Survey on Digital Operational Resilience Act

February 2023

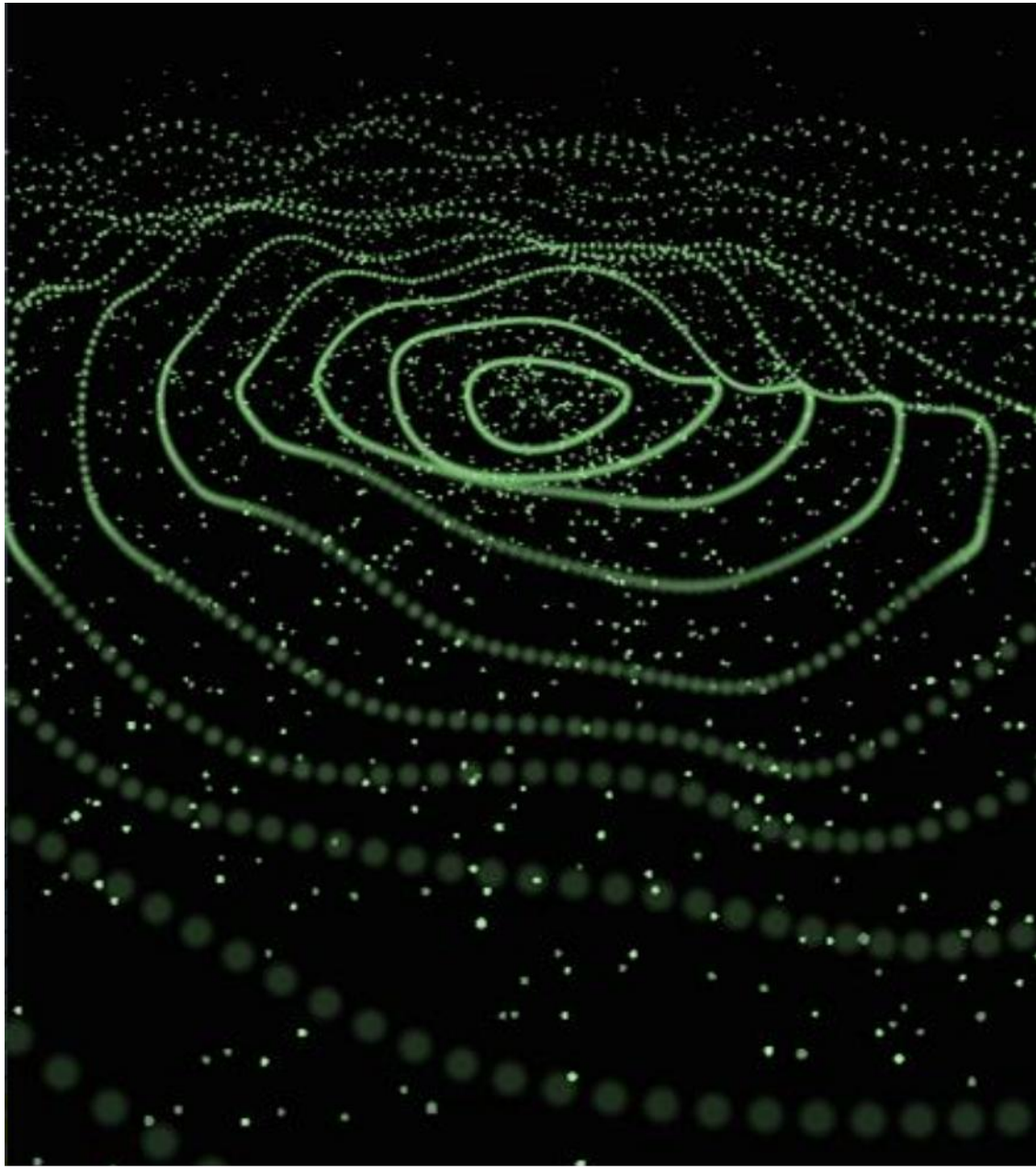
Resilience is business critical

Major ICT incidents and cyber-attacks: is the financial sector resilient enough?

The DORA will require firms to adopt a broader business view of ICT resilience with **accountability clearly established at the senior management level across the organization**. It applies to the majority of financial entities operating in the EU, and establishes binding rules for ICT risk management, incident reporting, resilience testing, and third-party risk management.

The DORA enables **operational resilience**, which consists of capabilities that financial entities require to **support the continued provision of financial services and their quality**.

There is a need for a **new holistic approach of building resilience against digital disruptions.**



The impact of the DORA on the Financial Sector

The DORA includes five (5) Pillars and expand on the existing regulations and guidelines

The DORA pillar V on the supervisory Authorities' roles is excluded from this survey.

