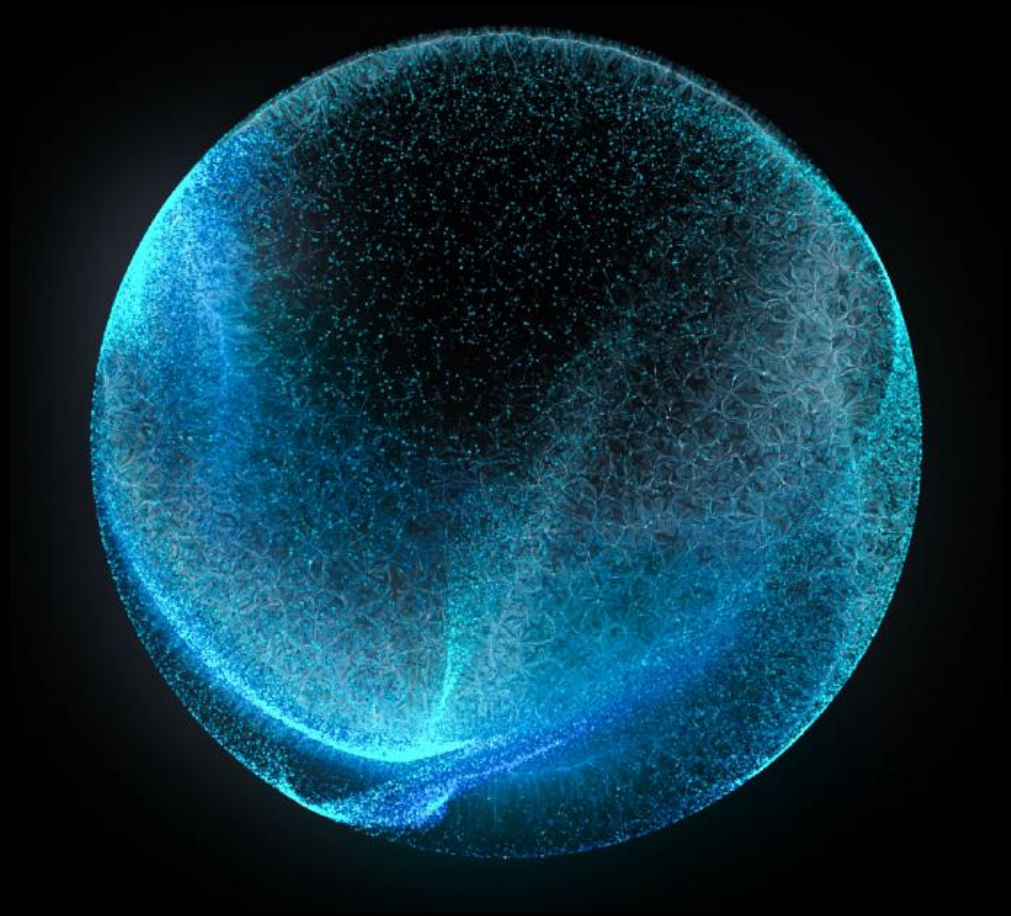
Deloitte.



Digital Operational Resilience Act

Survey for Financial Services Entities – Wave 3

March 2025

Operational Resilience in the Financial Services Industry

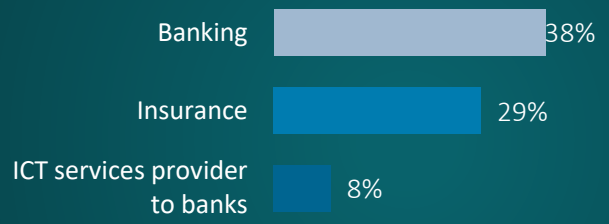
Now that the application date of the Digital Operational Resilience Act (DORA) has passed, and the Regulatory Technical Standards are finalized and issued in the Official Journal, Deloitte has conducted a follow-up survey with the objectives to understand the readiness of financial institutions in complying with the DORA, and the associated implementation challenges that these institutions are facing.

Key Facts and Figures

Survey respondents were CISO's, CRO's, and DORA Program Managers of the financial entities involved.

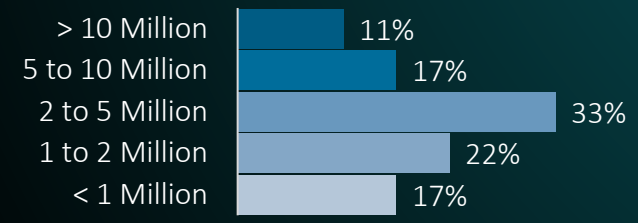
CISO and CIO were selected as the main responsible buying persona for compliance with DORA by the respondents.

Top Entity Industries Involved

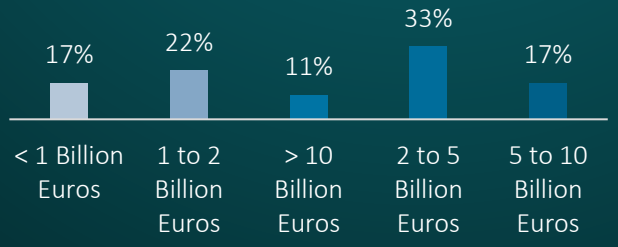


Followed by Credit Institution, Card Issuers, Financial Market Infrastructure, and Other systemically important institutions (O-SIIs) with O-SII score < 3000 at 25%

