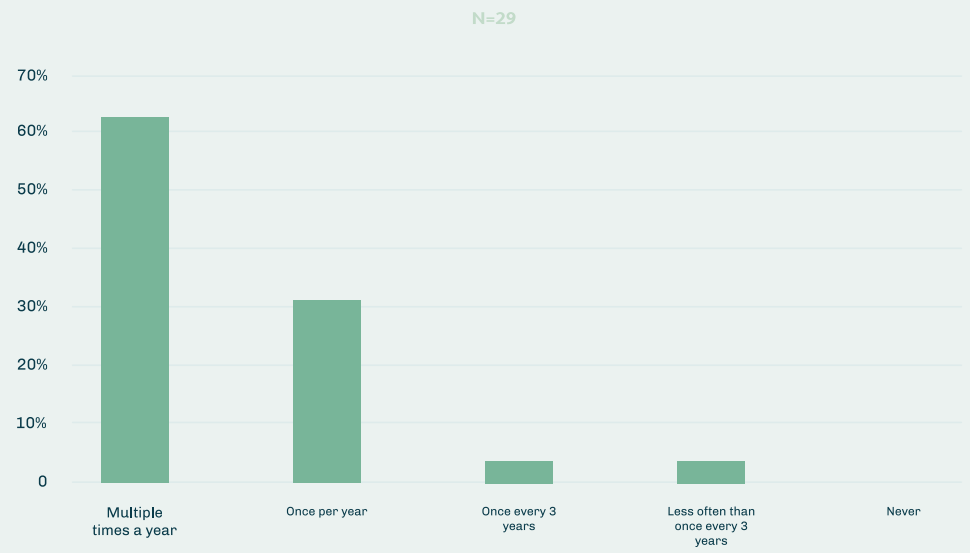
- *Maximum Credible Event:* For resilience of a single corporation that could mean for example that an attack would delete or encrypt all data, including all backup data, and the company would stop to operate as it would not be able to recover data – only current solution for such an event is so called cybervaulting (creating an isolated copy of data in the production environment).
- *Data Breach:* This scenario involves unauthorized access to sensitive data, such as customer information, financial data, or intellectual property.

3.2.7 Penetration testing

3.2.7.1 Threat-led penetration tests

Article 26 mandates Advanced testing of ICT tools, systems and processes based on Threat-Led Penetration Tests (TLPT). TLPTs are simulated cyberattacks based on current threats to identify security vulnerabilities that cover at least the critical functions and services of the financial entity and are conducted on the real production systems that support them. Financial entities define the scope of TLPT, based on the evaluation of critical functions and services, by finding the related ICT processes, systems and technologies, including functions and services outsourced or contracted to third-party ICT service providers. Based on the survey, companies typically conduct at least one test per year, usually driven by the First or Second Line, and only rarely by Internal Audit functions (next page).

FIGURE 22 — FREQUENCY OF PENETRATION TESTING OF INSURANCE COMPANIES

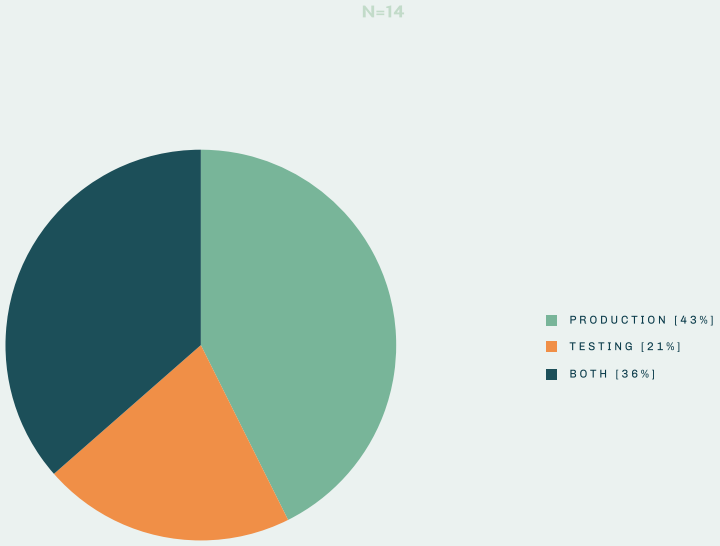


3.2.7.2 TLPT on testing or production environments

If penetration tests are conducted in the development environment, they need to match the production as much as possible to ensure the testing is reliable and insightful. Penetration tests done in production environments can detect all of types of issues and how serious their impact is in real time. This allows to correct any security gaps timely, however it requires a coordinated effort with key functions involved to avoid disruption of the business.

According to the survey, most insurance companies test in production, but testing in test environments or using combined approaches is also quite common.

FIGURE 23 — ENVIRONMENTS IN WHICH TLPT TESTS ARE PERFORMED BY INSURANCE COMPANIES



DORA (Article 26) requires a TLPT to be conducted at least every 3 years, and at a minimum every 3 tests should be executed by the so-called Red Team an external penetration test team mimicking an external attacker, according to the proportionality principle. According to experience within the industry a mix of internal and external teams is most efficient. As highlighted above, these tests are usually managed by First- or Second-Line Functions on a regular basis, while Internal Audit may independently evaluate the quality of these tests and the respective controls. Credit institutions that are classified as significant in accordance with article 6 of Regulation (EU) No 1024/2013, shall only use external testers in accordance with DORA (article 27).

