**Audit points for internal organisation and internal control system**

**Overview**

|  |  |
| --- | --- |
| **Subject:** | **Internal organisation and internal control system**  |
| **Elements covered/Audit depth:** | Covered elements: [xx]Audit depth: [Audit/critical assessment][[1]](#footnote-2) |
| **Regulations**(non-exhaustive list) | Arts. 3 para. 2 let. a and cbis Banking Act (BA)Arts. 9 and 11 Financial Institutions Act (FinIA)Arts. 9-12 Banking Ordinance (BO)Arts. 12 and 66-68 Financial Institutions Ordinance (FinIO)FINMA Circular 2017/1 “Corporate governance – banks” (FINMA Circ. 17/1; margin nos. 1-61 & 63 & 98-105)FINMA Circular 2010/01 “Remuneration schemes” (FINMA Circ. 10/1)[[2]](#footnote-3)FINMA Circular 2016/1 “Disclosure - banks” (FINMA Circ. 16/1, margin nos. 20, 41.1 & appendix 4) |
| **Sign-offs:** |

|  |  |  |  |
| --- | --- | --- | --- |
| **Sign-offs:** | **Name:** | **Function:** | **Date:** |
| Prepared by:  | [Name] | [Assistant / Senior / Manager / Senior Manager / Partner] | [DD MM YYYY] |
| Reviewer: | Name] | [Senior / Manager / Senior Manager / Partner] | [DD MM YYYY] |

 |

**This is the standard work programme that is to be implemented for every element covered in this audit field, under the terms of the audit strategy (margin no. 28ff FINMA Circ. 13/3). It is the audit team’s responsibility to adapt the standard audit programme to the audited institution’s specific situation (size, business model, organisation, processes, risk exposure etc.). If the specified audit procedures are not carried out in full, the underlying rationale must be explained in the working paper. Audit points marked with an asterisk are not applicable to Category 4 or 5 banks.**

**Overall conclusion**

| **Topic:** | **Information/description:** |
| --- | --- |
| Elements to be covered gradually over a period of 6 years (including audit depth) |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Elements:** | **20XX-2** | **20XX-1** | **20XX** | **20XX+1** | **20XX+2** | **20XX+3** |
| Adequacy of the overall internal organisation (organisational structure, segregation of duties, job descriptions, responsibilities and competences) | [A / CA / –] | [A / CA / –] | [A / CA / –] | [A / CA / –] | [A / CA / –] | [A / CA / –] |
| Adequacy of the internal directives (structure, clarity, up-to-datedness, periodic review and approval process, etc.) | [A / CA / –] | [A / CA / –] | [A / CA / –] | [A / CA / –] | [A / CA / –] | [A / CA / –] |
| Adequacy of the internal control system (methods for risk identification, assessment, measurement, monitoring and reporting, implementation of controls) | [A / CA / –] | [A / CA / –] | [A / CA / –] | [A / CA / –] | [A / CA / –] | [A / CA / –] |
| Measures to adequately limit conflicts of interest (including remuneration schemes) | [A / CA / –] | [A / CA / –] | [A / CA / –] | [A / CA / –] | [A / CA / –] | [A / CA / –] |
| Internal reporting (content, recipient, periodicity, escalation processes, etc.) and corporate governance disclosures | [A / CA / –] | [A / CA / –] | [A / CA / –] | [A / CA / –] | [A / CA / –] | [A / CA / –] |
| Risk policy and principles of institution-wide risk management | [A / CA / –] | [A / CA / –] | [A / CA / –] | [A / CA / –] | [A / CA / –] | [A / CA / –] |

 |
| Overall conclusion |

|  |  |
| --- | --- |
| **Confirmation in audit report:** | **Conclusion:** |
| Confirmation that corporate governance rules and guidelines have been respected and the areas “internal organisation” and “internal control system” have been adequately designed (based on audits results of covered elements). | **Yes** (Audit/critical assessment) / **No** |
| Confirmation that an adequate separation between the Board of Directors and the Executive Board exists (based on audit results of covered areas). | **Yes** (Audit / Critical assessment) / **No** |

 |
| Summary of significant findings(For details, see below.) | [Summary of significant findings] |
| Audit areas, results and work performed by Internal Audit on which audit firm placed reliance (including audit firm’s own assessment) | [Description] |