Number of Customers of surveyed entities

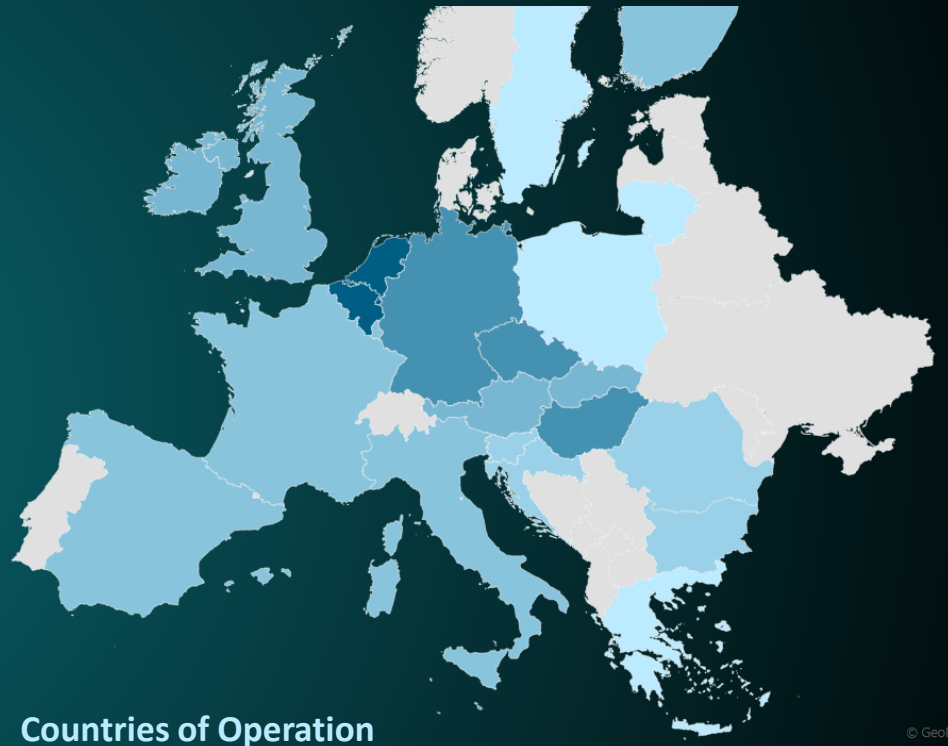


Revenue of surveyed entities



Surveyed Market Presence Across Europe

36 entities surveyed across 28 countries



Countries of Operation

12% per country
BE, NL

8% per country
HU, DE, CZ

6% per country
MT

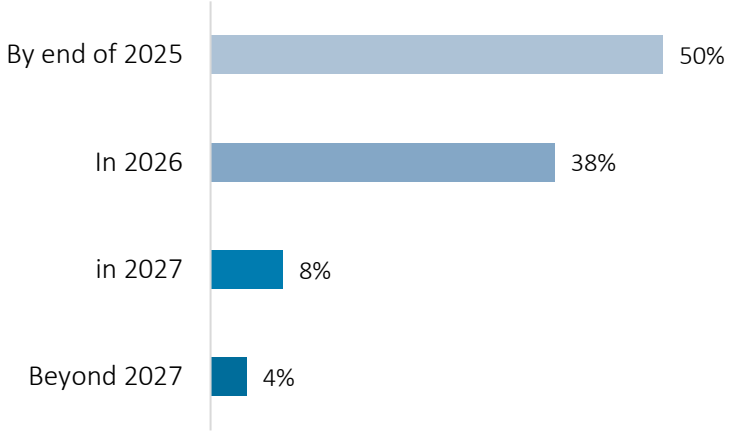
5% per country
AT, IE, SK, UK, LU

4% per country
SE, FI, IT, FR, ES

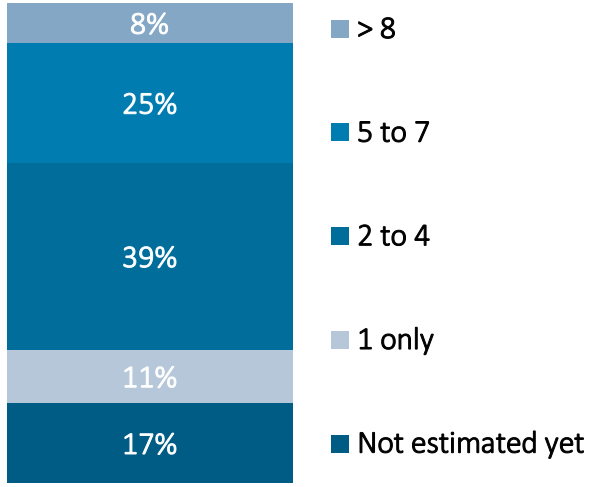
<3% per country
BG, HR, RO, SI, CY, GR, LT, PL, PS, IS, DK, NO

Financial Institutions and DORA Assessment

When do financial institutions expect to reach full compliance with the DORA?



Have financial institutions estimated the total number of FTEs dedicated to compliance?



How much are Financial Entities planning to spend for compliance with the DORA?

Now that the application date of the DORA has been crossed, a significant **96%** of Financial Entities have an estimate for DORA compliance

The Road to DORA Compliance: what is most challenging to comply with?

46% classify the requirement to complete the DORA Register of Information as the most challenging.

17% Followed by 17% for the requirement to complete due diligence and risk assessments on the ICT third-party service providers

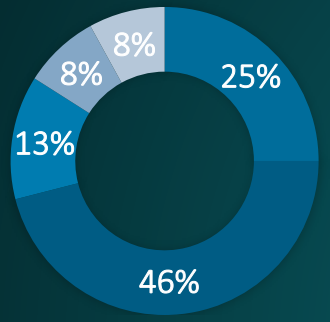
25% Followed by 25% for the requirement of testing the ICT business continuity plans considering scenarios linked to insolvency or failures of the ICT third-party service providers or linked to political risks.

12% Followed by 12% for the segregation and segmentation of ICT systems and networks taking into account the criticality or importance of the function they support, the classification and the overall risk profile of ICT assets using them

Compliance By Pillar of DORA

Results indicate that DORA Pillar II has the highest compliance amongst Financial Entities, nearly half of the surveyed entities achieved full compliance. However, Financial Entities face the most challenges with **Pillar III** and **Pillar IV**, for which **only 8%** of entities have reached full compliance on each Pillar.

