

FINMA Circular 2023/1

What does it mean for your data strategy and data management?

Background

On 13 December 2022, the Swiss Financial Market Supervisory Authority FINMA published the fully revised circular on operational risks and resilience at banks ([FINMA Circular 2023/1](#)). With the total revision of the 'Operational Risk – Banks' Circular 2008/21, FINMA **refines** its **supervisory practice** regarding the management of operational risks, particularly in connection with **information and communication technology, handling of critical data** and **cyber risks** (see chapter IV, letter A-F of the Circular). In addition, the revision incorporates the requirements for **operational resilience** (see chapter V of the Circular).

The Circular will **enter into force on 1 January 2024**, where additional gradual transitional provisions for ensuring operational resilience apply over two years.

For the entire Circular, the principle of proportionality applies, i.e. the respective margin numbers are to be implemented on a case-by-case basis, depending on the size, complexity, structure and risk profile of each institution.

In the following section, we would like to provide a brief overview regarding the specified requirements for the risk management of critical data (see chapter IV, letter D of the Circular).



Chapter IV, letter D – 'Critical data risk management' of the FINMA Circular 2023/1 expands the previous focus on **confidentiality** of Client Identification Data (CID) to include the dimensions **integrity and availability** of critical data.

This clarification of the handling of critical data is also accompanied by an increase in the desired level of protection compared to Annex 3 of FINMA Circular 2008/21.

FINMA defines critical data as **data that**, in view of the **institution's size, complexity, structure, risk profile and business model**, are of such **crucial significance** that they require increased security measures.

These are data that are:

- **crucial** for the successful and sustainable **provision of the institution's services** or
- for **regulatory purposes**.

Data can be classified as critical based on each of the following aspects:



Confidentiality



Availability



Integrity

Data shall be categorised on the basis of its criticality (confidentiality and/or availability and/or integrity)

Critical data in terms of confidentiality:

- Confidential data is business information, customer or personal data that must be protected from unauthorised access to protect the privacy or security of an individual or organisation.

Critical data in terms of integrity and availability:

- Relates to the institution's ability to operate efficiently and effectively – or in some cases to operate at all. Critical data are therefore vital for the functioning of the institute ('mission-critical data').
- If this type of data is damaged, destroyed or becomes inaccessible, the institute and its units and staff may no longer be able to perform their duties.
- Critical data related to integrity and availability are to be defined by a risk-based approach.
- e.g. data used in financial reports (both internal and external), regulatory reports, for a decision-making process, a technical realisation or to measure business performance.

The circular sets out the following main responsibilities and requirements:

Board of Directors (BoD)

- **Approve and supervise** the protection of critical data such as the establishment of a **data strategy** including a governance and organisation framework, processes, data and information architecture as well as data security (Mn 23-25, 71).

Executive Board (ExB)


- **Manage the protection of critical data through its entire lifecycle** (incl. data ownership, data storage, retention and purging) as well as the definition of sufficient processes, procedures and controls including clear tasks, roles and responsibilities (Mn 25, 72, 74-75).



Organisation and risk control (RC)

- Raise awareness, monitor and list employees with access to critical data (Mn 26, 80).
- Identify and categorise the critical data (Mn 73).
- Define data responsibilities and access rights (Mn 73, 76-78).
- In case critical data is stored abroad or can be assessed from abroad, additional risk mitigation and monitoring measures should be implemented (Mn 79).
- Due diligence and monitoring of employees and service providers who can assess critical data (Mn 80, 82).
- Create and keep up-to-date a list with persons with privileged access rights (Mn 80).



 Proportionality principle applies
Mn refers to margin



Key action items

To ensure compliance with the requirements regarding critical data risk management of FINMA Circular 2023/1, organisations need to specifically address the following topics:

Establish a data strategy

- Such a strategy shall include the strategy definition and information regarding governance and organisation framework, processes, data and information architecture as well as data security (see Explanatory Notes to the FINMA Circular 2023/1).
- The strategy needs to be linked to the overarching business strategy of the institution, as well as other relevant strategies, e.g. IT strategy and needs to be approved by the Board of Directors (BoD).*

* Either directly or indirectly via the overarching business strategy.

Note:

Data strategies differentiate in their general approach towards a more defensive or offensive setup. The chosen approach often depends on the overall business objectives of the organisation.

- **Defensive:** is about minimising risk. It includes being compliant with industry-specific regulations, using analytics to detect and limit fraud, and implement controls to prevent theft.
- **Offensive:** focuses on supporting business objectives, such as increasing revenue, profitability and customer satisfaction.

Define and implement data governance structures

- Based on our experience, the definition of clear tasks, competencies and responsibilities for dealing with critical data is a challenging topic, as it is very often also a political discussion.
- Exemplary questions organisations should consider:
 - Which unit shall be responsible for data management and how 'senior' should the data management lead be (strategic vs. operative orientation of the role)?
 - Which roles are required for an efficient and effective data governance (chief data officer/head data management, data owner(s), data steward(s) and data custodian(s))?
 - How should tasks, competencies and responsibilities be split across the roles?
 - Is the setup of a data committee required or can existing committees be leveraged?