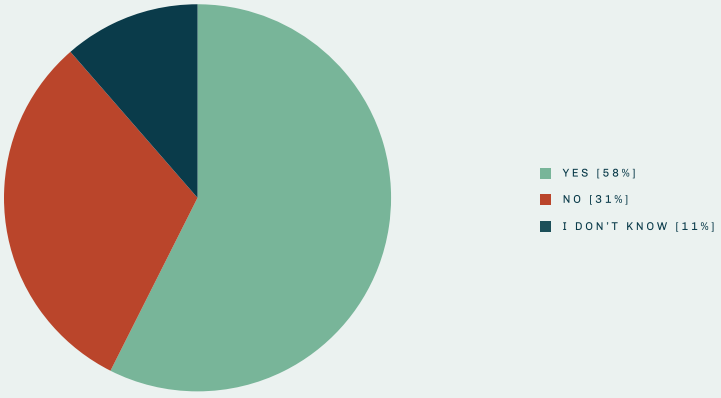
FIGURE 24 — TEAM SETUPS DURING TLPT TESTING

N=29

The survey confirms that the majority of companies already involve external parties in their penetration testing activities.

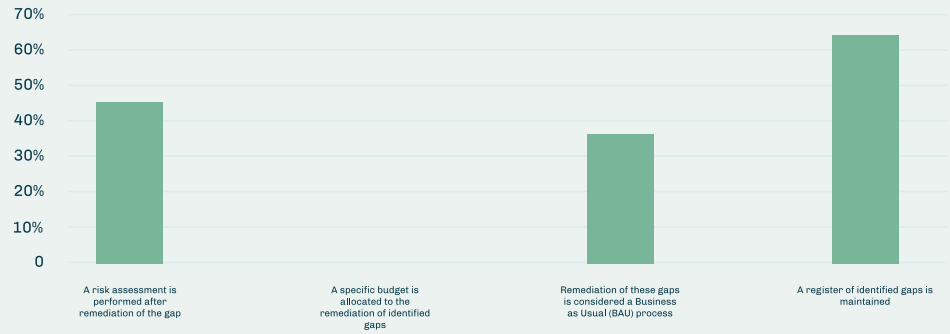
FIGURE 25— COMPANIES THAT INVOLVE THIRD PARTIES IN THEIR TLPT TESTING

N=26



Most of the surveyed companies formally manage their cybersecurity gaps, but none allocate a specific budget to address these gaps. However, just around 40% of insurance companies consider fixing them to be a Business as Usual (BAU) process. This means that around 60% have no specific budget for those gaps but also don't consider them in their BAU process, which may indicate lacking budget allocated to those shortcomings.

FIGURE 26 — HOW INSURANCE COMPANIES DEAL WITH GAPS IDENTIFIED DURING PENETRATION TESTING



3.2.8 Managing the Outsourcing Risk

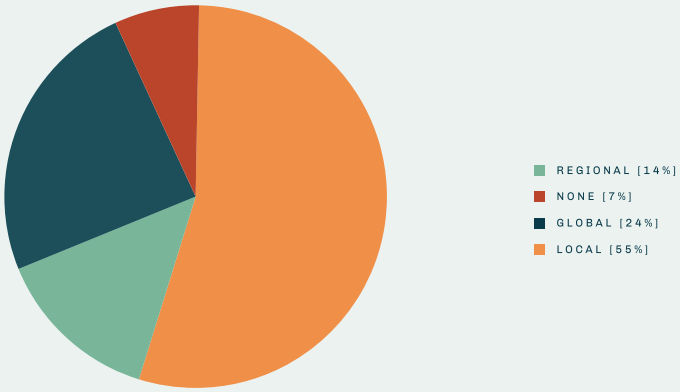
3.2.8.1 Third-Party audits

DORA has very specific requirements on ICT third-party risk and requires controls to be applied during the whole third-party management lifecycle (Article 28). In particular, as part of a third line accountability, Internal Audit should test the overall governance, the accountability for ICT third-party management and the related reporting. Financial entities shall report at least yearly to the competent authorities on the number of new arrangements on the use of ICT services (Article 27 of the RTS for ICT risk management framework specifies the format and content of the report on the review of the ICT risk management framework which need to be submitted to the regulator), as well as assess the contractual arrangement management, including the exit strategy for ICT services supporting critical or important functions.

One of DORA's main goals is to assess and monitor the risks that arise from working with third parties. The RTS for ICT risk management framework defines rules and standards that financial institutions (FIs) need to comply with when they rely on ICT third-party service providers (TPS). The RTS lays out guidelines and requirements that financial institutions have to follow when contracting ICT third-party service providers. Most companies (55%) have a local oversight model in place for third parties, as opposed to 38% with a global or regional oversight model (next page):

FIGURE 27 — OVERSIGHT MODEL USED FOR THIRD PARTY PROVIDERS

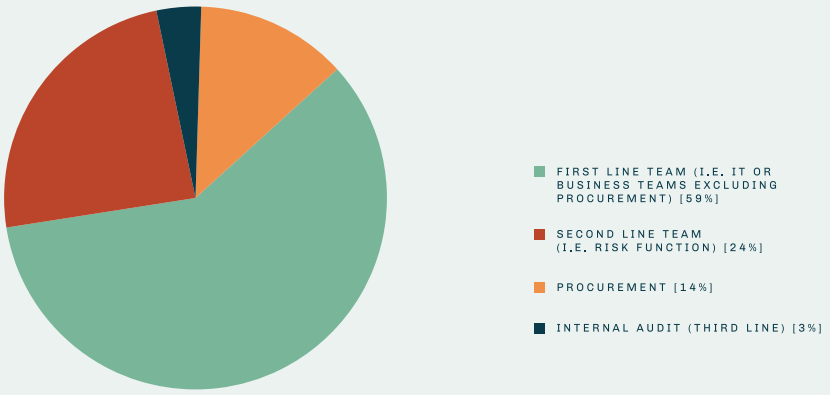
N=29



Based on the survey, the majority of the companies apply a first-line principle for accountability for the third-party risk assessment, as opposed to allocating this responsibility to the second-line risk management function.