Financial Entities' readiness in terms of complying with DORA Pillar I on ICT Risk Management



Only 25% of surveyed entities see themselves as fully compliant with DORA Pillar I on ICT Risk Management.

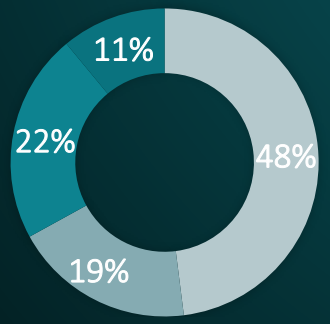
46% have the roadmap **up to 75% complete**.

For **13%** the roadmap is **halfway complete**.

8% of respondents have the roadmap up to **25% complete.**

8% of surveyed entities are at the **early stage** of compliance**.**

Financial Entities' readiness in terms of complying with DORA Pillar II on ICT Incident Management, Classification and Reporting



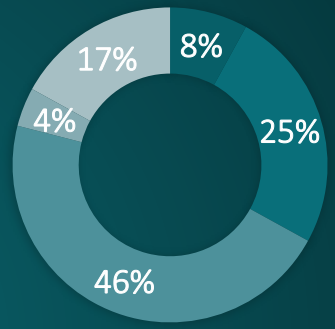
A great majority of respondents **(48%)** are already fully compliant.

19% of survey respondents have their roadmap **up to 75% complete.**

For **22%** of entities, completion of the roadmap does **not exceed 50%.**

Participants that are in **the early stage** of readiness make up **11%** .

Financial Entities' readiness in terms of complying with DORA Pillar III Digital Operational Resilience Testing



Only **8%** of participants see themselves as **fully compliant**.

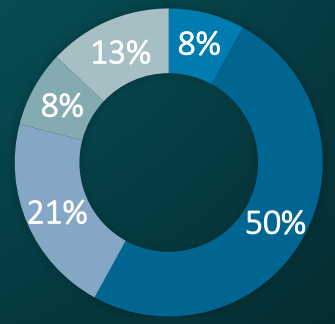
A fourth of surveyed entities have their roadmap **up to 75% complete.**

46% have the roadmap **up to 50% complete**.

For 4% of Financial Entities surveyed, their roadmap is **up to 25%** complete.

17% of respondents are at the **early stage** of compliance.

Financial Entities' readiness in terms of complying with DORA Pillar IV on ICT Third-Party Risk Management



Only **8%** of participants see themselves as **fully compliant**.

Half of the participating Financial Entities have a roadmap that is up to 75% complete.

21% have their roadmap **50% complete**.

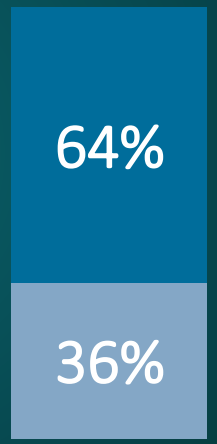
Surveyed entities that have **up to 25%** complete roadmap make up **8%** of respondents.

13% of data contributors are at the **early stage** of compliance**.**

Pillar I: ICT Risk Management

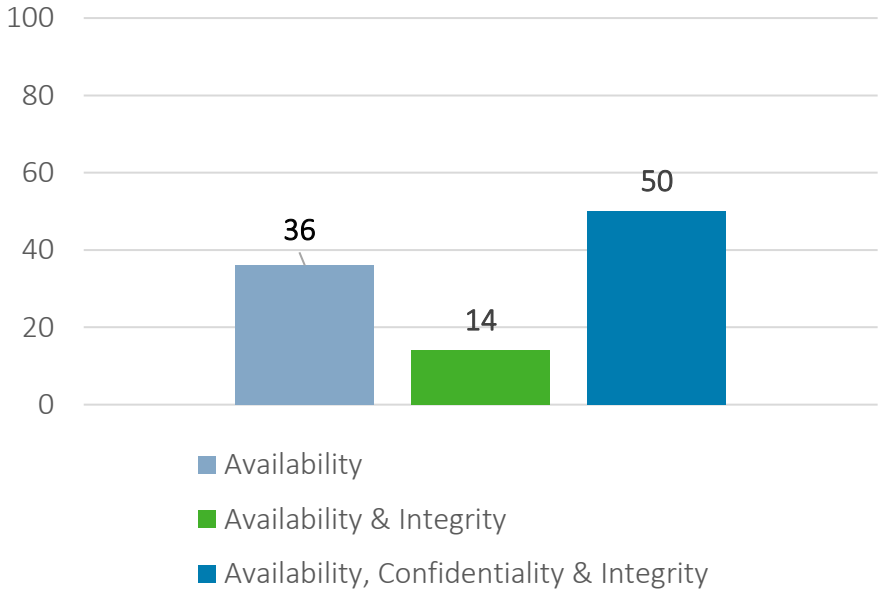
How many Critical or Important Functions (CIF) for the DORA have you identified at entity level?

Surveyed Financial Entities fall into two categories. **64%** have identified **20 to 30** Critical or Important Functions at entity level, while **36%** have identified **30 to 100** Critical or Important Functions.



Criteria from the Confidentiality, Integrity, and Availability (CIA) triad that are considered applicable when associating an ICT asset to support a DORA Critical or Important function (CIF)?

All financial institutions consider Availability as an applicable criteria when associating an ICT asset to support a DORA Critical or Important Function. **14%** of these consider Integrity as an additional criteria, while **50%** include Confidentiality and Integrity. In contrast, **36%** consider Availability as the only applicable criteria.



How are Financial Entities identifying the critical and important functions (CIF)?*

45% of surveyed entities identify CIF based on a strategic business impact assessment, while **23%** based on **operational business impact assessment**, **12%** based on the **classification of critical and essential services** stipulated in the EU by the **Single Resolution Board** (SRB), **3%** based on the classification by the **European Insurance and Occupational Pensions Authority** (EIOPA), **7%** based on a custom approach, and the last **10%** based only on the definition of CIF in the DORA.

