**Audit points for centralised risk control and risk mitigation functions**

**Overview**

|  |  |
| --- | --- |
| **Subject:** | **Centralised risk control and risk mitigation functions (risk control function, compliance function)** |
| **Audit depth:** | [Audit/critical assessment][[1]](#footnote-2) |
| **Regulations**  (non-exhaustive list) | Art. 3 para. 2 let. a Banking Act (BA)  Art. 9 Financial Institutions Act (FinIA)  Art. 12 Banking Ordinance (BO)  Art. 12 and 66-68 Financial Institutions Ordinance (FinIO)  FINMA Circular 2017/1 “Corporate governance - banks” (FINMA Circ. 17/1, margin nos. 62-81 & 98-99) |
| **Sign-offs:** | |  |  |  |  | | --- | --- | --- | --- | | **Sign-offs:** | **Name:** | **Function:** | **Date:** | | Prepared by: | [Name] | [Assistant / Senior / Manager / Senior Manager / Partner] | [DD MMMM YYYY] | | Reviewer: | [Name] | [Senior / Manager / Senior Manager  / Partner] | [DD MMMM YYYY] | |

**This is the standard work programme that is to be implemented for every audit in this 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 work 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:** |
| --- | --- |
| Overall conclusion | |  |  | | --- | --- | | **Confirmation in audit report:** | **Conclusion:** | | Confirmation that the technical and personnel resources of the compliance function were adequate and it actually assumed responsibility. | ***Yes*** *(Audit/critical assessment) /* ***No*** | | Confirmation that the technical and personnel resources of the risk control function were adequate and it actually assumed responsibility. | ***Yes*** *(Audit/critical assessment) /* ***No*** | | Confirmation that the organisational set-up of the functions and the compensation system did not lead to a conflict of interest. | ***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 relied on by the audit firm (including audit firm’s own assessment). | [Description] |

**Work programme – Compliance function**

| **No.** | | **Topic:** | **Procedures for audit depth  “critical assessment”:** | **Additional procedures for audit depth “audit”:** | **Procedures performed/findings** | **WP ref.:** |
| --- | --- | --- | --- | --- | --- | --- |
| *“Confirmation that the technical and personnel resources of the compliance function were adequate and it actually assumed responsibility”.*  *„Bestätigung, dass die technischen und personellen Ressourcen bei der Funktion Compliance ausreichend waren und dass diese ihre Verantwortung effektiv wahrgenommen hat“.*  *„Confirmation que les ressources techniques et personnelles de la fonction de compliance étaient suffisantes et qu’elle a assumé effectivement ses responsabilités“.* | | | | | | |
|  | | **Personnel resources** | *Assess whether the personnel resources of the compliance function are adequate considering the size, business and organisational complexity and the compliance risk of the institution (margin no. 64 FINMA Circ. 17/1), specifically:* |  |  |  |
|  | | Obtain a basic understanding of the institution’s compliance function, the number of its employees and the allocated tasks. |  |  |  |
|  | | Obtain for example the CVs and job descriptions of key persons/employees of the compliance function and assess their know-how. |  |  |  |
|  | | **Technical resources** | *Assess whether the technical resources of the compliance function are adequate considering the size, business and organisational complexity and the compliance risk of the institution (margin no. 64 FINMA Circ 17/1), specifically:* |  |  |  |
|  | | Assess the adequacy of technical resources, e.g. with the help of a list of information technology applications and other working tools used by the compliance function, including the name of the system, a description of the purpose and the implementation date. |  |  |  |
|  | | **Assumption of responsibility** | *Assess whether the compliance function assumes its responsibility in relation to the size, business and the organisational complexity and compliance risk of the institution (margin nos. 77-81 FINMA Circ. 17/1), specifically:* |  |  |  |