FIGURE 28 — WHO IN INSURANCE COMPANIES IS ACCOUNTABLE TO PERFORM THIRD PARTY RISK ASSESSMENTS

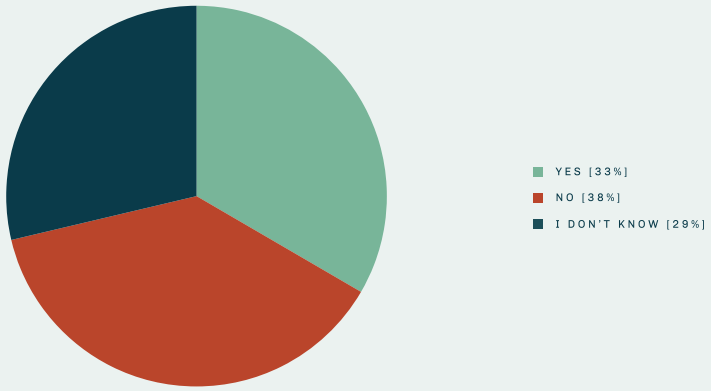
N=29



Another result of the questionnaire indicates that the management of third-parties should be strengthened further. Just a quarter of the response indicate that a multi-vendor strategy – as described and required in Article 6 (9) by DORA – has been established in their company. An ICT multi-vendor strategy is required to identify key dependencies on third party ICT providers, and to explain the rationale procurement mix.

FIGURE 29 — INSURANCE COMPANIES THAT HAVE ESTABLISHED A MULTI-VENDOR STRATEGY

N=21

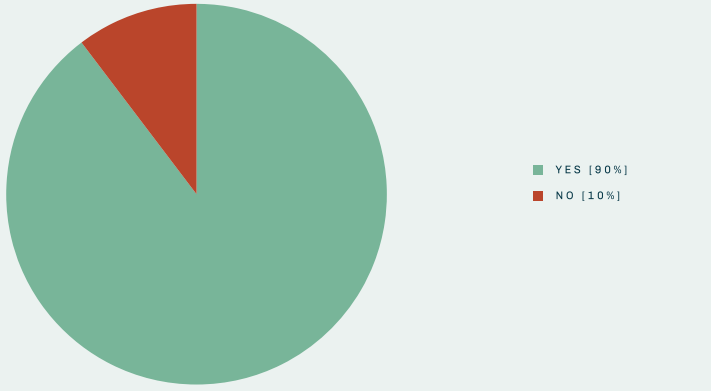


3.2.8.2 Standards for Third Party audits and the Right to Audit

The positive message in this context is that the vast majority (90%) of participants in the survey have audit rights defined within their third-party contracts, which makes it possible to execute audits on the provider. Such audits can also be provided by an independent tester.

FIGURE 30 — INSURANCE COMPANIES WITH AUDIT RIGHTS DEFINED IN THEIR THIRD PARTY CONTRACTS

N=29

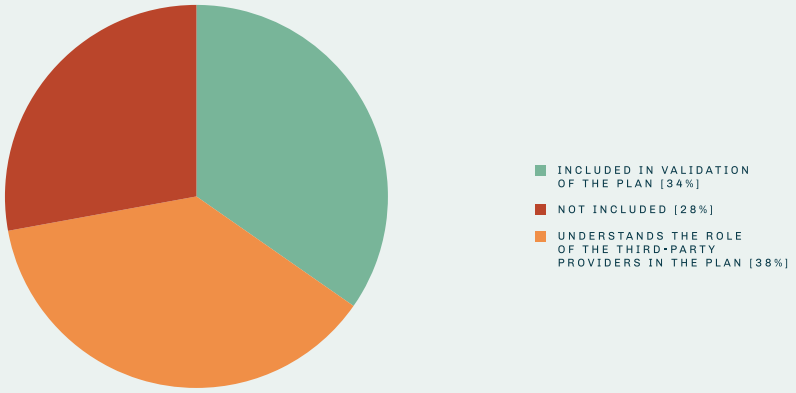


3.2.8.3 Incident management and Third Parties

As a first example for the elevated necessity to audit third parties, the question was raised on the extent to which third party providers are included in the validation of incident response plans. The results showed that only 34% include third-party service providers in the validation of incident response plans, when 38% know and have evaluated the role of third-party service providers in these plans. About 28% of companies have not included third-party service providers in their incident response plans, which poses a significant risk that should be evaluated during audit engagements.