Which is most challenging for Financial Entities to comply with

When addressing RTS Section 6 – Network Security, Article 13 Network security management

42% see as most challenging the segregation and segmentation of ICT systems and networks considering the criticality or importance of the function they support, the classification and the overall risk profile of ICT assets using them.

To address this challenge:

- **25%** Plan to implement dedicated application subnets that strictly limit data flows across all applications supporting DORA CIF to only allow the whitelisted subnets and prevent all other data traffic, while documenting and maintaining the end-to-end data flows.
- **25%** Group applications with high BIA score on Confidentiality or Integrity behind one dedicated segment, medium BIA score on Confidentiality or Integrity behind another dedicated segment, etc, then document and maintain end-to-end data flows.
- **17%** Consider DORA proportionality principle to group ICT assets with high availability, confidentiality or integrity behind a dedicated segment, medium C/I/A behind another dedicated segment, and low C/I/A behind a third dedicated segment. Also to update the segmentation as the BIA is refreshed on yearly basis.
- **33%** Others, such as outsourcing

11% identify the biggest challenge in the documentation of all of the financial entity's network connections and data flows.

13% consider the encryption of network connections for communication protocols used taking into account the results of the approved data classification and the results of the ICT risk assessment as most challenging.

22% of Financial Entities view the use of a separate and dedicated network for the administration of ICT assets as the most challenging to comply with.

To address this challenge:

33% view administering all ICT assets through a Jump Host and restricting direct connections to databases from the low privileged user network as the most adequate approach.

25% perform administration of all ICT assets via an API gateway that provides a layer of security for IT backend services, using various forms of authentication, including user-password credentials, key-based authentication, LDAP, & authentication protocols like OAuth or OIDC.

9% Perform administration of all ICT assets via dual network interfaces (NICS of dual-homing), one for the regular business user interface and another one for IT administration.

33% have not addressed it yet

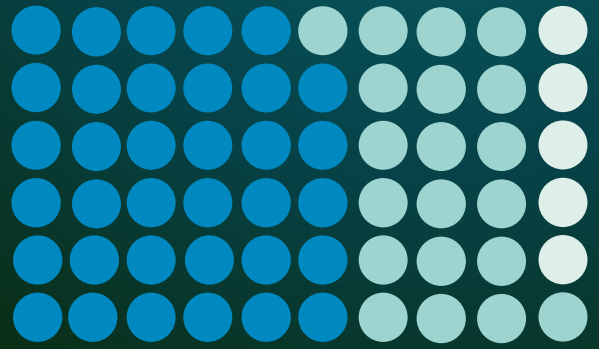
RTS Section 4 – Encryption and cryptography, Article 6 Encryption of data at rest and in transit

Encryption of Data at rest

54% consider **Full Disk Encryption** as the most adequate implementation approach for data at rest: Encrypting the entire disk, including the operating system and all files with a single key, and covering all data classification levels (sensitive, personal…)

33% consider **application layer encryption (ALE):** using transparent data encryption (TDE) to encrypt physical files, such as data and log files or (ALE) encrypts data at the application layer before it is transmitted or stored; and covering all data classification levels (sensitive, personal…)

13% consider other encryptions but not well specified.

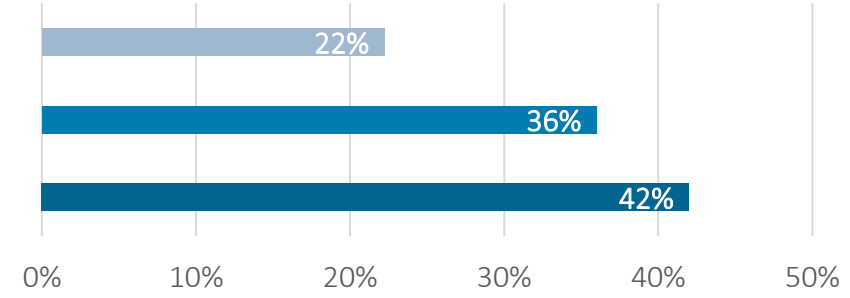


Encryption

42% consider encryption of all data flows **in between the dedicated segmented application subnets.**

36% consider encryption of all data flows **upon leaving the data center and leave internal network flows unencrypted.**

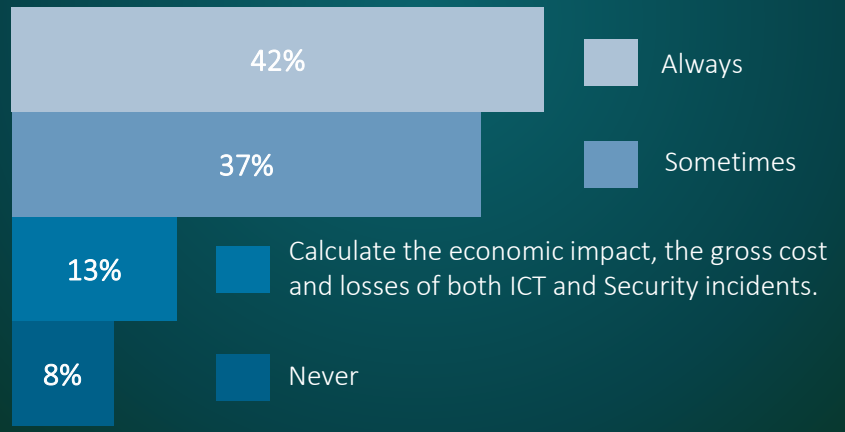
22% consider other encryptions but not well specified.



