**Audit points for critical data risk management**

**Overview**

|  |  |
| --- | --- |
| **Subject:** | **Critical data risk management** |
| **Audit depth:** | [Audit/critical assessment][[1]](#footnote-2) |
| **Basis:**  (non-exhaustive list) | Art. 3 para. 2 let. a Banking Act (BA)  Art. 9 Financial Institutions Act (FinIA)  Art. 12 Banking Ordinance (BO)  Arts. 12, 67, 68 and 73 Financial Institutions Ordinance (FinIO)  Art. 11 para. 4 and 15 Financial Market Infrastructure Ordinance (FinMIO)  Margin nos. 13, 50, 52, 53, 58 and 59 FINMA Circular 2017/1 “Corporate governance – banks” (FINMA Circ. 17/1)  Margin nos. 71-82 FINMA Circular 2023/1 “Operational risks and resilience – banks” (FINMA Circ. 23/1) |
| **Sign-offs:** | |  |  |  |  | | --- | --- | --- | --- | | **Sign-offs:** | **Name:** | **Function:** | **Date:** | | Auditor: | [Name] | [Assistant / Senior / Manager / Senior Manager / CEO / Partner] | [DD MM YYYY] | | Reviewer: | [Name] | [Manager / Senior Manager /  CEO / Partner] | [DD MM YYYY] | |

**This is the standard work programme that is to be implemented for every intervention under the terms of the audit strategy (margin no. 28ff FINMA Circ. 13/3 “Auditing”). It is the responsibility of the audit team to adapt the standard work programme to the specific situation of the institution (size, business model, organisation, processes, risk exposure etc.). If the specified audit procedures are not carried out completely, an appropriate rational must be provided in the working paper. Audit procedures marked with an asterisk (\*) are not applicable to Category 4 or 5 banks. Audit procedures marked with two asterisks (\*\*) are not applicable to institutions specified under Article 47a to 47e CAO, persons specified under Article 1b BA and investment firms (non-proprietary trading).**

**Overall conclusion**

| **Topic:** | **Information / description:** |
| --- | --- |
| Overall conclusion | |  |  | | --- | --- | | **Confirmation in audit report:** | **Conclusion:** | | Confirmation that the area “critical data risk management” was designed adequately.  Confirmation that the institution complied with the stricter requirements ordered by FINMA. | ***Yes*** *(Audit/critical assessment) /* ***No***  ***Yes*** *(Audit/critical assessment) /* ***No*** | |
| Summary of significant findings / notices of reservations and recommendations (see details below) | [Summary of significant findings / notices of reservations and recommendations] |
| Audit areas, results and procedures performed by Internal Audit on which audit firm placed reliance (including audit firm’s own assessment) | [Description] |