FIGURE 31 — INSURANCE COMPANIES THAT HAVE INCLUDED THIRD PARTIES IN THE VALIDATION OF THE INCIDENT RESPONSE PLAN(S)

N=29

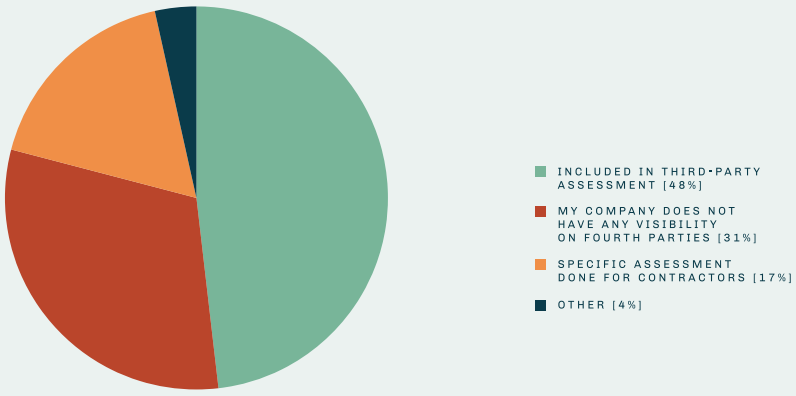


3.2.8.4 Fourth Parties

4th-party risk is the term used to describe the possible dangers and weaknesses that come from the subcontractors, vendors, or service providers that work with an organization's direct third-party service provider. Our survey found that 4th-party risks is primarily covered by third-party assessments:

FIGURE 32 — HOW INSURANCE COMPANIES HANDLE FOURTH PARTIES

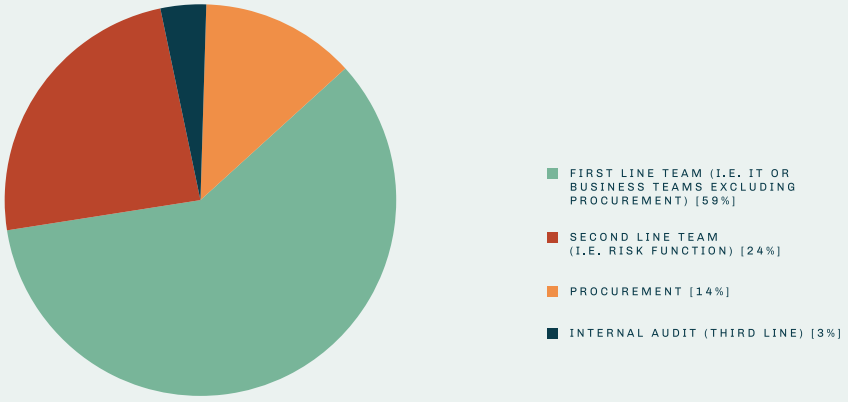
N=29



DORA Article 28(6) states that “in exercising access, inspection and audit rights over the ICT third-party service provider, financial entities shall, on the basis of a risk-based approach, pre-determine the frequency of audits and inspections as well as the areas to be audited through adhering to commonly accepted audit standards in line with any supervisory instruction on the use and incorporation of such audit standards.”.

FIGURE 33 — WHO IN INSURANCE COMPANIES IS ACCOUNTABLE TO PERFORM THIRD PARTY RISK ASSESSMENTS

N=29



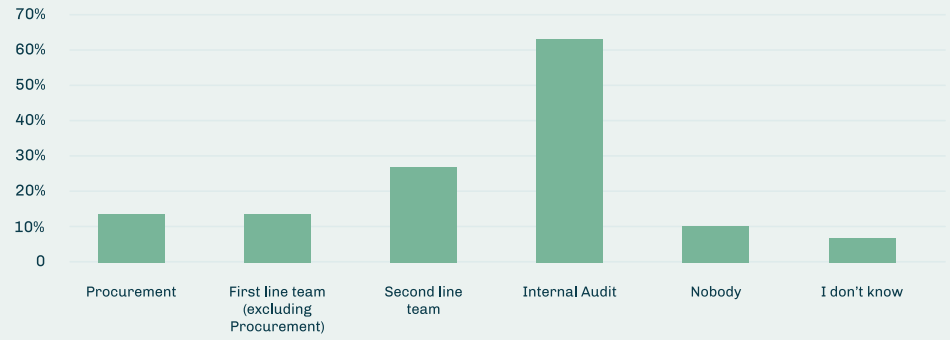
ICT third-parties have their own regulatory regime defined in DORA, and inspection rights of the Lead Overseer are defined in Article 39 and 40.

DORA Article 30 defines the obligations for the third party as ”the obligation of the ICT third-party service provider to fully cooperate during the onsite inspections and audits performed by the competent authorities, the Lead Overseer, financial entity or an appointed third-party; and the obligation to provide details on the scope, procedures to be followed and frequency of such inspections and audits”.

Most companies taking part in the survey answered that Internal Audit performs third party audits. However, it makes sense that also first and second line – according to their accountabilities – perform third-party assessments to establish assurance on the control framework of the ICT third-party service provider and not solely rely on the third line (next page).