Dora	Consolidates and expands
Pillar I	*EBA/GL/2019/04, NIS2, PSD2*
Pillar II	*EBA/GL/2021/03, PSD2, NIS2, Target2, GDPR, ECB/SSM Supervisory Incident Reporting Framework, eIDAS 910/2014*
Pillar III	*TIBER-EU, TIBER-BE, NBB Handbook*
Pillar IV	*EBA/GL/2019/02, PSD2, NIS2*

*Source: European Central Bank, Q3 2022

Timeline of the DORA

Compliance Journey has started

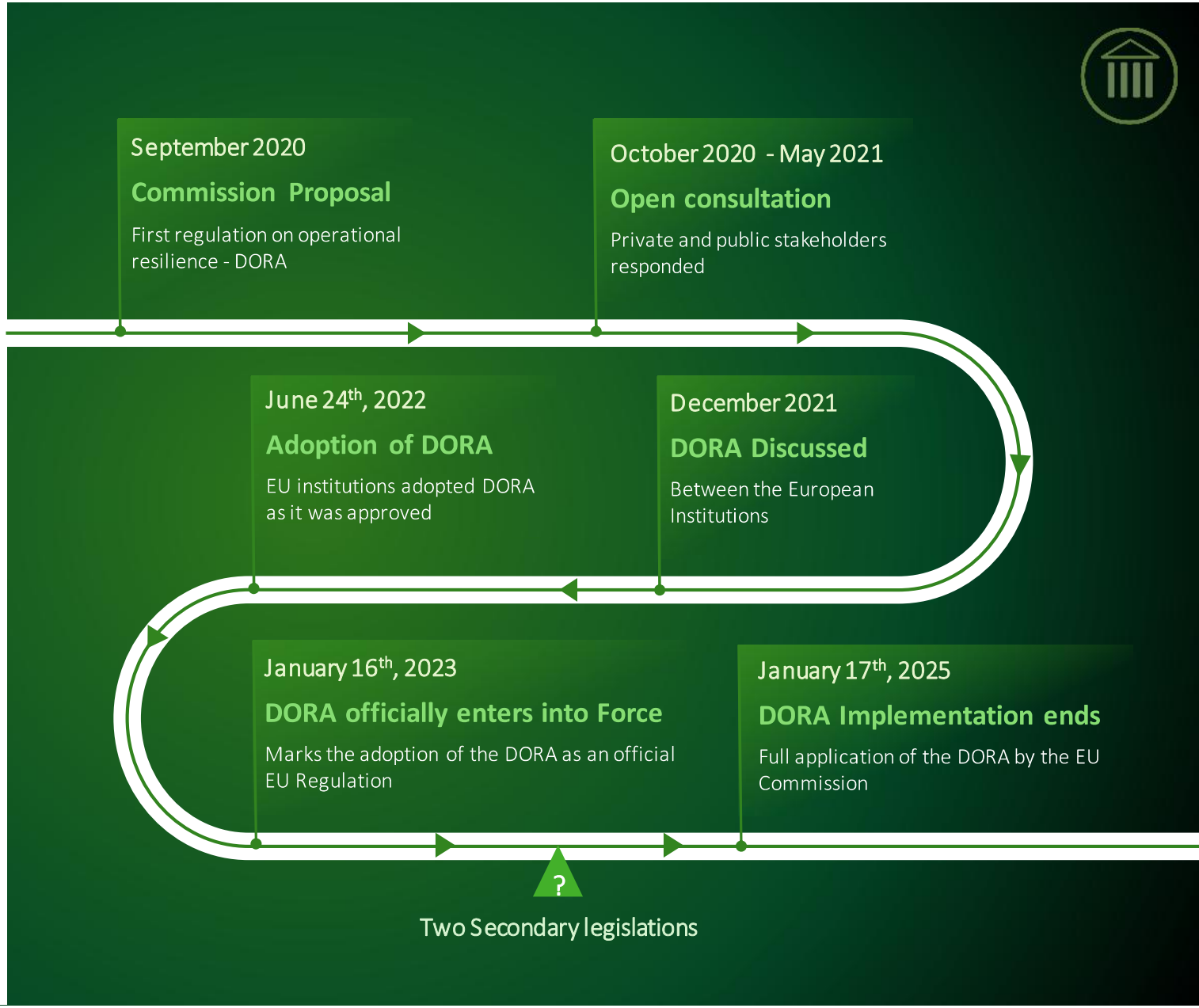
A 24 month-long implementation **period** that will lead to full application on 17 January 2025.

Two Secondary Legislations

Two secondary legislations will be released by the **European Supervisory Authorities** (ESAs) by 17 January and 17 July 2024.

Six phases

Five out of six main phases were **already completed** by the 16 of January 2023.



Looking into Operational Resilience in the Financial Services Industry

The EU Commission proposal on Digital Operational Resilience has started in September 2020. Throughout the journey of the creation, consultation, discussion and adoption of the Act (DORA), financial entities across Europe have been awaiting the final approval of the DORA by the Commission, and the timeline for implementation. While the DORA came into force on 16 January 2023, Deloitte has conducted a survey between November 2022 and January 2023 with the **objectives to understand the readiness of financial institutions in complying with the DORA, and the associated challenges that these institutions are facing.**

Surveyed Market Presence Across Europe

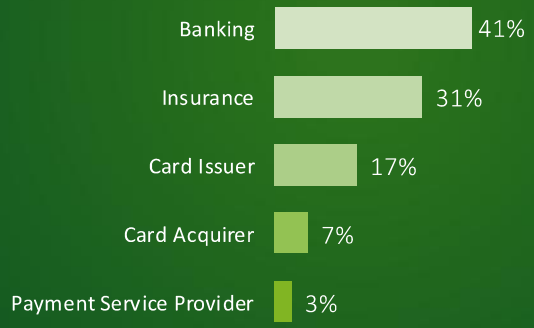
20 entities surveyed across **20 countries**

Key Facts and Figures

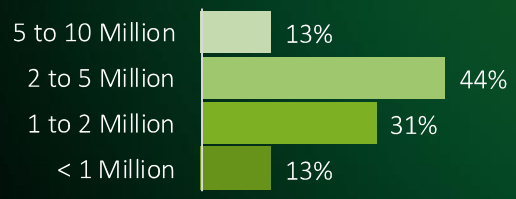
Survey respondents were CISO's, CIO's, ORM, IT Risk, and CRO's of the financial entities involved