**Audit programme – critical data risk management**

| **No.** | **Procedures for audit depth  “critical assessment”:** | **Additional procedures for audit depth “audit”:** | **Procedures performed/findings:** | **WP ref.:** |
| --- | --- | --- | --- | --- |
| *Management of critical data risks considering the principle of proportionality, i.e. taking into account the size, complexity (especially with regard to ICT and outsourcing), structure and risk profile:* | | | | |
| 1 | Obtain a basic understanding of the institution’s general handling of critical data, considering the principle of proportionality and the following audit procedures. |  |  |  |
| 2 | Assess the adequacy of the institution's policies in relation to critical data and managing critical data risks (such as policies, procedures, standards guidelines) . | Assess the consistency of the strategy for dealing with critical data risks with the institution's policies (such as risk policy, risk management principles, operational risk management, business strategy, ICT and data strategy etc.). |  |  |
| *Integration into overarching operational risk management and strategy, governance and awareness (margin nos. 23–26, 30-31, 40 and 71 FINMA Circ. 23/1):* | | | | |
| 3 | Assess whether critical data risks (such as lack of data governance, poor data quality, unavailability, unauthorised data manipulation, data loss, data theft, data corruption) are integrated into the overarching operational risk management as a separate taxonomy and thus adequately and comprehensively addressed in the identification, assessment, mitigation, monitoring and reporting of operational risks. |  |  |  |
| 4 | Assess whether audit results and/or other risk and control assessments are considered as part of the risk identification and risk assessment of operational risks in accordance with margin no. 30 . |  |  |  |
| 5 | Assess whether the executive board regularly approves a strategy for dealing with critical data risks and monitors its compliance. | Assess whether the strategy for dealing with critical data risks and/or other protective measures adequately addresses the following aspects of managing critical data risks:   * institution-specific definition of critical data, * systematic identification of data and categorisation, * comprehensive critical data risk management, * tasks, competencies and responsibilities for handling critical data, * measures for ensuring the confidentiality, integrity and availability of critical data. |  |  |
| 6 | Assess whether the board of directors regularly (at least annually) evaluates and approves the risk tolerance for critical data risks in accordance with the risk policy, taking into account the institution’s strategic and financial objectives. |  |  |  |
| 7 | Assess the adequacy of the identification of material inherent risks with respect to critical data risks, i.e. if critical data risks are not identified as material inherent risks, assess the plausibility of the explanation provided. | Review, on an appropriate sample basis, the elements for identifying material critical data risks and assess whether potential risks associated with critical data are identified and addressed, and whether the assessment of the materiality of inherent risks is in line with the risk tolerance. |  |  |
| 8 | Assess the organisational measures taken to raise awareness among employees and key external personnel (including contractors) with regard to their tasks, competencies and responsibilities for the reduction of risks in handling critical data. | Assess, on the basis of appropriate sample through random sampling testing of key personnel and external personnel (including contractors),whether sufficient measures are in place to raise awareness of the handling of critical data. A selection of the following measures might be expected:   * confirmation of acknowledgement of and compliance with the Code of Conduct, * training to raise awareness on the handling of critical data, * internal notices and regular communication about the handling of critical data, data security and data protection, * target group-specific training for internal and external personnel with (elevated) access rights to critical data. |  |  |
| 9 | Assess the adequacy of the training provided on the topic of handling critical data, taking into account current risks and the needs of specific audiences (e.g. for employees with access to critical data, employees with privileged or elevated rights, managers, external personnel [including contractors]). |  |  |
| 10 | Assess the adequacy of reporting to the executive board (content, frequency etc.) on the development of relevant ICT risks (incl. critical data risks), the effectiveness of key controls, and major internal and external incidents. |  |  |  |
| 11 | Assess the results of audit and control procedures performed by Internal Audit and/or other control functions (e.g. Independent Risk Control) related to the management of critical data risks, and review minutes of relevant committees and function meetings. |  |  |  |
| *Tasks, competencies and responsibilities (margin nos. 72 and 75 FINMA Circ. 23/1):* | | | | |
| 12 | **\*\*** Assess the adequacy, qualifications and independence of the entity providing the (independent) control function to ensure the confidentiality, integrity and availability of critical data through appropriate processes, procedures and controls. |  |  |  |
| 13 | **\*\*** Assess the adequacy of the tasks, competencies and responsibilities for handling data identified by the institution as critical throughout the life cycle of such data to ensure confidentiality, integrity and availability. | **\*\*** Assess, on the basis of appropriate samples of key personnel, whether the tasks, competencies, and responsibilities for handling critical data are adequately defined and assigned. The following aspects should be considered:   * clear description of roles (e.g. data producer, data consumer, data administrator, data quality analyst, data owner / steward / custodian etc.), * clear description of the tasks, competencies and responsibilities of the roles, * clear description of the organisation, functional distinctions, reporting lines and communication channels. |  |  |
| 14 | **\*\*** Assess the adequacy of the assignment of tasks, competencies and responsibilities for handling the data identified as critical by the institution throughout the life cycle of such data to ensure confidentiality, integrity and availability. | **\*\*** Assess, on the basis of appropriate samples of key personnel, whether the following are adequately addressed:   * qualifications and experience, * function, * proportionality of the allocation of data elements per data controller. |  |  |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Procedures, processes and controls (margin nos. 74, 75 and 76–78 FINMA Circ. 23/1): | | | | |