**Work programme – Internal organisation and internal control system – Adequacy of overall internal organisation**

| **No.** | **Topic:** | **Procedures for audit depth “critical assessment”:** | **Additional procedures for audit depth “audit”:** | **Procedures performed/findings** | **WP ref.:** |
| --- | --- | --- | --- | --- | --- |
|  |
|  | **Adequacy of the internal organisation**(organisational structure)Art. 3 para. 2 let. a and d BA / Arts. 9-11 BO & Art. 9 FinIA / Art. 12 and 66 FinIO | *Assess the adequacy of the organisational structure considering the size, business and organisational complexity of the institution, specifically:* |  |  |  |
| Obtain by-laws, organisational business regulations, partnership agreements or regulations and organisation chart including all geographical locations.Assess whether the division and its coverage area correspond to finance resources and the organisation of management.Assess whether the institution is actually managed from Switzerland and whether the members of the Executive Board are actually managing the institution and doing so responsibly.Assess whether the bank's Board of Directors (BoD) has at least three members. | Assess whether the information in the by-laws, the organisational business regulations and organisational charts corresponds to the business and the geographical dimensions of the business. |  |  |
| Based on organisation chart obtained, identify responsible departments and assess the adequate organisation of key functions (functional and hierarchical integration, reporting lines, etc.). |  |  |  |
|  | **Adequacy of the internal organisation**(segregation of duties) | *Assess the overall adequacy of the segregation of duties considering the size, business and organisational complexity of the institution, specifically:* |  |  |  |
| For banks: Assess whether members of the BoD are organisationally separated to the Executive Board (Art. 3 para. 2 let. a BA & Art. 11 BO). |  |  |  |
| Assess organisational independence between risk-taking departments and the departments monitoring the risks (e.g. appropriate segregation of duties between credit business, trading desk, asset management and settlement within the institution [Art. 12 BO / Art. 67 FinIO]). |  |  |  |
|  | **Adequacy of the internal organisation**(job descriptions) | *Assess the overall adequacy of job descriptions considering the size, business and organisational complexity of the institution, specifically:* |  |  |  |
| Assess whether job descriptions for key personal are available and set-up based on uniform, adequate guidelines (form, content, authorisation, review processes). | Assess based on appropriate samples of job descriptions or other relevant documents for key personnel whether the following have been addressed in detail:* description of responsibilities
* description of competencies
* definition of reporting lines
* definition of escalation lines
* approval of job descriptions
* timeliness of the information provided.

Compare and assess in detail the adequacy of job descriptions with respect to the employees actual activities on a sample basis. |  |  |
|  | **Adequacy of the internal organisation**(responsibilities and competencies [checks & balances]) | *Assess the overall adequacy of responsibilities and competencies considering the size, business and organisational complexity of the institution, specifically:* |  |  |  |
| Assess whether the institution has defined the responsibilities and competencies of its key functions in written policies that are available to and known by them. |  |  |  |
|  | Assess if the BoD and the Executive Board have sufficient management competences and knowledge and experience of the banking and financial sector. Assess if the BoD is sufficiently diversified (margin nos. 16 and 51 FINMA Circ. 17/1). |  |  |  |
|  | Assess whether the BoD complies with the independence principles and at least one-third of its members are independent (margin nos. 17 to 25 FINMA Circ. 17/1). |  |  |  |
|  | Assess if the BoD complies with principles governing a directorship and, to this regard, ensures that every member devotes sufficient time to his role, defines or approves requirements profiles, which form part of its competences and makes at least once a year a critical assessment of its own performance (margin nos. 26 to 28, FINMA Circ. 17/1). |  |  |  |
|  | **Adequacy of the internal organisation**(division of responsibilities and committees) | *Assess the overall adequacy of the division of responsibilities and the set-up of committees considering the size, business and organisational complexity of the institution, specifically:* |  |  |  |
|  | Assess if the chair of the BoD assumes the internal and external representation and if that person has a key role in shaping the strategy, communication and culture of the company (margin no. 30, FINMA Circ. 17/1). |  |  |  |
|  | If there is an audit committee: Assess if the personnel composition of the audit committee differs sufficiently from that of other committees, if the majority of the members of the audit committee and of the risk committee are independent and if the other rules regarding the organisation are complied with (margin nos. 32 and 33 FINMA Circ. 17/1).  |  |  |  |
|  | **\*** Assess if both an audit committee and a risk committee have been established (however, institutions in supervisory category 3 may combine these into a single committee) and if these committees have ensured appropriate reporting to the BoD (margin no. 31, FINMA Circ. 17/1). |  |  |  |
|  | For systemically important institutions Assess if a remuneration and appointments committee has been established, at least at group level (margin no. 31, FINMA Circ. 17/1) |  |  |  |
|  | Assess whether the tasks of the audit committee (margin nos. 34-39 FINMA Circ. 17/1) have been adequately performed by the responsible body (audit committee or BoD). | Inspect minutes and reports for the purpose of assessing the actions taken by the competent body (audit committee or BoD). |  |  |
|  | Assess whether the tasks of the risk committee (margin nos. 40-46 FINMA Circ. 17/1) have been adequately fulfilled by the competent body (risk committee or BoD).  | Inspect minutes and reports for the purpose of assessing the actions taken by the competent body (risk committee or BoD). |  |  |