FIGURE 34 — WHO PERFORMS THIRD PARTY AUDITS IN INSURANCE COMPANIES

N=29



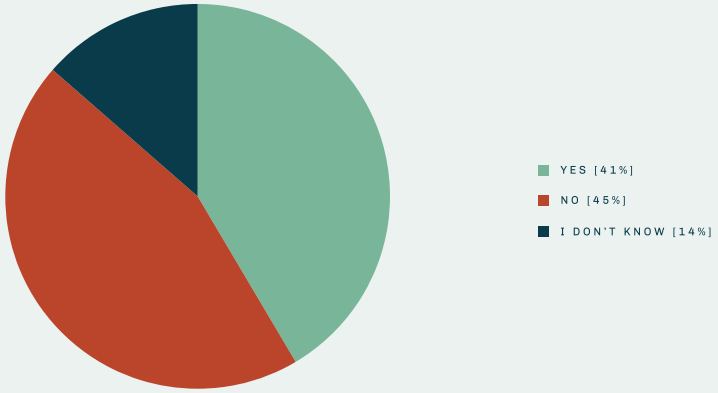
3.2.8.5 Pooled audits for Third Parties

DORA emphasizes the importance of auditing third-party service providers and points to the option of facilitating **pooled audit resources** to achieve this common goal.

The experience with pooled audits is divided. It seems to be a 50/50 split between companies that have already had experience in this field and those where it is an entirely new approach. The majority of companies that have already gained experience in this field come from the banking sector, where this topic appears to be present for a longer time.

FIGURE 35 — INSURANCE COMPANIES PERFORMING POOLED AUDITS WITH THIRD PARTY PROVIDERS

N=29



The key advantage of pooling audit resources to address the risks is the creation and consolidation of appropriate skills and knowledge – in addition to learning from each other – to effectively perform these audit engagements on service providers and creating the necessary human resources to evaluate the not uncommon complex environment and assess the comprehensive number of controls IT service providers have established.

An additional benefit of the pooling approach is that it creates leverage with large third-party service providers, allowing a critical mass of customers to more effectively exercise their rights. This approach also generates synergies for the third-party providers, as they no longer need to manage and coordinate numerous separate customer audits. They as well can facilitate one or just a lower number of pooled audits in an adequate and efficient way.

However, this idea or approach is not entirely new, but it is now welcomed to be stipulated by European law. A group of financial institutions formed the Collaborative Cloud Audit Group for the Financial Services Industry in the European Union (CCAG). This group formed an association for financial institutions to join. They have their primary focus on Cloud Service Providers (CSP) and for now the big three (Microsoft, Amazon and Google) in scope, but are open to extending their range of evaluation based on the needs of their members.

The CCAG's vision is: "Supporting Internal Audit departments of CCAG members in compliance with the EU regulations of the financial industry using a common collaborative audit methodology for building independent, objective assurance to Cloud Services. The CCAG Association provides an efficient and scalable approach at a fair share for its members."

In addition to the general vision and strategy of the group a solid audit framework incl. clear methodology and process descriptions comes with it. The non-profit oriented organization provides in addition to that a central administration including a common IT platform, structured cooperation between CCAG members and the establishment of core teams per CSP.

In order to understand if an initiative like the CCAG meets the requirements stipulated by DORA towards third-party service provider the revisit of the concrete passages of the DORA Article 28, point 6 is of use: "In exercising access, inspection and audit rights over the ICT third-party service provider, financial entities shall, on the basis of a risk-based approach, pre-determine the frequency of audits and inspections as well as the areas to be audited through adhering to commonly accepted audit standards in line with any supervisory instruction on the use and incorporation of such audit standards. Where contractual arrangements concluded with ICT third-party service providers on the use of ICT services entail high technical complexity, the financial entity shall verify that auditors, whether internal or external, or a pool of auditors, possess appropriate skills and knowledge to effectively perform the relevant audits and assessments."

To understand how the CCAG approach fits into this, it must be clarified that the audit process of the CCAG splits in five phases:

1. Pre-Preparation
2. Audit Preparation
3. Fieldwork
4. Results Reporting
5. Lessons Learned

Particularly the first phase addresses the regulators' requirement for a risk-based approach and predetermined audit frequency. In this phase the group aligns which members are participating in a planned audit based on the individual members' risk assessments and audit needs. For this reason, each member has the possibility to follow their risk-based approach. In the Pre-Preparation phase, it also becomes clear how the audit team looks like, which auditors with which skillset are joining the particular audit engagement. For this reason, each institute can – before the Audit Preparation phase starts – assess if the stipulated appropriate skills and knowledge to effectively perform the relevant

audits are given and could potentially take countermeasures. But since from each participating financial institute at least one auditor has to be provided, it is highly unlikely that resources are not provided in the necessary quality or quantity.

The next three phases are in line with common audit standards since members generally adhere to global audit standards and for this reason these phases align as well with those requirements. The fifth and last phase is called Lessons Learned and services the purpose of learning from the particular audit and sharpen the approach for the future.

The attentive reader might have noticed that a follow-up phase is missing in the CCAG audit process. This is because the group summarizes key conclusions, but the individual audit report is issued by every financial institute individually. For this reason, the follow-up process is as well performed by each financial institution individually.

This already field-tested approach of pooled auditing in the area Cloud Service Provider (CSP) can be seen as a good example of how this DORA requirement can be put into practice.

3.3. DORA audit program

The following content does not aim to provide a complete audit guide for the DORA regulation. Instead, it focuses on extracting the key audit controls to tailor the review process according to the specific nature of each audited entity. By considering the unique characteristics of these entities, auditors can effectively assess compliance and identify areas for improvement.