| 15 | Assess the adequacy of key controls for handling critical data to ensure confidentiality, integrity and availability. Adequate key controls are performed regularly and protect critical data throughout its life cycle. This includes the generation, collection, processing,storage, retention, use, modification, disclosure, transfer, archiving, deletion and destruction of data. | **\*** Assess the operational effectiveness of key controls to ensure:   * confidentiality, e.g. with respect to controls in the area of information security and privacy, compliance checks, access management, Code of Conduct, awareness training etc. * integrity, e.g. in terms of data quality controls, plausibility controls, automatic and/or manual reconciliation controls, business approval, 4 eyes principle, segregation of duties etc. * availability, e.g. regarding monitoring of data transmission and processing, data traceability, data backup and recovery etc. * completeness with respect to data destruction |  |  |
| 16 | **\*** Assess the processes, procedures and controls of the institution to ensure an appropriate level of confidentiality and security in the handling of critical data during the operation, development, modification and migration (change) of critical data. | **\*** Assess the operational effectiveness of key controls to ensure an appropriate level of confidentiality and security in the handling of critical data during the operation, development, modification and migration (change) of critical data. |  |  |
| *Inventory (margin nos. 53, 63 and 73 FINMA Circ. 23/1):* | | | | |
| 17 | Assess whether the critical data of the organisation is systematically identified, recorded and categorised. For example, a data inventory contains the following information (attributes):   * storage location and/or cloud environment, * software (incl. version control), * categorisation (criticality), * dependencies within the institution, * internal and external sources, * interfaces to external service providers, * data ownership. | Assess, on a sample basis as appropriate, the institution's data quality controls (e.g. plausibility checks, reconciliations) that help to ensure the completeness and accuracy of the data inventory. |  |  |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| *Access management (margin nos. 76–78 and 80 FINMA Circ. 23/1):* | | | | |
| 18 | **\*** Assess the adequacy of processes, procedures and controls for managing access to critical data and processing functions to employees and third parties (definition of roles, approval processes etc.). | **\*** Assess, on a sample basis as appropriate, the operational effectiveness of controls over the managing of access to critical data and processing functions to employees and third parties. In particular, the following should be considered:   * need-to-know / least privilege principle, * existence of an Identity & Access Management (IAM) system, * degree to which systems with critical data integrate with the authorisation and identification process, * degree of integration of different user accounts (such as technical accounts, system accounts, privileged accounts, guest accounts, remote service accounts etc.). |  |  |
| 19 | \* Assess the adequacy of the processes and controls to identify, manage and monitor access (standard and privileged) to critical data. | **\*** Assess, on a sample basis as appropriate, the operational effectiveness of key controls for identifying, managing and monitoring access (both standard and privileged) to critical data. |  |  |
| 20 | **\*** Assess whether the physical and logical ICT that stores or processes the critical data is adequately protected. | **\*** Assess, on an appropriate sample basis of critical components[[2]](#footnote-3) whether critical data is adequately protected, e.g. by encryption, secure transmission and other technical measures. |  |  |
| 21 | | **\*** Assess the adequacy of the controls and security requirements for user profiles with elevated privileges. | **\*** Assess the adequacy of the controls (e.g. analysis of log files, temporary assignment of access rights, more frequent review controls, eyes principle / peer reviews) and security requirements for individuals with elevated privileges, and whether a list of such individuals is maintained and regularly updated. |  |  |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| *Management of access from abroad (margin no. 79 FINMA Circ. 23/1):* | | | | |
| 22 | **\*\*** If critical data is stored outside Switzerland or can be accessed from abroad, assess whether the increased risks are adequately mitigated and the data is adequately protected. | **\*\*** Assess, on a sample basis as appropriate, whether organisational and technical measures are in place for adequately control the increased risks and adequately protect critical data when it is stored outside Switzerland or can be accessed from abroad. |  |  |
| *Incidents (margin no. 81 FINMA Circ. 23/1):* | | | | |
| 23 | Assess the adequacy of the processes, procedures and controls for managing incidents that significantly affect the confidentiality, integrity or availability of critical data. | Assess the operational effectiveness of the reporting process to FINMA based on an appropriate sample of incidents that have impaired the confidentiality, integrity or availability of critical data. |  |  |
| Due diligence review (*margin no.* *82 FINMA Circ. 23/1):* | | | | |
| 24 | Assess the adequacy of the due diligence process when selecting service providers that may access or manage critical data. | Assess, on an appropriate sample basis, whether the due diligence process for selecting service providers with access to critical data has been adequately performed |  |  |
| 25 | | Assess whether appropriate criteria for dealing with service providers with access to critical data are defined and set out in the contractual agreement. | Assess, on a sample basis as appropriate, whether service providers with access to critical data have agreed the institution's terms and conditions for the handling of critical data prior to entering into a contractual arrangement. |  |  |
| 26 | | Assess whether service providers with access to critical data are regularly monitored and reviewed as part of the institution’s internal control system. | Assess on an appropriate sample basis, whether service providers with access to critical data and their data usage are regularly monitored and audited. |  |  |

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

1. Margin nos. 33 and 34 FINMA Circ. 13/3 [↑](#footnote-ref-2)
2. FINMA Circ. 23/1 Annex 1 [↑](#footnote-ref-3)