- consider encryption of all data flows in between the dedicated segmented application subnets.
- Consider Encryption of all data flows upon leaving the data center and leave internal network flows unencrypted
- Consider Other Encryptions but not well specified

Pillar II: Incident Reporting

Are financial entities recording all costs and losses caused by ICT disruptions and ICT incidents, in line of the Regulatory Technical Standards on annual aggregated costs & losses

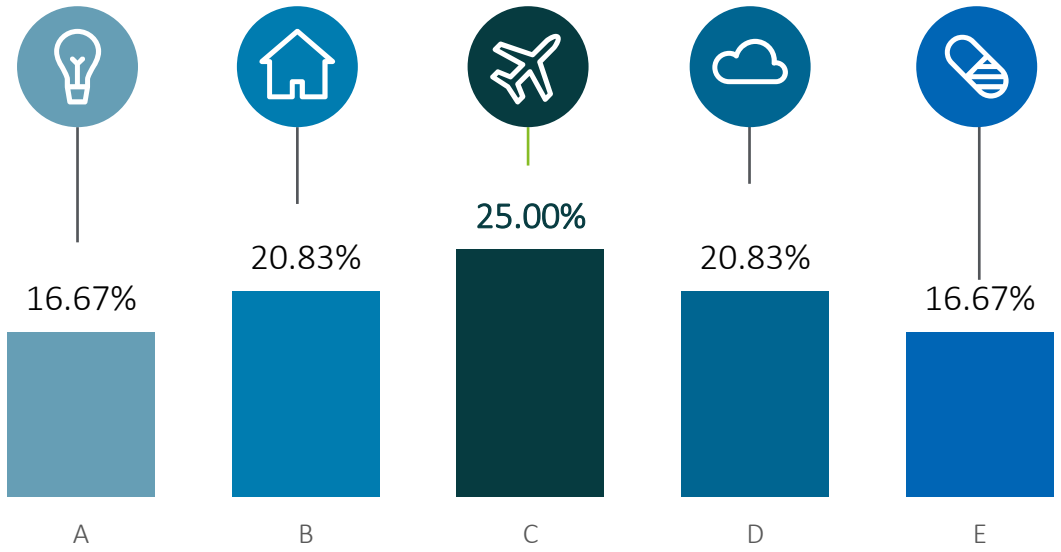


Which data set correlated to the primary and secondary criteria of the DORA Major incidents were identified by the financial entities:

1. **Only 18%** identified the data set that correlates the **incident to the impacted clients, financial counterparties, and amount and quantity of impacted transactions**
2. **Only 7%** identified the data set that correlates the incident with its impact on the entity reputation
3. **Only 13%** identified the **service downtime and duration** Data set
4. **Only 7%** identified the **geographical** data set
5. **Only 7%** identified the data set that correlates the incident to the **impacted CIF**
6. **Only 22%** identified the data set that correlates the incident to the **CIF and the source of the impacted asset**
7. **Only 18%** identified the data set that correlates the incident to the **impact on data supporting the CIF considering confidentiality, integrity, availability, authentication, and non-repudiation aspects**
8. **While 8%** did **not identify any data set**

Only 7% of participants have identified all the required criteria

Have financial entities performed a drill testing in the past 12 months on their incident response plan considering the (CIF) and the critical assets



A: performed a simulation of an ICT and a security incident that impact a CIF, where they correlated the data set to calibrate and validate the measurement of the 7 classification criteria for major incidents.

B: performed a simulation of a security incident that impacts a CIF, where they correlated the data set and classified the incident as major impacting one primary criteria, and two secondary criteria.

C: surveyed participants performed a simulation of an ICT incident that impacts a CIF, where they correlated the data set and classified the incident as major impacting two primary criteria.

D: performed a simulation of a security incident that impacts a CIF, where the incident started from the ICT service provider, correlated the data set and classified the incident as major impacting one primary criteria, and two secondary criteria.

E: did not perform a drill testing via simulation on their incident response plan

Are Third-Party Providers included in the Entity Validation for the Incident Response Plan?

54% of surveyed financial entities exclude Third-Party Providers from the entity validation of the incident response plan

25% of surveyed financial entities train the ICT providers on their role and include them in the crisis resilience simulation for the DORA include Third-Party Providers, while **25% just include** Third-Party Providers.

- 21% Yes
- 54% No
- 25% Trained the ICT providers on their role & included them in DORA crisis resilience simulation

Pillar III: Digital operational resilience testing

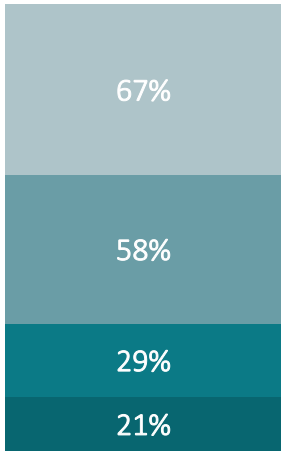
67% include **scenarios of switchover** from primary ICT infrastructure to the redundant capacity, backups and redundant facilities

58% include scenarios of partial or total **failure of premises**, including office and business premises, and data centers.

Components of ICT Business Continuity and Response & Recovery Plan Testing for Financial Entities:

29% include **scenarios** linked **to insolvency or failures** of the ICT third- party service providers or linked to **political risks** in the ICT third-party service providers' jurisdictions.

21% have not identified any test yet or and are in progress of doing so.



What are the components of the Digital Operational Resilience Testing Programs for the surveyed financial entities*

1. **50%** of financial entities have **weekly automated testing** (SAST, DAST, SCA) on CIF-supporting systems, plus **regular scans** for all other ICT assets to ensure full coverage.

2. **70%** of financial entities have **yearly network security assessments** for network components supporting the ICT services classified as (CIF).

3. **None** of the financial entities create a **Software Bill of Materials "SBOM"** to track the used third-party libraries and monitor the version for any possible updates. For the case of "off-the-shelf assets", request the ICT provider to provide this information via a structured report.

4. **70%** of financial entities conduct **yearly penetration testing** on the ICT tools and ICT infrastructure supporting (CIF), including different types of ethical hacking with supply chain involvement.