**Work programme – Internal organisation and internal control system – Adequacy of internal directives**

| **No.** | **Topic:** | **Procedures for audit depth “critical assessment”:** | **Additional procedures for audit depth “audit”:** | **Procedures performed/findings** | **WP ref.:** |
| --- | --- | --- | --- | --- | --- |
|  |
|  | **Adequacy of the internal directives / policies framework** (structure, clarity, up-to-datedness, periodic review and approval process, etc.) | *Assess the overall adequacy of the internal directives / policies framework considering the size, business and organisational complexity of the institution, specifically:* |  |  |  |
| Obtain an overview of all internal directives/policies available and assess whether relevant aspects of the entity’s activities are appropriately addressed. | Take an appropriate sample of key internal directives/policies to check whether these adequately cover the relevant aspects of the business activities and have been approved by the competent body. |  |  |
| Assess through inquiry the internal directives/policies establishing, review, update and approval process and assess whether the process is adequate (design). | Perform test of operating effectiveness of identified key controls with regards to the policy establishment, review, update and approval process. |  |  |
|  |
|  |  | Assess through inquiry and review of relevant documents (policies, directives, manuals, etc.) the overall adequacy of the institution’s guidelines to identify the need for changes in existing directives or for the issuance of new directives (as a result of strategy changes, process changes, regulatory developments, etc.). | Assess through examination of relevant documents the institution’s adherence to the internal guidelines regarding changes in existing directives and/or the issuance of new directives on a sample basis. |  |  |

**Work programme – Internal organisation and internal control system – Adequacy of internal control system**

| **No.** | **Topic:** | **Procedures for audit depth “critical assessment”:** | **Additional procedures for audit depth “audit”:** | **Procedures performed/findings** | **WP ref.:** |
| --- | --- | --- | --- | --- | --- |
|  |
|  | **Adequacy of internal control system** (methods for risk identification, assessment, measurement, monitoring and reporting, implementation of controls) | *Assess the adequacy of the methods for identification, assessment, measurement, monitoring and reporting of risks considering the size, business and organisational complexity of the institution, specifically:* |  |  |  |
| Assess whether the BoD sets the business strategy, and adequately addresses the establishment of policies and processes in relation to the identification, assessment, measurement, monitoring and reporting of risk, in order to establish and monitor an effective risk management and to manage overall risks (margin no. 10, FINMA Circ. 17/1). |  |  |  |
| Assess whether the BoD complies effectively with its duties regarding the organisation, the financial situation and for ensuring that the institution has appropriate levels of personnel and other resources (*inter alia* the appointment and the dismissal of the members of the committees) (margin nos. 11 to 13, FINMA Circ. 17/1).  |  |  |  |
| Assess whether the BoD ensures that all material risks are recorded, mitigated and monitored at the institution by way of internal controls embedded in the systematic risk analysis and monitoring system (appropriate risk and control environment) (margin no. 14, FINMA Circ. 17/1). |  |  |  |
| Assess with the minutes of the BoD whether it oversees effectively the work of the Executive Board (margin no. 14, FINMA Circ. 17/1). |  |  |  |
| Assess whether appropriate procedures are in place in order that the employees of all ranks are familiar with and understand their duties and responsibilities. |  |  |  |
| Assess if the BoD takes decisions on major changes to the structure and to the investments (margin no. 15, FINMA Circ. 17/1).  |  |  |  |
| Assess whether the BoD regularly meets with the Executive Board to discuss its assessment of the appropriateness and effectiveness of internal controls. | Inspect the minutes of the meetings held with the Executive Board and/or of the meetings of the BoD or its committees and assess the adequacy of the discussions regarding the assessment of the appropriateness and effectiveness of internal controls and assess the respective decisions taken. |  |  |
| Assess whether the Executive Board implements the instructions of the BoD with regard to the operational business activities, in compliance with the business strategy, and to the setting up, maintaining and regular supervision of internal controls (margin nos. 47 to 50, FINMA Circ. 17/1). The Executive Board is responsible for:* managing day-to-day business, operational revenue and risk management and representing the institution towards third parties in operational matters;
* submitting applications regarding transactions for which the BoD is responsible or for which its approval is required, and issuing rules for regulating business operations;
* developing and maintaining effective internal processes, an appropriate management information system and an internal control system (ICS) as well as a suitable technological infrastructure.
 | Inspect the documentation related to the examination of the appropriateness of the internal control system and assess the adequacy of the discussion and decisions taken. |  |  |
| Assess the overall adequacy of the internal control system (design) with regard to:* documentation principles
* institution’s size/complexity
* consideration of 4-eye-principle
* reporting (results, issues)
* authorisation process.
 | Take a sample of the ICS documentation and assess whether the institution’s guidelines related to documentation, consideration of 4-eye-principle, reporting and authorisation have been complied with including the execution of controls defined (operating effectiveness).  |  |  |
| Understand the update process for ICS documentation and assess whether the process is adequate to identify changes and to keep the internal controls system up to date (design). | Take a sample of the ICS documentation and assess whether the institution’s guidelines related to the update and authorisation processes have been complied with including the execution of controls defined (operating effectiveness). |  |  |