Note:

Data governance must be anchored in the organisation and its culture, which is why no 'one-size-fits-all' solution can be applied. The implementation of a Data Governance function in the existing structures of an organisation therefore requires individual decisions on the operational and strategic implementation.

Identify and categorise critical data

- Define a structured methodology to identify and categorise critical data regarding confidentiality, integrity and availability.
- Consider electronic and physical data.
- Establish efficient maintenance processes to ensure an up-to-date inventory of storage locations of critical data (see mn. 53-54).

Note:

- A limitation that only data which is required for critical functions qualifies as critical data is not adequate, as important risks could be overlooked. Also vice versa there is no automatism that data which is required for critical functions is automatically critical data. See section 3.3.2 of the report on outcome of consultation (= 'Anhörungsbericht').
- Data must be categorised based on its criticality towards the aspects of confidentiality, integrity and availability. It is not sufficient to simply flag data as 'critical data'.

Define appropriate processes, procedures and controls for dealing with critical data

Non-exhaustive list:

- Define concrete and relevant risk tolerance statements, including tolerance limits (KRIs / KPIs) for data management risks.
- Define appropriate protection measures for identified critical data based on its criticality.
- Ensure appropriate access rights management for critical data (incl. critical data in test environment).
- Promote employee awareness programmes for critical data and trainings.
- Ensure management of critical data as part of tasks outsourced to third-party service providers (i.e. increased due diligence, monitoring and controlling requirements).
- Implement procedures for detecting and evaluating incidents involving data (theft and/or loss) including incident reporting and analysis processes.

Note:

- The entire data lifecycle needs to be covered (data creation/acquisition, data processing, data analysis, data storage, data sharing, data retention, data purging)

Critical data and data protection

Besides compliance with the provisions of the FINMA Circular 2023/1, organisations also need to ensure compliance with the requirements of the applicable data protection law for critical data falling into the definition of personal data. Considering the interdependencies and the similarities in terms of entry into force of the FINMA Circular and the revised Data Protection Act in Switzerland, which will apply as of 1 September 2023, it is

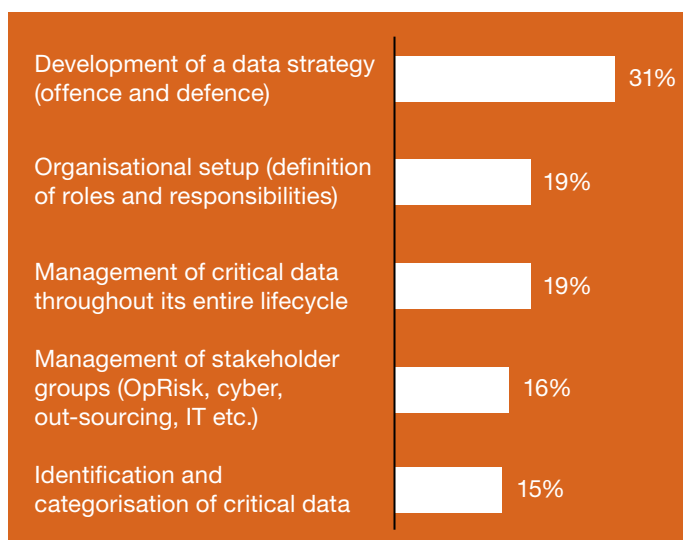
highly recommended to align the implementation projects for both regulations in order to ensure consistency and synergy effects. For example, insights regarding data mapping, flows and transfers gained during the creation of the register of processing activities (RoPA) could be leveraged to define the appropriate protection measures for critical data.

Survey January 2023

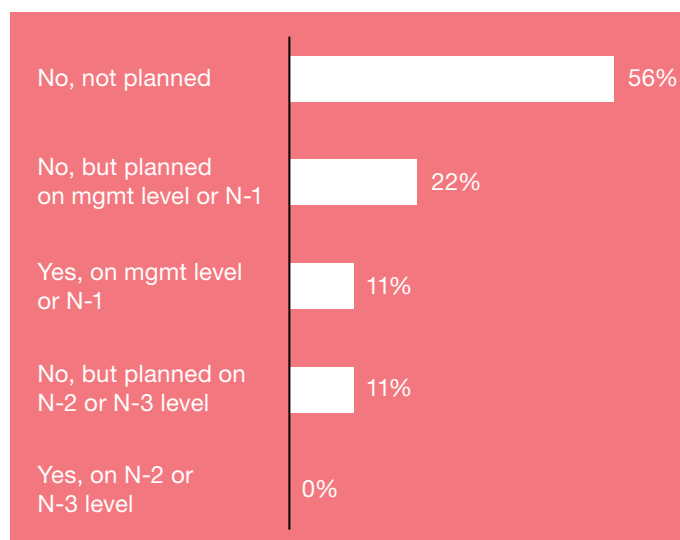
We have asked our clients where they see the biggest challenges within their organisations in regard to the management of critical data (see below figure). The development of a data strategy as well as definition of roles and responsibilities is at the top of the list, as it is

very often also a political discussion on who should be responsible for the data. This is also shown in the fact that the majority has not yet nominated a chief data officer/ head data management.