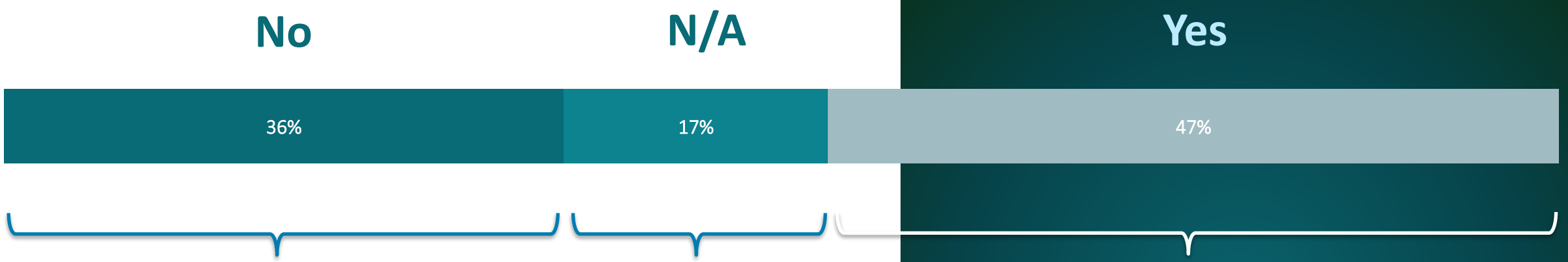
5. **3%** of financial entities still need to plan their digital operational resilience testing programs.

6. **58%** of financial entities **monitor vulnerability patching trends** of ICT providers on their public channels on an on-going basis. Obtain and review on a yearly basis the ICT provider's critical vulnerabilities and statistics and trends reports.

7. **83%** of financial entities conduct a **review of firewall rules and connection filters** every 6 months

*Multiple answers were selected.

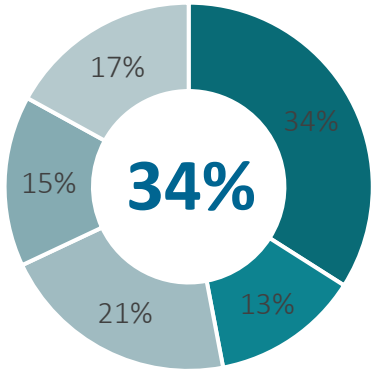
Involvement of Third-Party Providers in the Threat Led Penetration Testing



17% of surveyed financial entities were not eligible to Threat Led Penetration Testing.

15% of surveyed financial entities **only identified potential vulnerabilities** via **scanning and boundary discovery** of the third-party vendor environment, without attempting to exploit them.

21% of surveyed financial entities **did not involve third-party providers** in threat led penetration testing.

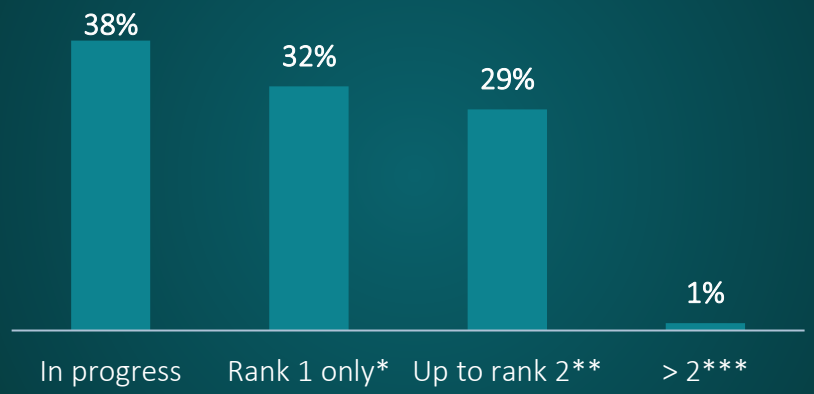


34% of FEs **included testing around the vendor infrastructure** boundary and exploited the vulnerabilities identified on the system and infrastructure hosted at the third-party vendor computing environment (servers, networks…).

Meanwhile, **13%** of financial entities **involved third party providers only for coordination purposes** but never attempted to exploit the boundary of the systems that are outsourced to third party vendors.

Pillar IV: ICT Third-Party Risk

Identification of Interconnections within the Full-Service Supply Chain of ICT Third-Party Providers Supporting Critical and Important Functions (CIF)



*Have identified the third-party direct connection (rank 1) but have not identified yet the rest of supply chain (rank 2 and higher) as per the template RT.05.02 — ICT service supply chains

** Have identified the third-party direct connection up to rank 2 as per the template RT.05.02 — ICT service supply chains

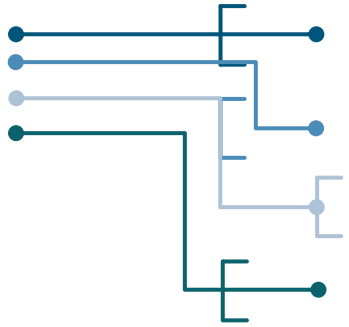
*** Very low % have identified the entire Service Supply Chain

How did the surveyed financial entities analyze the ICT concentration risk in their portfolio of existing ICT third-party service providers, as per article 28 and 29 of the DORA final text

25%	Respondent's multi-vendor strategy requires to explain the rationale behind the procurement mix of ICT third-party service providers.
22%	Respondent's multi-vendor strategy requires to show key dependencies on ICT third-party service providers.
25%	Respondent's multi-vendor strategy requires to track ICT third-party service providers by geographic location / member states
10%	Respondent's multi-vendor strategy requires to identify concentration risk for each ICT contractual arrangement supporting Critical and Important Functions provisioned by the same ICT third-party service providers.
10%	When an ICT contractual arrangement supporting critical or important functions would lead to increase in the concentration risk at entity level, the respondent's multi-vendor strategy requires to weigh the benefits and costs of alternative solutions, such as in-sourcing or the use of different ICT third-party service providers, taking into account if and how envisaged solutions match the business needs and objectives set out in their digital resilience strategy, without hindering the conduct of business or restraining the contractual freedom.
8%	In progress of assessing ICT Concentration risk in the ICT Service Supply Chain

Preferred Option

Have the surveyed financial entities completed identifying and documenting the mapping of business functions / processes with the ICT Assets, the ICT third-party providers and the ICT third-party contracts?



