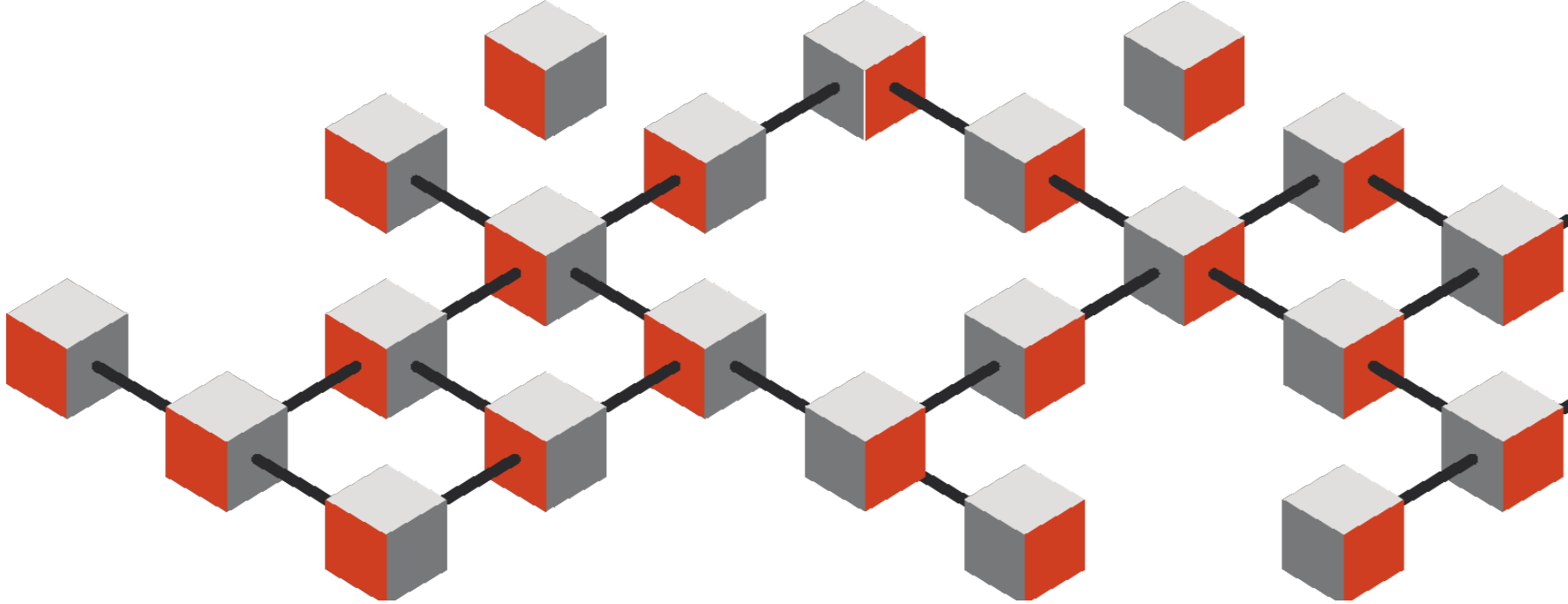
pwc



Operational Resilience and Interdependencies with Risk Management Framework

#2

Operational Resilience & Risk Management

Operational Resilience, is the ability of an organization to deal with risks of disruption to processes and applications that support its business while maintaining its viability.

The Digital Operational Resilience Framework ultimately aims at identifying, assessing, mitigating and managing risks that may impact critical functions related to the organization's core business.

Key action areas

- Identify and map critical functions
- Collect data and information
- Define impact tolerances
- Perform (stress) scenario testing
- Monitor and mitigate risks

Operational Resilience Framework

The Operational Resilience Framework enables financial institutions to **minimise** the impact of critical events on their core business by identifying, assessing and mitigating them.

In developing an **Operational Resilience Framework** that meets the objectives, it is essential that financial institutions consider their business model and protect the "critical or important functions".

With this in mind, the **Business Model Analysis (BMA)** - regularly conducted as part of the SREP - is the process of identifying not only the "critical or important functions" of financial institutions, but also potential vulnerabilities that may have a **disruptive** impact on the institutions themselves and their ability to provide relevant services.

Structure of the Risk Operational Resilience Framework

1 Mapping of critical functions and processes

- The first step is to identify and map the so-called **"critical or important functions"**, taking into account the organisation's **business model** and considering synergies **with what has already been defined in the Recovery Plan and Resolution Plan**.
- Once the "critical or important functions" are defined, **all key processes, technological chain and third parties** that support them need to be **identified and mapped**.

2 Identification of metrics and data collection

- A necessary and fundamental step for a robust operational resilience assessment methodology is the **identification and establishment** of **assessment metrics**.
- Proper identification and calculation of assessment measures **requires data** to be **collected** in a **regular** and **structured manner**.

3 Set of Impact Tolerance

- Once the "critical or important functions" have been identified, the metrics defined and the underlying information collected, the organisation can estimate the **impact tolerance**, i.e. the level **of risk tolerance**, **for each critical function and underlying operational process, in line with its risk appetite**.

4 Definition of Scenario-Testing

- As the future scenarios in which operational resilience is to be modelled may vary, an **assessment methodology based on scenario analysis** should be envisaged.
- It checks the **consistency of the scenarios** with those used in other **risk management processes** of the company (for operational risk modelling and business continuity, as an example).