Board of directors' involvement with Cybersecurity and ICT risk is required to increase as a result of the DORA

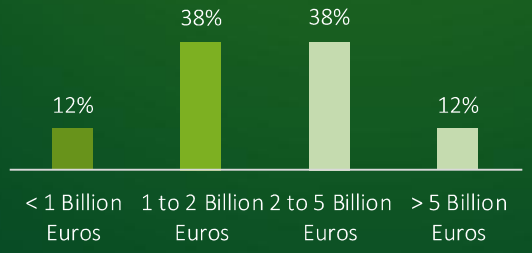
Top Entity Industries Involved



Number of Customers of surveyed entities



Revenues of surveyed entities



Countries of Operation

17% per country

BE

9% per country

LU, CH

5% per country

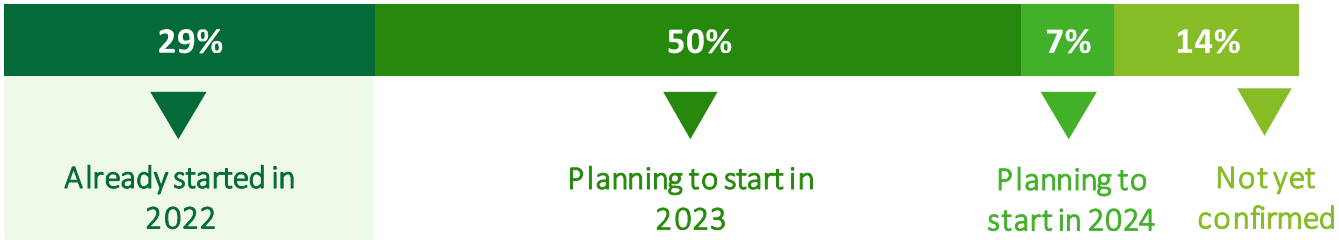
FR, DE, NL, NO, PT, ES, CZ

3% per country

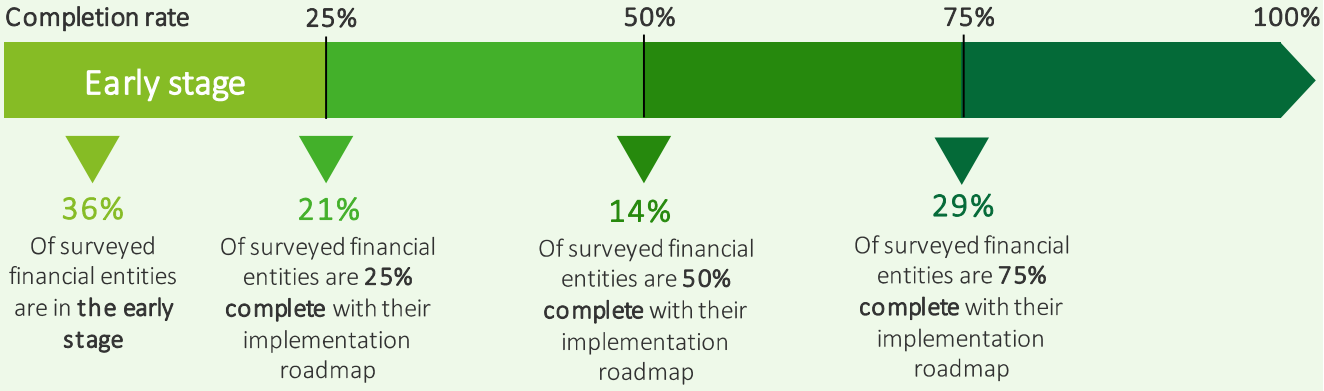
DK, HU, IE, IT, SK, SE, UK, RS, MK, BG

The Status of Preparation for the DORA

Timeframe of surveyed entities planning to start the roadmap to DORA compliance



Current Status of The Implementation Roadmap



Implementation period

The 24-month implementation period will challenge most surveyed financial entities, including large and sophisticated ones, in areas such as advanced testing, incident reporting, and business impact analysis.

The most challenging Pillar for compliance

67% of surveyed entities find **ALL 4 Pillars** equally challenging; While **33%** find **Pillar 4** on ICT third-party risk the hardest to comply with.

Gap Analysis

7% of surveyed entities have performed a gap analysis between their current practice and DORA requirements.
In comparison, **36% of entities have not yet begun** and **57% are in progress.**

Pillar I: ICT Risk Management

The DORA suggests an ICT risk management framework around a set of key principles and requirements such as:

- Emphasis on the importance of Board involvement.
- A set of mandatory measures to be applied (e.g. asset inventory, risk assessment, incident handling).

Expected Challenges

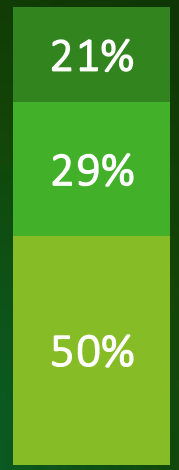
- Annual review of ICT system mapping and asset catalogues, and identification of interconnectedness with Critical Third-party Technology Providers. The survey revealed that most entities still lack a level of ICT risk maturity for DORA.
- Creating a program management on DORA, including a roadmap and adequate resources and budget.
- Inclusion of the criteria for classifying a process as a Critical or Important function (CIF) and continuously updating the list of CIF.
- Maintaining an updated list of ICT / Technology Third-Party Providers on a continuous basis.
- Mandatory Business Impact Assessments given growing supervisory pressure to develop resilience scenario testing methods and multi-vendor strategy, as well as the risk of building redundancy into systems that support CIFs.