17% **Identified** and **documented** in a GRC

42% **Identified** but **not yet documented** in a GRC

38% In progress

3% Not yet

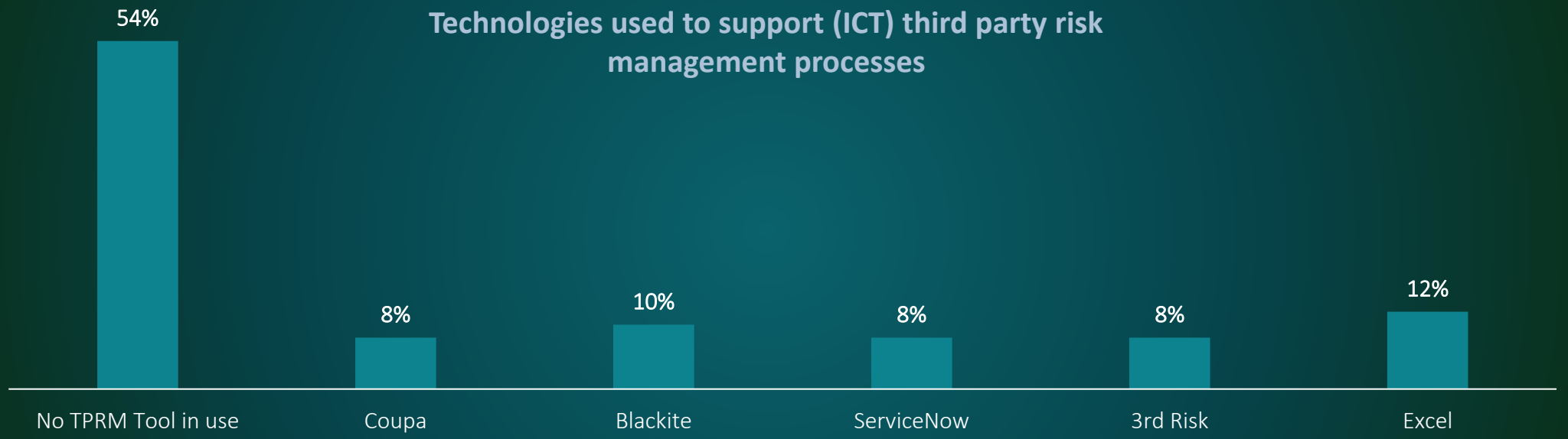
Reliance on Security Certificates from Third-Party Providers Supporting Critical and Important Functions (CIF) Service organization controls report (SOC I and 2 reports, ISO 27001 with statement of applicability, PCI-DSS, HIPAA)

51% of surveyed financial entities would rely on security certificates but would **see the need to perform additional due diligence** on the providers by reviewing additional evidence of controls in place.

While **44%** would rely on security certificates but believe **not all providers have these certificates**.

5% would rely on security certificates.

Technologies used to support (ICT) third party risk management processes



What actions are taken during the pre-contractual due diligence phase, when measuring the impact of the prospective ICT provider on the ICT concentration risk at entity level?

22%

Do not proceed with the ICT contractual arrangement that increases the ICT concentration risk level concurrently on **the three (3) aspects:**

1. of having in place multiple contractual arrangements with the same ICT third-party service provider or with closely connected ICT third-party service providers (same service supply chain)
2. services are provisioned from the same geographic location / member states
3. And the ICT third-party **service provider is classified as "Not substitutable"** under the register of information – template field "b_07.01.0050".

19%

Proceed with the ICT contractual arrangement that increases the ICT concentration risk level concurrently on the **three (3) aspects:**

1. of having in place multiple contractual arrangements with the same ICT third-party service provider or with closely connected ICT third-party service providers (same service supply chain),
2. Services are provisioned from the same geographic location / member states,
3. and the ICT third-party **service provider is classified as "Highly complex substitutability"** under the register of information – template field "b_07.01.0050"; However, ensure to increase the frequency of due diligence and risk assessments to twice per year covering the domains of information security, data privacy and business continuity, sanction and geopolitical risks, and insolvency / bankruptcy risk, and maintain a viable exit strategy with an exit time < 6 month.

25%

Proceed with the ICT contractual arrangement that increases the ICT concentration risk level concurrently on **the two (2) aspects**

1. of having in place multiple contractual arrangements with the same ICT third-party service provider or with closely connected ICT third-party service providers (same service supply chain)
2. And when services are provisioned from the same geographic location / member states.

Additionally, the ICT third-party service provider is **rather classified as "medium complexity in terms of substitutability"** under the register of information – template field "b_07.01.0050". However, ensure to perform due diligence and risk assessments once per year covering the domains of information security, data privacy and business continuity, sanction and geopolitical risks, and insolvency / bankruptcy risk, and maintain a viable exit strategy.

37%

Proceed with the ICT contractual arrangement that increases the ICT concentration risk level concurrently on **the two (2) aspects:**

1. of having in place multiple contractual arrangements with the same ICT third-party service provider or with closely connected ICT third-party service providers (same service supply chain)
2. and when services are provisioned from the same geographic location / member states. Additionally, the ICT third-party service provider is rather **classified as "easily substitutable"** under the register of information – template field "b_07.01.0050". However, ensure to maintain a viable exit strategy.

10%

In progress.

5%

No actions in place yet.

Completion Status of DORA Requirements for Contractual Agreements with ICT Third-Party Service Providers

5% Are currently in the process of completing these.

20% Are having challenges identifying the ICT concentration risk in the existing portfolio

32% Are currently preparing a risk-based allocation of Due Diligence and Risk Assessments over 3 years cycle in order to spread out the workload.

5% Haven't completed anything.