3.3.1 Governance and Organisation

Area	*DORA requirement*	*Indicative matters to consider*
Governance and organisation	General	• At first, the audit team should evaluate if the entity has completed a GAP analysis to identify potential DORA requirements that are not implemented, or whose level of implementation is not adequate. The output of this GAP analysis should be a comprehensive action plan to address those controls that are not fully met. The audit team should verify if this analysis has been performed, and the status of the corresponding action plans. • The proportionality principle should consider the entity´s size and overall risk profile, and the nature, scale and complexity of their services, activities and operations. As such, the audit team should review how this principle has been defined and implemented within the organization. This will determine the rest of the efforts to ensure DORA compliance. • Considering the proportionality principle, the next step should be to identify the critical or important functions of the organization. The auditor should evaluate the completeness and adequacy of the process that has been followed to determine those functions.

3.3.2 ICT Risk Management

Area	DORA requirement	Indicative matters to consider
ICT risk management[1]	Financial entities shall identify all information assets and ICT assets, including those on remote sites, network resources and hardware equipment, and shall map those considered critical. They shall map the configuration of the information assets and ICT assets and the links and interdependencies between the different information assets and ICT assets.	For this purpose, the audit team should assess how the entity is managing ICT assets inventories. As an example, to streamline this effort, some companies may be using Configuration Management Database (CMDB) software.
ICT risk management	Financial entities shall identify and document all processes that are dependent on ICT third-party service providers and shall identify interconnections with ICT third-party service providers that provide services that support critical or important functions.	The internal audit team should request the list of service providers that are supporting any of the critical or important functions and evaluate its completeness and accuracy.
ICT risk management	The ICT risk management framework shall include at least strategies, policies, procedures, ICT protocols and tools that are necessary to protect all information assets and ICT assets (computer software, hardware, servers, physical components, etc). Also, it shall be documented and reviewed at least once a year, or periodically in the case of microenterprises, as well as upon the occurrence of major ICT-related incidents.	The internal audit team should regularly review the ICT risk management framework in line with the financial entities' audit plan.
ICT risk management	Financial entities shall ensure appropriate segregation and independence of ICT risk management functions, control functions, and internal audit functions, according to the Three Lines of Defence Model, or an internal risk management and control model.	Internal Audit should assure in all their audit engagements that the required independence of all functions is assured. Internal Audit should be independent.
ICT risk management	The ICT risk management framework shall define a holistic ICT multi-vendor strategy, at group or entity level, showing key dependencies on ICT third-party service providers and explaining the rationale behind the procurement mix of ICT third-party service providers.	Internal Audit should review the ICT multi-vendor strategy
ICT risk management	Financial entities shall design, procure and implement ICT security policies, procedures, protocols and tools that aim to ensure the resilience, continuity and availability of ICT systems, in particular for those supporting critical or important functions.	Some minimum controls to be audited are: The Information Security Policy; • Physical or logical access controls to ICT assets; • Strong authentication mechanisms (in example, Multi Factor Authentication); • Documented policies, procedures and controls for ICT change management; • Documented policies for patches and updates.

1 Further requirements are being developed by the ESAs, through the Joint Committee and in consultation with the ECB and ENISA, within RTS/ITS 6.5, 9.2 - 9.4.c, 10.1 - 10.2, 11.1 - 11.3 - 11.6 and 11.10.

Area	*DORA requirement*	*Indicative matters to consider*
ICT risk management	As part of the ICT risk management framework financial entities shall put in place a comprehensive ICT business continuity policy, including a Business Impact Analysis (BIA). Moreover, entities should have in place ICT response and recovery plans.	This documentation should be evaluated by the internal audit team, making sure that the entity has allocated enough resource to ensure the recovery of its critical or important functions in case of disruption in its business operations.
ICT risk management	Financial entities shall: (1) test the ICT business continuity plans and the ICT response and recovery plans in relation to ICT systems supporting all functions at least yearly, as well as in the event of any substantive changes to ICT systems supporting critical or important functions; (2) test the crisis communication plans established.	The internal audit team should request all the documentation of the latest ICT business continuity plan, as well as the process defined to re-test when substantive changes to ICT systems are performed. Moreover, the crisis communication plan should be requested and evaluated, including any supporting evidence of the activation of the communication plan, if applicable.
ICT risk management	Financial entities shall have a crisis management function.	Auditors should verify if this function has been properly formalized, including the definition of the corresponding responsibilities.
ICT risk management	Financial entities shall report to the competent authorities, upon their request, an estimation of aggregated annual costs and losses caused by major ICT-related incidents.	For this purpose, internal auditors should assess the manual and/or automated processes that are defined to calculate and report ICT incidents costs and losses.
ICT risk management	Financial entities shall develop and document: (1) backup policies and procedures specifying the scope of the data that is subject to the backup and the minimum frequency of the backup, based on the criticality of information or the confidentiality level of the data; (2) restoration and recovery procedures and methods.	This documentation should be evaluated by the internal audit team, to ensure that backups are properly executed, and the information could be recovered if needed.
ICT risk management	Testing of the backup procedures and restoration and recovery procedures and methods shall be undertaken periodically.	The results of the last restoration tests should be provided to the internal audit team. It should be verified if the restoration tests are covering all the ICT assets that are supporting critical or important functions.
ICT risk management	When restoring backup data using own systems, financial entities shall use ICT systems that are physically and logically segregated from the source ICT system. The ICT systems shall be securely protected from any unauthorized access or ICT corruption and allow for the timely restoration of services making use of data and system backups as necessary.	To meet this goal, internal auditors should check if there is a physical and logical segregation between production and backup networks. Also, access controls to backup networks should be restricted as much as possible.