The DORA Strategy

21% of the surveyed entities consider the digital operational resilience strategy as established.

29% have been setting their digital operational resilience strategies but have not completed them yet.

Half of the surveyed financial entities **did not define a Digital Operational Resilience strategy/plan**, at group or entity level.

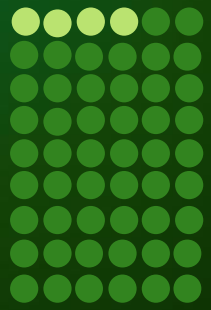


Are dedicated budgets available to prepare for the DORA?

93%

of surveyed financial entities **don't have a budget** available to comply with DORA requirements.

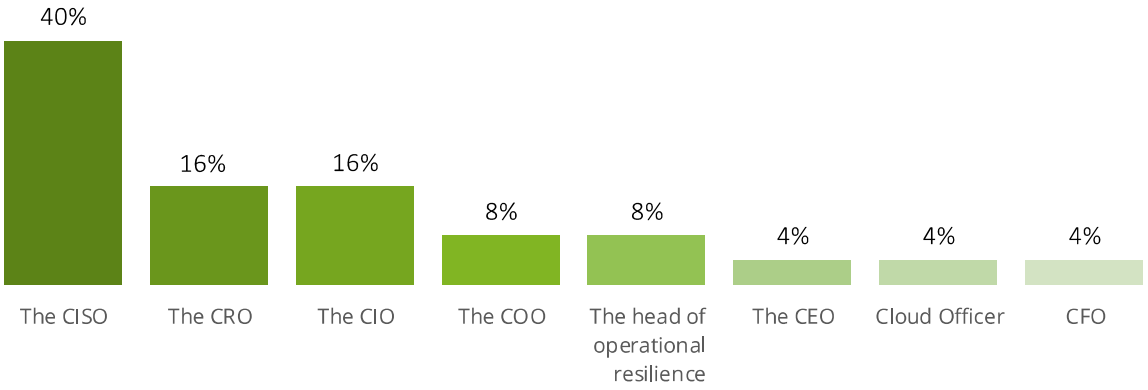
Only **7%** of surveyed financial entities have a budget available.



From a governance perspective: did the entities establish a program to prepare for compliance with DORA requirements?

The program to prepare for compliance with the DORA requirements is **not established yet for most of the surveyed financial entities**.
Only 21% of the entities have established a program to comply with DORA requirements.

The responsible (buying persona) for compliance with DORA



DORA and Critical or Important Functions (CIFs) at the Surveyed Financial Entities

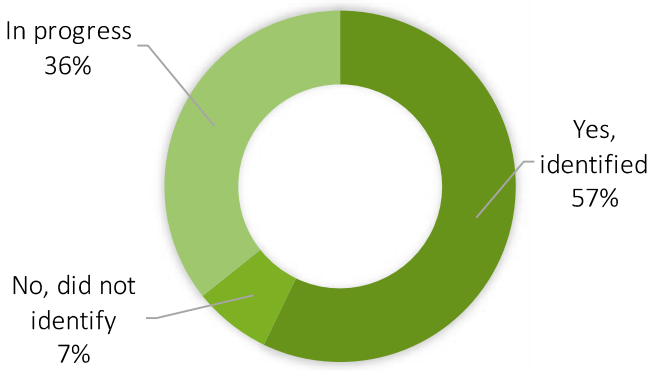
The DORA requires firms to identify CIFs as a focal point for the work they must do to build their resilience

43% of surveyed financial entities **have not yet identified** the interconnections with third-party providers that support the entities' **Critical and Important functions**.

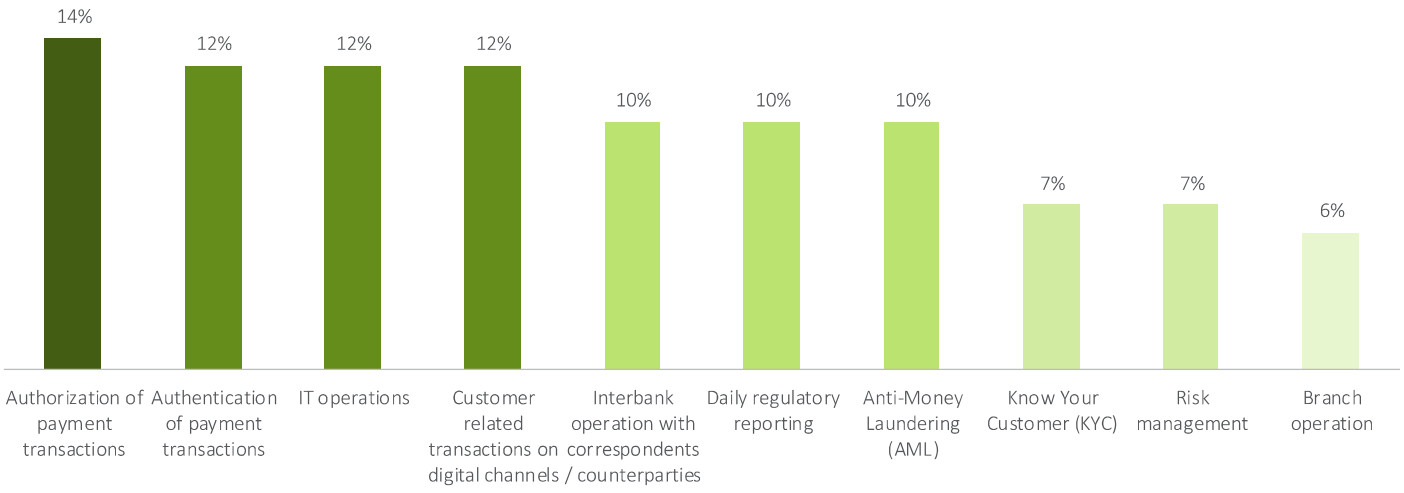
Critical or Important Function is a function whose disruption would **impair** the financial **performance** of a firm, or the **continuity** of its services, or the continuing **compliance** of its authorization and legal obligations