Where do you see the biggest challenges within your organisation in regard to the management of critical data?



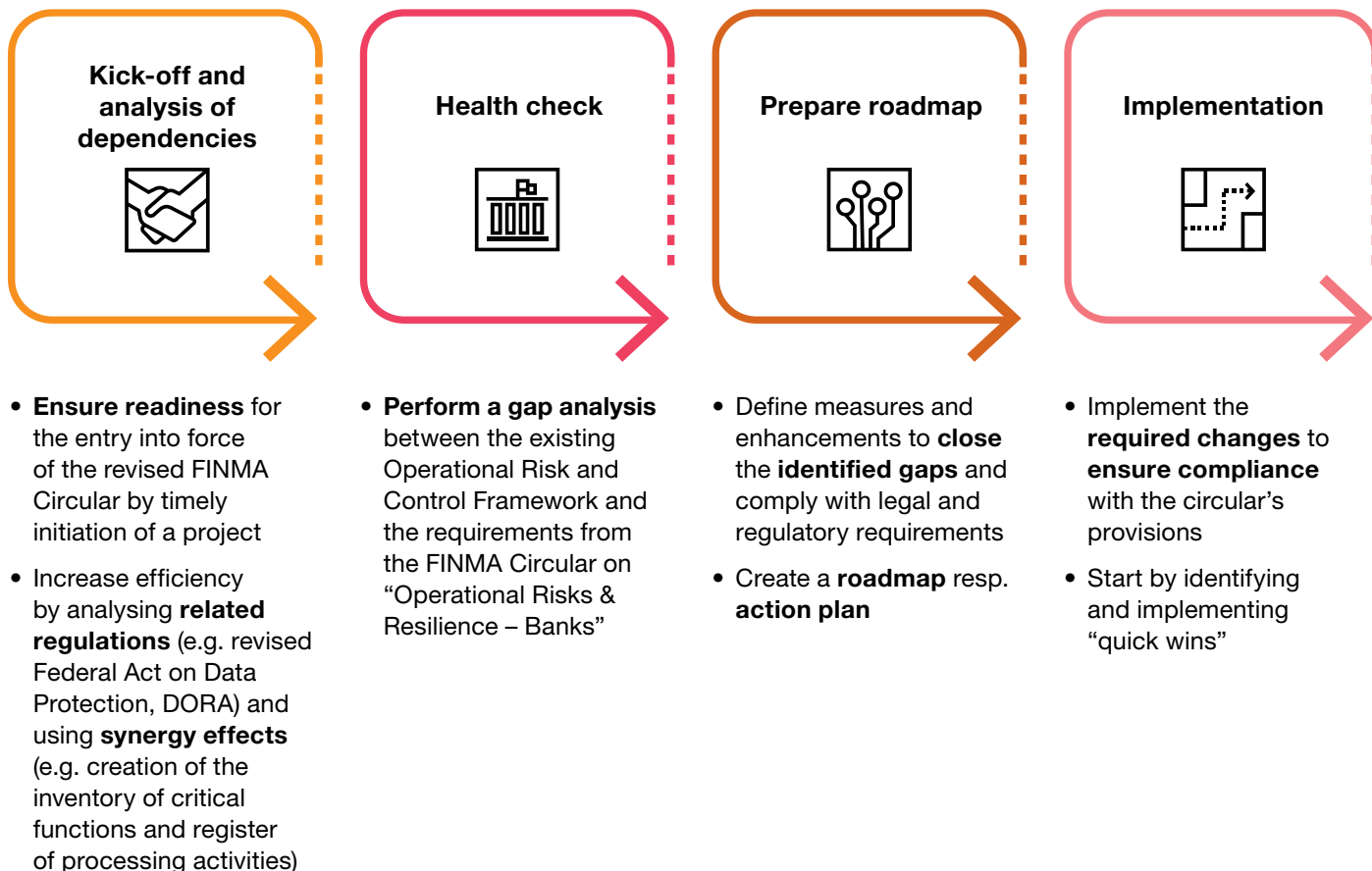
Chief data officer/head data management already nominated?



Source: PwC Roundtable, survey 25 banks, January 2023



Proposed next steps



This blogpost is part of PwC’s series on data in financial services, where we provide insights on recent topics and debates ranging from regulations and governance to data strategy and commercialisation. Going forward, our next episode will focus on the establishment of a holistic data strategy.

Contacts

Please do not hesitate to contact us if you are interested in an exchange on how we can support you in becoming compliant with the FINMA Circular 2023/1 or require assistance for any other topic related to data management.



Prafull Sharma
Partner,
CIO Advisory,
Cloud & Data
prafull.sharma@pwc.ch



Beate Fessler
Senior Manager,
FS Business and
Regulatory Transformation
beate.fessler@pwc.ch