Area	DORA requirement	Indicative matters to consider
ICT risk management	The secondary processing site shall be: (1) located at a geographical distance from the primary processing site to ensure that it bears a distinct risk profile and to prevent it from being affected by the event which has affected the primary site; (2) capable of ensuring the continuity of critical or important functions identically to the primary site, or providing the level of services necessary to ensure that the financial entity performs its critical operations within the recovery objectives; (3) immediately accessible to the financial entity's staff to ensure continuity of CIFs in the event that the primary processing site has become unavailable.	These three controls should be included as part of the audit workplan to ensure the availability of the secondary processing site in case of disruption. It should be noted that the capacity of the secondary processing site should be enough to properly recover all the systems that are supporting any of the critical or important functions.

3.3.3 ICT-related Incident Management, Classification, and Reporting

Area	DORA Requirement	Indicative matters to consider
ICT-related incident management, classification and reporting[1]	Financial entities shall define, establish and implement an ICT-related incident management process to detect, manage and notify ICT-related incidents. They should record all ICT-related incidents and significant cyber threats. Also, appropriate procedures and processes shall be established to ensure a consistent and integrated monitoring, handling and follow-up of ICT-related incidents, to ensure that root causes are identified, documented and addressed in order to prevent the occurrence of such incidents.	The audit team should review the processes that are defined to detect, manage, remediate, notify and quantify ICT-related incidents, including cyber threats.
ICT-related incident management, classification and reporting	[RTS 18.1] Financial entities shall classify ICT-related incidents and shall determine their impact based on the following criteria: (1) the number and/or relevance of clients or financial counterparts affected and, where applicable, the amount or number of transactions affected by the ICT-related incident, and whether the ICT-related incident has caused reputational impact; (2) the duration of the ICT-related incident, including the service downtime; (3) the geographical spread with regard to the areas affected by the ICT-related incident, particularly if it affects more than two Member States; (4) the data losses that the ICT-related incident entails, in relation to availability, authenticity, integrity or confidentiality of data; (5) the criticality of the services affected, including the financial entity's transactions and operations; (6) the economic impact, in particular direct and indirect costs and losses, of the ICT- related incident in both absolute and relative terms.	The criteria defined to classify ICT-related incidents should be assessed by the auditors to ensure alignment with DORA requirements.
ICT-related incident management, classification and reporting	Financial entities shall classify cyber threats as significant based on the criticality of the services at risk, including the financial entity's transactions and operations, number and/or relevance of clients or financial counterparts targeted and the geographical spread of the areas at risk.	The criteria defined to classify cyber threats should be assessed by the internal auditors to ensure alignment with DORA requirements.

1 Further requirements are being developed by the ESAs, through the Joint Committee and in consultation with the ECB and ENISA, within RTS/ITS 18.1, 19.2, 19.4.

Area	*DORA Requirement*	*Indicative matters to consider*
ICT-related incident management, classification and reporting	Financial entities shall report major ICT-related incidents to the relevant competent authority, and submit the following information: (1) an initial notification; (2) an intermediate report after the initial notification referred to in point (a), as soon as the status of the original incident has changed significantly or the handling of the major ICT-related incident has changed based on new information available, followed, as appropriate, by updated notifications every time a relevant status update is available, as well as upon a specific request of the competent authority; (3) a final report, when the root cause analysis has been completed, regardless of whether mitigation measures have already been implemented, and when the actual impact figures are available to replace estimates.	The internal audit team should consider reviewing the process of reporting major ICT-related incidents to the relevant competent authorities, in order to validate if all the information needed in being provided efficiently and on time.

3.3.4 Digital Operational Resilience Testing

Area	*DORA Requirement*	*Indicative matters to consider*
Digital operational resilience testing[1]	DORA defines "digital operational resilience" as the ability of a financial entity to build, assure and review its operational integrity and reliability by ensuring, either directly or indirectly through the use of services provided by ICT third-party service providers, the full range of ICT-related capabilities needed to address the security of the network and information systems which a financial entity uses, and which support the continued provision of financial services and their quality, including throughout disruptions.	Some of the key controls to be reviewed by the audit team could be: • Verify if the digital operational resilience strategy has been documented, approved and communicated. • Evaluate if the scope of the digital operational resilience strategy considers at least the following elements: o Risk tolerance level for ICT risk. o Security objectives. o Communication strategy in the event of ICT-related incidents. o Business Continuity Plan (BCP). o Business Impact Analysis (BIA). o Secondary processing site capacity and testing plans. o ICT risk management framework. o Backup management and data recovery capabilities. o Management of both ICT-related incidents and cyber threats. o Vendor risk management. o Other operational resilience testing efforts such as penetration tests, Red Team exercises, vulnerability management, etc.

1 Further requirements are being developed by the ESAs, through the Joint Committee and in consultation with the ECB and ENISA, within RTS/ITS 26.2, 27.2.

3.3.5 ICT Third-Party Service Providers

Area	*DORA Requirement*	*Indicative matters to consider*
ICT third-party service providers[1]	Financial entities' management of ICT third-party risk shall be implemented in light of the principle of proportionality, taking into account: (1) the nature, scale, complexity and importance of ICT-related dependencies, (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 the potential impact on the continuity and availability of financial services and activities, at individual and at group level.	The audit team should evaluate if these requirements have been implemented and formalized within the organization.
ICT third-party service providers	As part of their ICT risk management framework, financial entities shall maintain and update at entity level, and at sub-consolidated and consolidated levels, a register of information in relation to all contractual arrangements on the use of ICT services provided by ICT third-party service providers. The contractual arrangements shall be appropriately documented, distinguishing between those that cover ICT services supporting critical or important functions and those that do not.	Auditors should request the inventory of all the third-party services, at both sub-consolidated and consolidated levels, and verify its completeness and accuracy.
ICT third-party service providers	Financial entities shall report at least yearly to the competent authorities on the number of new arrangements on the use of ICT services, the categories of ICT third-party service providers, the type of contractual arrangements and the ICT services and functions which are being provided.	The process of periodically reporting to the competent authorities should be also included within a potential audit review.