Authorization and authentication of payment transactions are the most viewed by the surveyed financial entities as critical and important function, at **26%**.

Have the entities identified interconnections with third party providers that support the CIF of the entity?



A snapshot on several operations deemed as a critical or important function (CIF) at the surveyed financial entities



Pillar II: Incident reporting

Financial entities need to report ICT (including cyber) incidents to different supervisory authorities, according to different thresholds, timelines and communication channels.

With the DORA, financial entities need to have an ICT-related incident management process to detect, manage and notify ICT-related incidents.

Supervisory authorities need to monitor compliance with incident reporting requirements.

Establishing a process that records cost, and losses caused by ICT disruptions and incidents.

Expected Challenges

- Establishing an adequate taxonomy for incident classification framework (MITRE, NIST, ENISA…) and efficiently eliminating false positives.
- Establishing a dashboard to manage the communication process of ICT and security incidents to the different authorities.
- Performing an annual test of the financial entity's incident response plan considering the critical and important functions and the critical assets and involving the Critical Third-Party and Technology Third-Party providers.
- Establishing a process and solution to detect, manage and notify ICT-related incidents in a timely manner and automate the response and recovery.
- Classifying the quantitative impact of ICT-related incidents in a timely manner with root cause analysis and reporting thereof to internal and external stakeholders.
- Communication of any impact or breach to critical and important functions in the same day.
- Assessment of customer exposure and identification of correct threat information sharing with them and counterparties in case of a significant cyberthreat exposure.

DORA and Incidents

DORA **does not** streamline the several incident reporting requirements that arise from frameworks in the financial sector.*

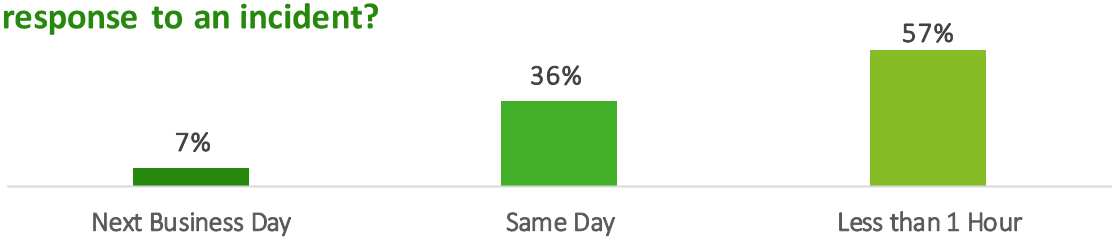
Financial entities need to report incidents to different supervisory authorities, according to different thresholds, taxonomies, timelines and communication channels.

The ESAs should be tasked to prepare in consultation with the ECB and ENISA a joint report exploring the feasibility of setting up a secure communication channel.

Automating incident reporting can **simplify compliance with multiple reporting requirements** and increase situational awareness on cyber threats at the national and EU level.

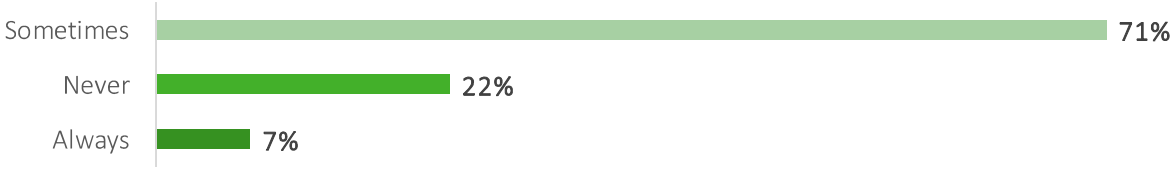
*Financial entities currently have to comply with the reporting requirements set by PSD2, NIS2, ECB/SSM, TARGET2 and GDPR

What do surveyed financial entities consider a timely detection and response to an incident?



The timeline to report incidents under DORA still needs to be set by the authorities in the Regulatory Technical Standards.

During ICT disruptions / incidents, do surveyed financial entities record all costs and losses caused by ICT disruptions and incidents?



DORA defines that **financial entities have to assess the quantitative impact of incidents** and analyze their root causes at least on a yearly basis:

"The economic impact, in particular direct and indirect costs and losses, of the ICT-related incident in both absolute and relative terms."

Executives are now demanding those in charge of cyber security to financially quantify cyber risks facing their organizations.

DORA and Incidents

Were third-party providers included in the validation of the incident response plan?

36%

Financial entities have **not** included third-party providers in their validation of the incident response plan.

43%

Financial entities **understand** the roles and responsibilities of their third party providers towards the incident response plan.

21%

Financial entities have **included** the third-party providers for the validation of the incident response plan.

Incident response plans shall consider dependencies on third-party providers.