|  | | Assess whether the institution's internal directives for the compliance function comply with FINMA Circ. 17/1 and are appropriate given recent and planned changes to the institution’s overall circumstances, controls and organisation. |  |  |  |
|  | | Assess whether the compliance function performs – at least annually – an assessment of the compliance risk of the business activities and based thereon develops a risk-based activity plan, which is to be approved by the Executive Board and made available to Internal Audit (margin no. 78 FINMA Circ. 17/1). | Inspect the risk-based activity plan and assess its adequacy/comprehensiveness. |  |  |
|  | | Assess whether the compliance function informs the Board of Directors – at least annually – about the assessment of the compliance risk and the activities of the compliance function (margin no. 80 FINMA Circ. 17/1). | Inspect the annual reporting to the Board of Directors (with copy for Internal Audit and the audit firm) and assess its adequacy/comprehensiveness. |  |  |
|  | | Obtain, inspect and assess evidence that the compliance function effectively assumes its further responsibilities (timely reporting to the corresponding functions i) on material changes in the assessment of compliance risks and ii) serious compliance breaches) (margin nos. 79 and 81 FINMA Circ. 17/1). |  |  |  |
|  | | Identify and document internal controls performed by the compliance function and assess their design effectiveness/comprehensiveness. | Develop and execute tests of controls to confirm the operating effectiveness of the internal controls performed by the compliance function. |  |  |
| *“Confirmation that the organisational set-up of the risk control function and the compensation system did not lead to a conflict of interest”.*  *„Bestätigung, dass die organisatorische Anordnung der Funktion Compliance und das Entschädigungssystem* *keine Zielkonflikte herbeiführten“.*  *“Confirmation que le positionnement de la fonction de compliance dans l’organisation et le mode de rémunération n’ont pas généré de conflits d’objectifs”.* | | | | | | |
|  | **Organisational set-up and prevention of conflicts of interest** | | *Assess whether the organisational set-up of the compliance function is adequate considering the size, business and organisational complexity of the institution and does not lead to a conflict of interest and if it is independent from the revenue-generating units. (margin nos. 62-68 FINMA Circ. 17/1), specifically:* |  |  |  |
|  | Assess whether the organisational set-up of the compliance function complies with FINMA Circ. 17/1 – especially regarding prevention of conflicts of interest and independence from revenue-generating units – and is appropriate given recent and planned changes to the institution’s overall circumstances, controls and organisation (margin nos. 60-64 FINMA Circ. 17/1). |  |  |  |
|  | Identify what member(s) of the Executive Board is/are responsible for the compliance function and assess whether the unlimited information, access and inspection rights as independent control body are ensured (margin nos. 64 and 65 FINMA Circ. 17/1). |  |  |  |
|  | Assess whether the remuneration scheme for employees of the compliance function (e.g. salary, bonuses, fees) does not set any incentives which could lead to a conflict of interest (margin no. 63 FINMA Circ. 17/1). | Execute substantive procedures to confirm that the remuneration of employees of the compliance function does not depend on the results of individual products or transactions. |  |  |
|  | Assess if the compliance function (independent control body) has direct access to the Board of Directors. |  |  |  |
|  | **\*** Assess if a separate compliance function exists as an independent control body (margin no. 67 FINMA Circ. 17/1). |  |  |  |