**Work programme – Internal organisation and internal control system – Measures to adequately limit conflicts of interest**

| **No.** | **Topic:** | **Procedures for audit depth “critical assessment”:** | **Additional procedures for audit depth “audit”:** | **Procedures performed/findings** | **WP ref.:** |
| --- | --- | --- | --- | --- | --- |
|  |
|  | **Measures to adequately limit conflicts of interest** | *Assess whether the internal organisation has been adequately designed for an adequate limitation of conflict of interest considering the size, business and organisational complexity of the institution, specifically:* | Obtain documentation on identified material deficiencies (e.g. fraud caused by override of controls) and assess how the institution dealt with it (e.g. reporting, remediation etc.). |  |  |
| Assess whether the institution’s internal policies and guidelines include guidance on avoiding and handling conflicts of interest. |  |  |  |
| Assess whether the BoD ensures that the handling of conflicts of interest is regulated (margin no. 29, FINMA Circ. 17/1). If conflicts of interest cannot be avoided, assess if the institution has taken measures to properly address them. | Inquire if any conflicts of interest could not be avoided and assess if the measures taken are/were appropriate for a sample. |  |  |
| Assess whether the BoD ensures that any pressure exerted on employees of all ranks to meet targets does not result in shortcuts with respect to control mechanisms. The BoD ensures that the compensation system does not contain incentives that could lead to conflicts of interest or to disregard control mechanisms (margin nos. 13 & 63 FINMA Circ. 17/1). | Inspect respective guidelines set by the BoD and assess whether they are complied with. |  |  |
| Assess whether the Executive Board ensures appropriate segregation of functions and avoids the allocation of conflicting areas of responsibility. In cases where the segregation of functions principle cannot be fully implemented due to the size of the institution, the Executive Board emphasises the importance of higher management responsibility for the business line in question.  |  |  |  |
| Assess the institution’s procedures to detect potential conflicts of interest (including e.g. whistleblower policy and procedures). | Inquire if any conflicts of interest were reported and assess their handling for a sample. |  |  |
|  | **Remuneration schemes[[3]](#footnote-4)** | *Assess whether the internal organisation has been adequately designed in terms of remuneration schemes considering the size, business and organisational complexity of the institution, specifically:* |  |  |  |
| Understand and document the institution’s remuneration schemes. |  |  |  |
| Assess whether the institution considered the guidelines in FINMA Circ. 10/1 related to conflicts of interest. | Select an appropriate sample of key persons and assess whether the remuneration schemes (e.g. salary, bonuses and fees) are adequately designed to avoid incentives that could lead to a conflict of interest or to the override of controls (in particular margin no. 63 FINMA Circ. 17/1). |  |  |

**Work programme – Internal organisation and internal control system – Internal reporting and corporate governance disclosures**