Drill Testing on the Incident Response Plan

36% of respondents **have performed drill testing** in the past 12 months on their incident response plan considering the critical and important functions.

While 64% **have <u>not</u> performed drill testing** in the past 12 months, which is a DORA requirement.

Drill testing shall include critical and important functions.

Pillar III: Digital operational resilience testing

The DORA sets EU-wide standards for digital operational resilience testing, increasing the number of firms in scope to conduct mandatory and regular testing.

It applies across the full financial sector including Critical ICT third-party providers (CTPPs) who will be supervised by European Supervisory Authorities.

The digital operational testing requirements are based on the principle of proportionality: they vary according to the size, business and risk profiles of financial entities.

Expected Challenges

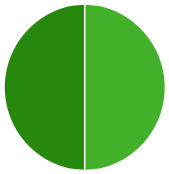
- Inclusion of the critical third-party providers and services outsourced or contracted to ICT third-party service providers in regular (once every three years or once per year based on complexity and risk profile) financial entity's threat led penetration testing.
- Resistance from the ICT third-party providers to be part of the threat led penetration testing of the financial entity, as well as unclarity on development and use of the "pooled testing" option (subject to an applicable security reason).
- Focus on the scenario-based testing and coverage of the critical and important functions as integral part of the resilience testing (applicable to all financial entities except microenterprises).
- Performance of the threat led penetration testing, covering all critical ICT systems and applications and important functions, on live production systems.
- Establishing effective remediation and follow-up process to address all vulnerabilities resulting from a threat led penetration testing prior to the next testing cycle.
- Coordination of timeline and effort to conduct threat led penetration testing among financial entities that share the same critical third-party provider.
- Availability of external/internal qualified parties to conduct threat led penetration testing.

A Snapshot on the Threat Led Penetration Testing

During the past 3 years

64% of the surveyed financial entities have **conducted threat led penetration testing** in the past 3 years. The other **36% have not.**

Live versus Test Environments



Half of the surveyed financial entities conducting threat led penetration testing, have done this on their live production environments, and the other half have limited it to Test (Non-Live) environments.*

* TIBER-EU is not mandatory in all countries of the surveyed entities

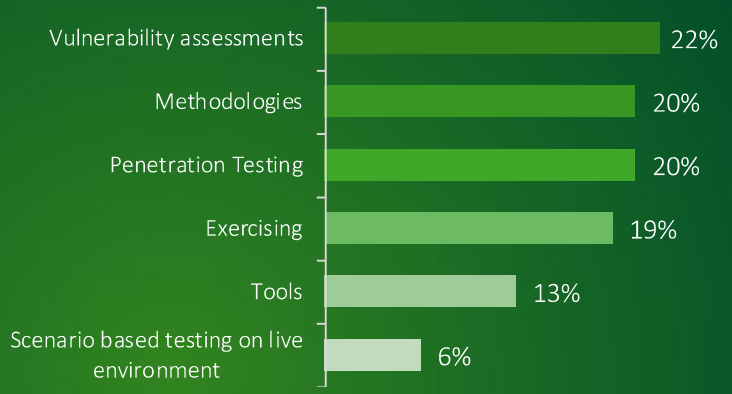
Automation of the threat led penetration testing at the financial entities

64%
Of surveyed financial entities **see the need to automate** ongoing threat led penetration testing (TLPT)

28%
Do not see the need to automate ongoing threat led penetration testing (TLPT)

8%
Aim to enroll in managed services to handle ongoing TLPT

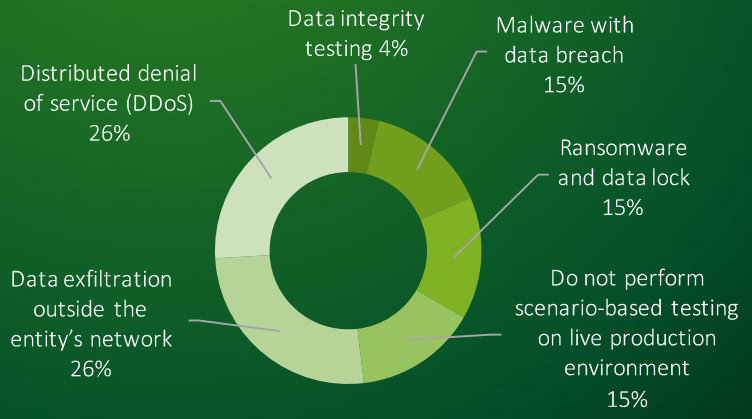
Components of the Digital Operational Resilience Testing Program



Vulnerability assessments, methodologies, penetration testing and exercising are the most common components of the operational resilience testing program.

Usage of Tools and scenario-based testing on live environment are the lowest followed components of the operational resilience testing program.

Types of scenario-based penetration testing on the financial entities' live production environment



Distributed Denial of Service and Data Exfiltration are the two types of scenario-based penetration testing most performed in the live production environment.

Data integrity is the least performed with **6%**, while **4%** of surveyed financial entities do <u>not</u> perform scenario-based penetration testing on their live production environment.

Third-Party Providers and Threat Led Penetration Testing

Surveyed financial entities are performing threat led penetration testing using a mix of internal teams and consultants.*

57% of surveyed financial entities have Blue Team role internally, Red and Purple Team activities are covered by external consultants.

For **38%** of surveyed financial entities, Red, Blue and Purple Team roles belong to them.

For **6%** of surveyed financial entities, Blue Team role belongs to the financial entity; Red and Purple Team activities are covered by third-party consultants.