1 Further requirements are being developed by the ESAs, through the Joint Committee and in consultation with the ECB and ENISA, within RTS/ITS 28.2, 28.3, 30.2.a, 31.8, 31.11, 35.1, 35.1.d, 42.3, 43.2.

Area	*DORA Requirement*	*Indicative matters to consider*
ICT third-party service providers	Before entering into a contractual arrangement on the use of ICT services, financial entities shall: (1) assess whether the contractual arrangement covers the use of ICT services supporting a critical or important function; (2) assess if supervisory conditions for contracting are met; (3) identify and assess all relevant risks in relation to the contractual arrangement, including the possibility that such contractual arrangement may contribute to reinforcing ICT concentration risk; (4) undertake all due diligence on prospective ICT third-party service providers and ensure throughout the selection and assessment processes that the ICT third-party service provider is suitable; (5) identify and assess conflicts of interest that the contractual arrangement may cause. Financial entities may only enter into contractual arrangements with ICT third-party service providers that comply with appropriate information security standards.	As part of the bidding process, the audit team should verify if aforementioned DORA requirements are being considered, or the process should be strengthened.
ICT third-party service providers	In exercising access, inspection and audit rights over the ICT third-party service provider, financial entities shall, on the basis of a risk-based approach, pre-determine the frequency of audits and inspections as well as the areas to be audited through adhering to commonly accepted audit standards in line with any supervisory instruction on the use and incorporation of such audit standards. Where contractual arrangements concluded with ICT third-party service providers on the use of ICT services entail high technical complexity, the financial entity shall verify that auditors, whether internal or external, or a pool of auditors, possess appropriate skills and knowledge to effectively perform the relevant audits and assessments.	For this requirement, the audit team should verify, at least, which team is leading ICT third-party audits and inspections, as well as the approach, scope and periodicity that is being followed.

Area	*DORA Requirement*	*Indicative matters to consider*
ICT third-party service providers	Financial entities shall ensure that contractual arrangements on the use of ICT services may be terminated in any of the following circumstances: (1) significant breach by the ICT third-party service provider of applicable laws, regulations or contractual terms; (2) circumstances identified throughout the monitoring of ICT third-party risk that are deemed capable of altering the performance of the functions provided through the contractual arrangement, including material changes that affect the arrangement or the situation of the ICT third-party service provider; (3) ICT third-party service provider's evidenced weaknesses pertaining to its overall ICT risk management and in particular in the way it ensures the availability, authenticity, integrity and, confidentiality, of data, whether personal or otherwise sensitive data, or non-personal data; (4) where the competent authority can no longer effectively supervise the financial entity as a result of the conditions of, or circumstances related to, the respective contractual arrangement.	Internal Audit should verify the presence of such requirements within the contractual agreements with third-party ICT service providers
ICT third-party service providers	For ICT services supporting critical or important functions, financial entities shall put in place exit strategies. The exit strategies shall take into account risks that may emerge at the level of ICT third-party service providers, in particular a possible failure on their part, a deterioration of the quality of the ICT services provided, any business disruption due to inappropriate or failed provision of ICT services or any material risk arising in relation to the appropriate and continuous deployment of the respective ICT service.	As part of the audit scope, the audit team should include both the termination and exit processes for ICT third party services, in order to verify if the DORA requirements are being considered.

4.0 Acknowledgements

ECIIA

The European Confederation of Institutes of Internal Auditing (ECIIA) is the professional representative body of 34 national institutes of internal audit in the wider geographic area of Europe and the Mediterranean basin. The mission of ECIIA is to: Advocate the profession of internal auditing, and promote the role and value of internal audit and strong corporate governance to European regulators and other European stakeholders; Support the National Institutes in advocacy activities and related services.

ECIIA INSURANCE COMMITTEE

ECIIA set up an Insurance Committee in 2012 of the largest European Insurance companies. The mission of the ECIIA Insurance Committee is: *"To be the consolidated voice for the profession of Internal Audit in the Insurance sector in Europe by dealing with the Regulators and any other appropriate institutions of influence at European level and to represent and develop the Internal Audit profession as part of good corporate governance across the Insurance Sector in Europe"*. ECIIA represents around 55.000 internal auditors and around 12.000 are active in the insurance sector.

Written by Robert Zergenyi (Zurich Insurance), Marco Bachmann (Zurich Insurance), Timothy Tikhonov (Zurich Insurance), Salvino Marigo (Assicurazioni Generali), Sergio Benigni (Assicurazioni Generali), Guillermo Martin Vidal (MAPFRE) and Gerhard Schreihans (UNIQA). Additionally, we would like to thank the members of the ECIIA Insurance Committee for their input, feedback and comments.

ECIIA

Industrious 6/9 Avenue des Arts
1210 — Brussels
TR: 849170014736 52
info@eciia.eu
https://eciia.eu

European Confederation of
Institutes of
Internal Auditing