5 Continuous monitoring

- Once the **definition and implementation** of the **Operational Resilience Risk Management Framework** is complete, the organization should establish and implement a **process for monitoring and reporting on the level of operational resilience**.

Note: The principle of proportionality should be taken into account when designing and implementing such a framework. Where 'Significant Institutions' can leverage the 'critical or important functions' already defined in the Recovery & Resolution plan, 'Less Significant Institutions' should carefully evaluate and define which functions are critical in light of their business model.

Mapping of critical functions and processes

"A function the disruption of which would materially impair the financial performance of a financial entity, or the soundness or continuity of its services and activities, or the discontinued, defective or failed performance of that function would materially impair the continuing compliance of a financial entity with the conditions and obligations of its authorisation, or with its other obligations under applicable financial services law".

Source: Digital Operational Resilience Act, Article 3, paragraph 22

1 **Defining critical or important functions**

When identifying and allocating the so-called "critical or important functions", the organisation's business model must be taken into account and synergies must be exploited by using what has already been established in the Recovery and Resolution Plan.

2 **Mapping the key processes**

Once the "critical or important functions" are defined, the organisation should identify and map all underlying 'key processes', also taking into account that a key process could support more than one "critical or important function".

3 **Identification of dependencies**

Identify dependencies for each "key process", the associated "dependencies" must be identified. The Key Dependencies represent the resources required for the correct and complete functioning of the "critical or important function".

Defining and setting impact tolerances

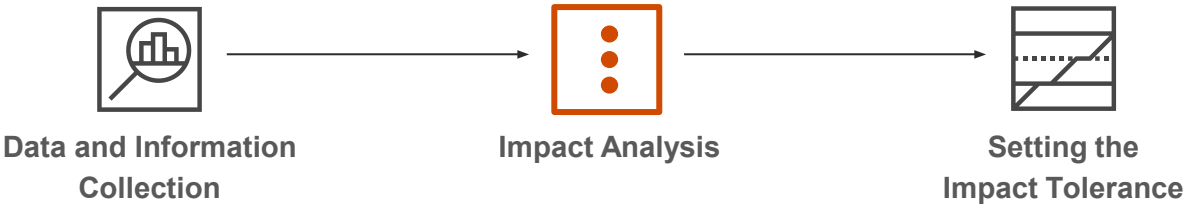
DORA requires that the organization defines a digital operational resilience strategy and sets a tolerance level consistent with the financial institution's risk appetite and impact tolerance for threats related to ICT risks analysis.

Definition and evaluation

Impact Tolerance can be defined as the **maximum tolerable level of disruption** of a "critical or important function", including the **maximum tolerable duration of such disruption**.

The organisation should establish impact tolerance levels **for all "critical or important functions"**, **processes** and **underlying key dependencies** in accordance with applicable regulation.

Logical steps



The crucial factor for the correct estimation of the impact tolerance is **the collection of all data and information underlying the metrics** useful for the estimation.

The **ultimate goal** for the organisation is to **establish the impact tolerance level consistent with the overall risk appetite** in order to determine the level of tolerable risk under different scenarios and to intervene with appropriate mitigation measures so that the conscious risk appetite is not exceeded. In this context, it is crucial to design and implement the **monitoring** process of the identified metrics.

Performing scenario testing

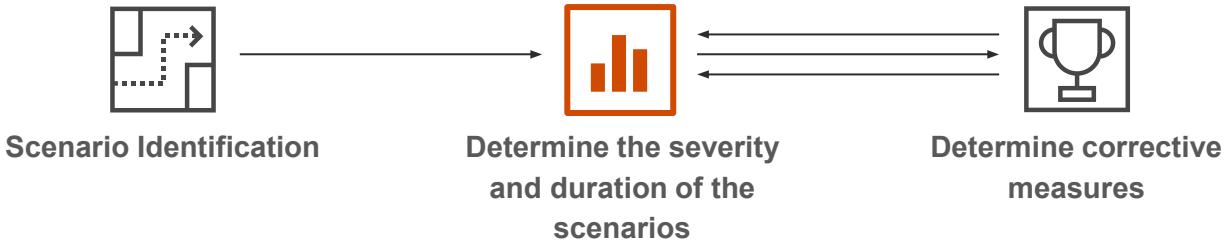
“For the purpose of assessing preparedness for handling ICT-related incidents, of identifying weaknesses, deficiencies and gaps in digital operational resilience, and of promptly implementing corrective measures, financial entities shall … establish, maintain and review a sound and comprehensive digital operational resilience testing programme as an integral part of the ICT risk-management framework …"

Definition and evaluation

In order to assess its ability **to be resilient over time and with respect to different scenarios**, the organisation shall define the reference scenarios and the scenario testing methodology, taking into account the principle of consistency with what has been adopted for the assessment of the different types of risks.

Test scenarios should focus on the **response and recovery actions** that the organization should implement when a **supply interruption occurs**, in order to maintain the functioning of the "critical or important function" active.

Logical steps



In identifying scenarios and determining their severity and duration, the organisation may refer to **incidents or events** that can be identified as **occurring internally** or **apply to the entire sector**.

The overall analysis should also assess the so-called emerging risks and **ESG risk drivers** (Environmental, Social and Governance).

In accordance with Article 24 of DORA, the organisation should, **at least once a year**, assess **all** its **ICT applications/systems associated with "critical or important functions"**.

Source: Digital Operational Resilience Act, Article 24, paragraph 1

Thank you.

pwc.de