Extent of involvement of the Third-Party Providers in the financial entities threat led penetration testing*

46%

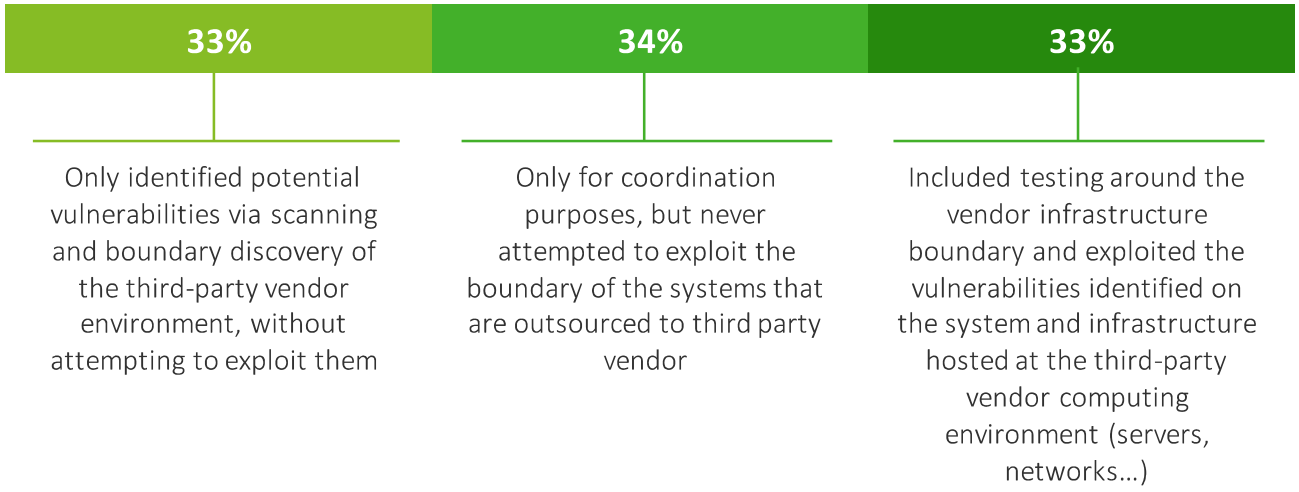
46% of the surveyed financial entities involve their Critical Third-Party Providers in the thread led penetration or red team testing.

54%

In comparison, **54%** of the surveyed financial entities **do not** involve Critical Third-Party Providers in any of the red team testing.

While performing resilience testing on the critical and important functions, surveyed financial entities cite the inclusion of the related third-party providers as a top challenge.

How were third-party providers **involved** in red-team testing?



*See Glossary

Pillar IV: ICT third-party risk

The DORA covers minimum contractual elements of the relationship with ICT third-party deemed crucial to enable complete monitoring by the financial entity.

The DORA envisages the monitoring of ICT risks deriving from third-parties in two ways:

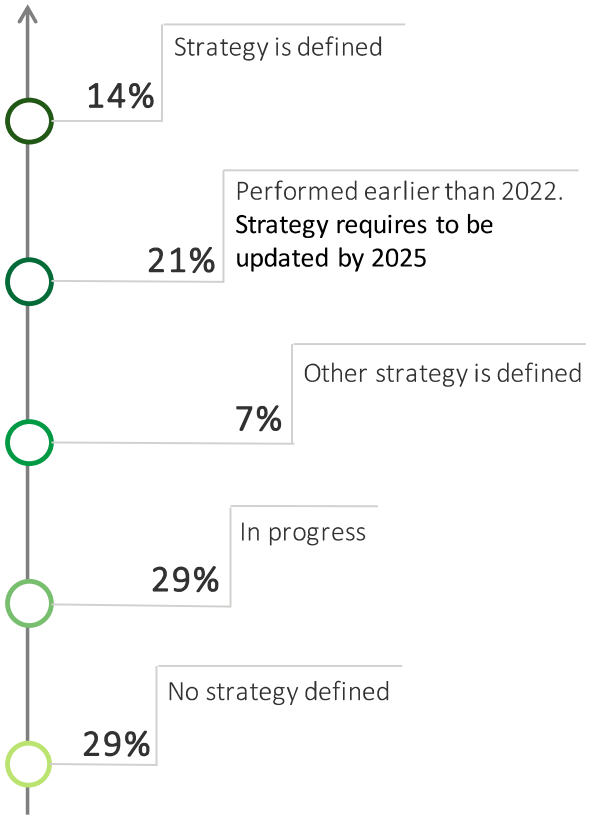
- Requirements for all third-party providers
- Requirements for critical third-party providers

Expected Challenges

- Regular review of strategy on ICT third-party risk considering the multi-vendor strategy.
- Yearly reporting to the competent authorities about 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 services and functions which are being provided.
- Establishing an effective process to verify the compliance of the ICT third-party service providers responsible for critical or important functions prior to concluding the contractual arrangements with them.
- Agreeing with the ICT third-party service provider to participate and fully cooperate in a threat led penetration testing of the financial entity and commitment to provide "unrestricted access to premises" in contracts concerning critical important functions.
- Defining the multi-vendor strategies with obligation to conduct concentration risk assessments of all outsourcing contracts that support the delivery of critical important functions.