| **No.** | **Topic:** | **Procedures for audit depth “critical assessment”:** | **Additional procedures for audit depth “audit”:** | **Procedures performed/findings** | **WP ref.:** |
| --- | --- | --- | --- | --- | --- |
|  |
|  | **Internal reporting** **Content** | *Assess whether an adequate internal reporting framework considering the size, business and organisational complexity of the institution has been designed, specifically:* |  |  |  |
| Understand and document the design of the reporting framework related to internal organisation and ICS as a whole including reporting lines, content and periodicity of reporting. |  |  |  |
| Inspect the reporting package to the BoD and to the Executive Board. Assess whether it contains all relevant aspects considering the size, business and organisational complexity of the institution on a sample basis. | Inspect reports to BoD and Executive Board on a sample basis and test the procedures and controls implemented in order to make sure the reports are accurate, complete and reliable. |  |  |
|  | **Internal reporting** **Recipients and periodicity** | *Assess whether the recipients and periodicity of the internal reporting on internal organisation and ICS have been adequately designed considering the size, business and organisational complexity of the institution, specifically:* |  |  |  |
| Assess whether internal reporting in connection with internal organisation and ICS is addressed to the adequate recipients with useful periodicities considering the size, business and organisational complexity. | Assess in detail whether reporting lines are appropriate considering the size, business and organisational complexity. |  |  |
|  | **Internal reporting** **Escalation process** | *Assess whether the internal escalation processes have been adequately designed considering the size, business and organisational complexity of the institution, specifically:* |  |  |  |
| Understand the implemented escalation processes to report control failures and further issues regarding the internal control system timely and to the adequate recipients. | Select a sample of major control failures and inspect whether they were reported to the adequate recipients and whether the institution has taken adequate measures. |  |  |
|  | **Corporate governance disclosures****(margin nos. 14.1, 20, 41.1, appendix 4, FINMA Circ. 16/1)[[4]](#footnote-5)** | Assess whether disclosure obligations in consideration of the size, business and organisational complexity of the institution have been adequately fulfilled. |  |  |  |
| Review of corporate governance disclosures. Assess whether the information required under margin nos. 1-6 appendix 4 of FINMA Circ. 16/1 has been disclosed, adequately explained and material changes have been updated on the website within three months. | Assess whether the information required under margin nos. 1-6 appendix 4 of FINMA Circ. 16/1 has been disclosed faithfully and in full. |  |  |
| **\*** Assess whether the information required under margin nos. 7-13 appendix 4 of FINMA Circ. 16/1 has been disclosed, adequately explained and material changes have been updated on the website within three months. | **\*** Assess whether the information required under margin nos. 7-13 appendix 4 of FINMA Circ. 16/1 has been disclosed faithfully and in full. |  |  |

**Work programme – Internal organisation and internal control system – Risk policy and principles of institution-wide risk management**

| **No.** | **Topic:** | **Procedures for audit depth “critical assessment”:** | **Additional procedures for audit depth “audit”:** | **Procedures performed/findings** | **WP ref.:** |
| --- | --- | --- | --- | --- | --- |
|  |
|  | **Risk policy and principles of institution-wide risk management**Art. 12 para. 2 BO and Art. 68 FinIO | Assess whether an adequate risk policy and principles have been established for the institution-wide risk management of the institution, considering the size, business and organisational complexity of the institution, specifically: |  |  |  |
| Assess whether the risk policy and the principles for institution-wide risk management have been developed by the Executive Board and approved by the BoD (margin no. 52, FINMA Circ. 17/1). |  |  |  |
|  |  | Assess if the risk policy and the principles for institution-wide risk management include risk tolerance and the risk limits based on it in all key risk categories (margin no. 53, FINMA Circ. 17/1). | Inspect in detail the risk policy and the principles for institution-wide risk management and review whether the risk tolerance and the risk limits based on it are adequately regulated in all key risk categories and have been effectively applied in operational risk monitoring. |  |  |
|  |  | Assess whether the responsibility and the procedure for authorising high-risk transactions have been defined by a directive or in internal policies (Art. 12 Banking Ordinance). |  |  |  |
|  |  | **\*** Assess whether the aspects to be considered in accordance with margin nos. 54-59 FINMA Circ. 17/1have been taken into account in the risk policy and in the principlesfor institution-wide risk management. Additional requirements for systemically important institutions: compliance with supplementary provisions, notably relating to data architecture and IT infrastructure (margin no. 59 FINMA Circ. 17/1, final clause). | **\*** Inspect in detail the risk policy and the principles for institution-wide risk management assessment and check whether the relevant aspects, considering the size and its business and organisational complexity, have been taken into account and if they are effectively applied in operational risk monitoring. |  |  |

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

1. Margin nos. 33 and 34 FINMA Circ. 13/3. [↑](#footnote-ref-2)
2. Basic audit of Category 1 institutions [↑](#footnote-ref-3)
3. The audit points for remuneration systems are only applicable to institutions concerned by margin no. 6 of FINMA Circ. 10/1. [↑](#footnote-ref-4)
4. Not applicable to the institutions falling within the definition under Art. 47a to 47e CAO, which simply need to disclose the key metrics applicable to them. See margin no. 8.1 FINMA Circ. 16/1 [↑](#footnote-ref-5)