15% Have already completed the DORA requirements regarding contractual agreements with ICT TPP.

23% Are having challenges identifying the action plan from the exit strategy of the ICT third-party providers classified as "Not Substitutable"

Who is Accountable and Responsible for ICT Third-Party Risk Management?

CISO

4% of surveyed financial entities have their CISO as accountable and responsible for ICT TPRM.

Compliance/Risk

29% of surveyed financial entities have their Compliance/Risk Team as accountable and responsible for ICT TPRM.

Procurement

4% of surveyed financial entities have their Procurement Team as accountable and responsible for ICT TPRM.

Business - Operation

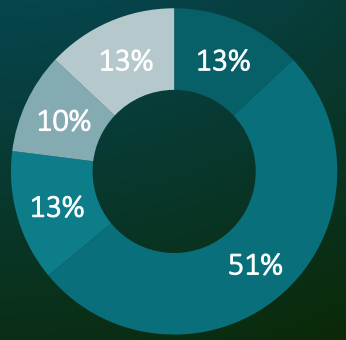
50% of surveyed financial entities have their Business – Operation Team as accountable and responsible for ICT TPRM.

Management Committee

13% of surveyed financial entities have their Management Committee as accountable and responsible for ICT TPRM.

Do the organizations outsource to Cloud Service Providers ICT Assets Supporting Critical or Important Functions?

- Yes, based on risk based approach and only where the level of reliance on the CSP is not significant or low reliance. (13%)
- Yes-risk based approach. The cases where level of reliance on the CSP is Material or Full mandate additional Due diligence and on-going monitoring of the CSP, Escrow Agreements to cover Portability of the SAAS solution, & backup on other CSP's. (51%)
- Yes and data backup is maintained on-prem or with another CSP. (13%)
- Yes (10%)
- No. (13%)



Glossary

CTTP	Critical technology third-party provider
System Risk	The European Systemic Risk Board (ESRB) has reaffirmed in a 2020 report addressing systemic cyber risk: how the existing high level of interconnectedness across financial entities, financial markets and financial market infrastructures, and particularly the interdependencies of their ICT systems, may potentially constitute a systemic vulnerability since localized cyber incidents could quickly spread from any of the approximately 22 000 Union financial entities to the entire financial system, unhindered by geographical boundaries.
ESA	European Supervisory Authority (European Banking Authority) ('EBA') established by Regulation (EU) No 1093/2010, the European Supervisory Authority (European Securities and Markets Authority) ('ESMA') established by Regulation (EU) No 1095/2010, and the European Supervisory Authority (European Investment and Occupational Pensions Authority) ('EIOPA') established by Regulation (EU) No 1094/2010 (hereinafter collectively referred to as "European Supervisory Authorities" or "ESAs"))
Red team	The offensive team performing the Threat led penetration testing
Blue team	The organization's defending team
White team	Consists of only concerned Institution's security and business experts who will monitor the Threat led penetration testing and intervene when needed
Purple team	Team that performs a replay between the Red Team ("RT") and the Blue Team to identify gaps, address findings and improve the overall capabilities of the Concerned Institution undergoing TLPT
TLPT	Threat led penetration testing: Threat Intelligence Based Ethical Red Teaming (TIBER-EU). The highest possible level of intelligence-based red teaming exercise using the same Tactics, Techniques and Procedures ("TTPs") as real adversaries, against live critical production infrastructure, without the foreknowledge of the organisation's defending Blue Team ("BT").
Geopolitical risk	Risk that the location of IT service provider or location of ICT subservice organization (4^{th}, 5^{th}, nth party) is in a country or region that is considered prone to geopolitical influence.
Sanction risk	Risk that the location of IT service provider or location of ICT subservice organization (4^{th}, 5^{th}, nth party) is in a country or region that is considered under sanction(s).

Contacts

Bert Truyman
Partner| Technology & Digital Risk
Gateway Building
Luchthaven Brussel Nationaal 1J
B-1930 Zaventem
Tel: +32 497 51 55 12
btruyman@deloitte.com

Andrea Radu
Partner | Cyber
Gateway Building
Luchthaven Brussel Nationaal 1J
B-1930 Zaventem
Tel: + 32 470 94 49 02
andrearadu@deloitte.com

Georges Gehchan
Senior Manager | Cyber
Gateway Building
Luchthaven Brussel Nationaal 1J
B-1930 Zaventem
Tel: + 32 499 82 57 49
ggehchan@deloitte.com

Deloitte.

Deloitte refers to one or more of Deloitte Touche Tohmatsu Limited (“DTTL”), its global network of member firms, and their related entities (collectively, the “Deloitte organization”). DTTL (also referred to as “Deloitte Global”) and each of its member firms and related entities are legally separate and independent entities, which cannot obligate or bind each other in respect of third parties. DTTL and each DTTL member firm and related entity is liable only for its own acts and omissions, and not those of each other. DTTL does not provide services to clients. Please see www.deloitte.com/about to learn more.

Deloitte is a leading global provider of audit and assurance, consulting, financial advisory, risk advisory, tax and related services. Our global network of member firms and related entities in more than 150 countries and territories (collectively, the “Deloitte organization”) serves four out of five Fortune Global 500® companies. Learn how Deloitte’s approximately 330,000 people make an impact that matters at www.deloitte.com.

This communication and any attachment to it is for internal distribution among personnel of Deloitte Touche Tohmatsu Limited (“DTTL”), its global network of member firms and their related entities (collectively, the “Deloitte organization”). It may contain confidential information and is intended solely for the use of the individual or entity to whom it is addressed. If you are not the intended recipient, please notify us immediately and then please delete this communication and all copies of it on your system. Please do not use this communication in any way.

None of DTTL, its member firms, related entities, employees or agents shall be responsible for any loss or damage whatsoever arising directly or indirectly in connection with any person relying on this communication. DTTL and each of its member firms, and their related entities, are legally separate and independent entities.

© 2025 Deloitte. All rights reserved.