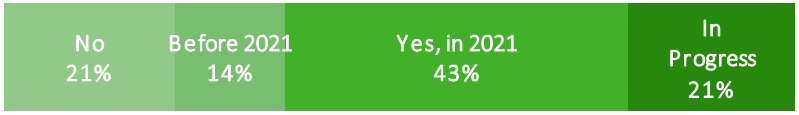
Multi-Vendor and Third-Party Providers

Status of defining a holistic ICT multi-vendor strategy, at group or entity level at surveyed financial entities*



*The DORA final Text indicates Multiple vendor strategy may be defined (Article 6.9)

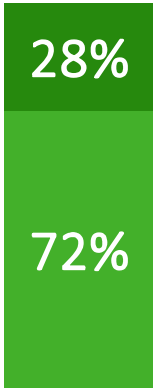
Have surveyed financial entities performed a business impact assessment to identify the dependency on the external vendors and third-party providers?



Concentration risk in the third-party portfolio of financial entities

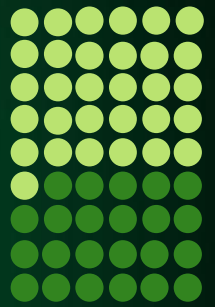
28% of surveyed financial entities analyzed the risk within their portfolio of third-party providers.

About **72%** of surveyed financial entities have **not** analyzed yet the concentration risk within their portfolio of third-party providers, **nor** the setup of business continuity measures in case of interruption of outsourced services.



Are Multi-Vendor Solutions ready at financial entities?

57% of surveyed financial entities do not have a multi-vendor solution implemented and tested.



43% of surveyed financial entities have analyzed business continuity scenarios where they terminate the contract with a third-party provider servicing their critical and important functions with the necessary continuity measures.

Third-Party Risk Assessments

Frequency of performing Third-Party Risk Assessments for providers

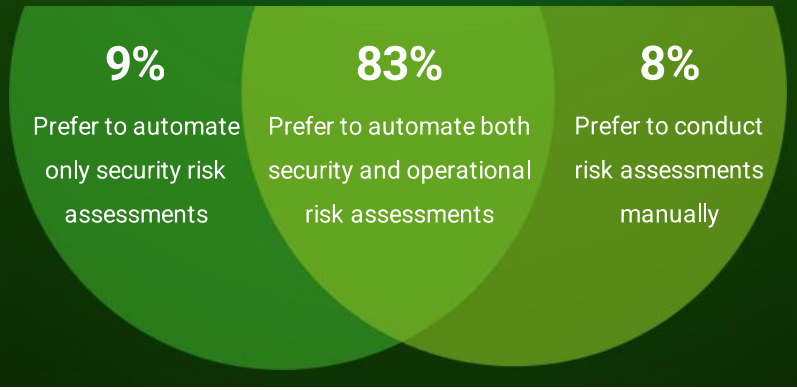
13%

Of surveyed financial entities perform third-party risk assessments on continuous basis as required by the DORA.

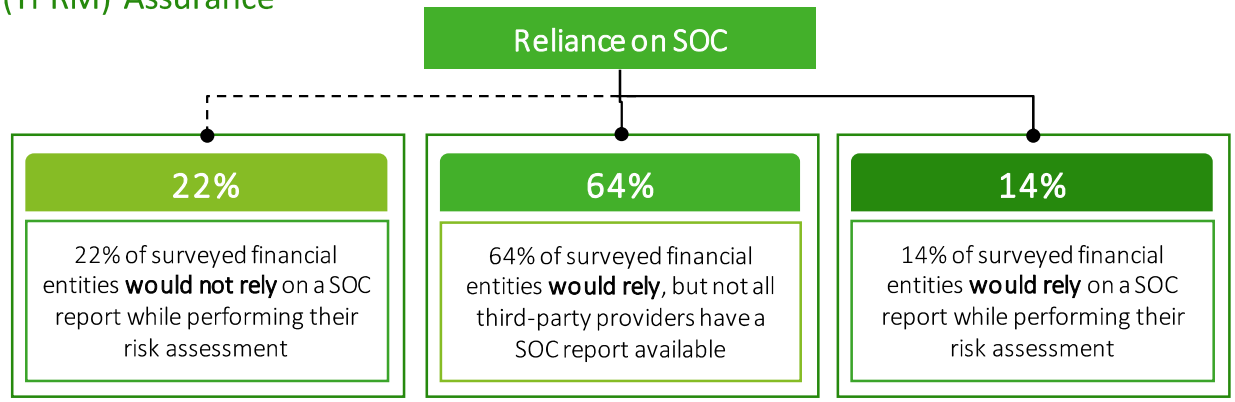
About **69%** of surveyed financial entities perform third-party risk assessments once per year, which is not enough to match the DORA requirements.

18% do not have a program established yet.

Automating the third-party risk assessments



Service Organization Controls (SOC) report for Third Party Risk Management (TPRM) Assurance



78% of surveyed financial entities would rely on Service Organization Controls report if available to perform the risk assessment on their third-party providers

Descriptive approaches of the entities regarding the ICT third-party management program*

71% 71% have TPRM personnel **manually analyzing and reviewing** the evidence provided from each third-party on their risk assessment

43% 43% of the surveyed financial entities **outsource the risk assessments** of third-party providers to a consulting company

29% 29% **outsource the analysis and review** of the evidence provided from each third-party on their risk assessment

29% 29% **aim to automate the analysis and review** of the evidence provided from each third-party on their risk assessment

*Multiple answers were selected

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

Anshuman Choudhary
Partner | Regulatory and Legal Support
Gateway Building
Luchthaven Brussel Nationaal 1J
B-1930 Zaventem
Tel: + 32 493 40 96 04
anschoudhary@deloitte.com

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").

Deloitte.