**Work programme – Risk control function**

| **No.** | **Topic:** | **Procedures for audit depth  “critical assessment”:** | **Additional procedures for audit depth “audit”:** | **Procedures performed/findings** | **WP ref.:** |
| --- | --- | --- | --- | --- | --- |
| *“Confirmation that the technical and personnel resources of the risk control function were adequate and it actually assumed responsibility”.*  *„Bestätigung, dass die technischen und personellen Ressourcen bei der Funktion Risikokontrolle ausreichend waren und dass diese ihre Verantwortung effektiv wahrgenommen hat“.*  *„Confirmation que les ressources techniques et personnelles de la fonction de contrôle des risques étaient suffisantes et qu’elle a assumé effectivement ses responsabilités“.* | | | | | |
|  | **Personnel resources** | *Assess whether the personnel resources of the risk control function are adequate considering the size, business and organisational complexity and the risk profile of the institution, specifically:* |  |  |  |
|  | Obtain a basic understanding of the institution’s risk control function, the number of its employees and the allocated tasks. |  |  |  |
|  | Obtain for example the CVs and job descriptions of key persons/employees of the risk control function and assess their know-how. |  |  |  |
|  | **Technical resources** | *Assess whether the technical resources of the risk control function are adequate considering the size, business and organisational complexity and the risk profile of the institution (margin no. 64 FINMA Circ. 17/1), specifically:* |  |  |  |
|  | Assess the adequacy of technical resources, e.g. with the help of a list of information technology applications and other working tools used by the risk control function, including the name of the system, a description of the purpose and the implementation date. |  |  |  |
|  | **Assumption of responsibility** | *Assess whether the risk control assumes its responsibility in relation to the size, business and the organisational complexity and compliance risk of the institution (margin nos. 69-76 FINMA Circ. 17/1), specifically:* |  |  |  |
|  | Assess whether the institution's internal directives for the risk control function comply with FINMA Circ 17/1 and are appropriate given recent and planned changes to the institution’s overall circumstances, controls and organisation. |  |  |  |
|  | Obtain, inspect and assess evidence that the risk control function ensures comprehensive and systematic monitoring and reporting of individual and aggregated risk positions (incl. conducting stress tests and scenario analyses),[[2]](#footnote-3) appropriate implementation of provisions relating to risk data aggregation and reporting (institutions in supervisory categories 1 to 3) as well as monitors the institution's risk profile (risk tolerance and risk limits) (margin nos. 69-71 FINMA Circ. 17/1). |  |  |  |
|  | Assess whether the risk control function effectively assumes its responsibilities with respect to design and application of concepts and methodologies for monitoring and measurement of risks (margin no. 72 FINMA Circ. 17/1). |  |  |  |
|  | Assess if risk control is to be appropriately consulted during the development of new or expanded product categories, services or business/market areas and for major or complex transactions (margin no. 73 FINMA Circ. 17/1). |  |  |  |
|  | Assess if risk control is actively involved in the process of defining risk limits and ensures that risks limits are consistent with the defined risk tolerance and reconciled to the results of the stress tests and that they are defined in such a way as to constitute an operationally effective management tool for the Executive Board (margin no. 74 FINMA Circ. 17/1). |  |  |  |
|  | Assess whether the risk control function submits to the Executive Board at least semi-annually a written report on the institution's risk profile and its activities (margin no. 75 FINMA Circ. 17/1). | Inspect the semi-annual risk report for the Executive Board and the annual risk report (including activities of the risk control functions) for the Board of Directors (with copy to Internal Audit and the audit firm) and assess their adequacy/comprehensiveness. |  |  |
|  | Assess whether the risk control function informs the Board of Directors at least annually on the institution's risk profile and its activities (margin no. 75 FINMA Circ. 17/1). |  |  |  |
|  | Obtain and assess the other evidence that risk control function effectively assumes its other tasks and responsibilities (prompt information in the event of special developments) (margin no. 76 FINMA Circ. 17/1). |  |  |  |
|  | Identify and document internal controls performed by the Function and assess their design effectiveness/ comprehensiveness. | Execute tests of controls to confirm the operating effectiveness of the internal controls performed by the risk control function. |  |  |
| “Confirmation that the organisational set-up of the risk control function and the compensation system did not lead to a conflict of interest”.  *„Bestätigung, dass die organisatorische Anordnung der Funktion Risikokontrolle und das Entschädigungssystem keine Zielkonflikte herbeiführten“.*  *“Confirmation que le positionnement de la fonction de contrôle des risques dans l’organisation et le mode de rémunération n’ont pas généré de conflits d’objectifs”.* | | | | | |
|  | **Organisational set-up and prevention of conflicts of interest** | *Assess whether the organisational set-up of the risk control function is adequate considering the size, business and organisational complexity of the institution and does not lead to a conflict of interest and if it is independent from the revenue-generating units (margin nos. 62–68 FINMA Circ. 17/1), specifically:* |  |  |  |
|  | Assess whether the organisational set-up of the risk control function complies with FINMA Circ. 17/1 – especially regarding prevention of conflict of interest and independence from revenue-generating units – and is appropriate given recent and planned changes to the institution’s overall circumstances, controls and organisation (margin nos. 60-64 FINMA Circ. 17/1). |  |  |  |
|  | Identify what member(s) of Executive Board is/are responsible for the risk control function and assess whether the unlimited information, access and inspection rights as independent control body are ensured (margin nos. 64 and 65 FINMA Circ. 17/1). |  |  |  |
|  | Assess whether the remuneration scheme for employees of the risk control function (e.g. salary, bonuses, fees) does not set any incentives which could lead to a conflict of interest. | Develop and execute substantive procedures to confirm that the remuneration of employees of the risk control function does not depend on the results of individual products or transactions. |  |  |
|  | Assess if the risk control function (independent control body) has direct access to the Board of Directors (margin. no. 66 FINMA Circ. 17/1). |  |  |  |
|  | **\*** Assess if a separate risk control function exists as an independent control body and if a chief risk officer has been appointed to head it up (margin no. 67 FINMA Circ. 17/1). |  |  |  |
|  | Applicable only to systemically important institutions:  Assess if a chief risk officer, who is member of the Executive Board, has been appointed (margin no. 68 FINMA Circ. 17/1). |  |  |  |

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

1. Margin nos. 33 and 34 FINMA Circ. 13/3. [↑](#footnote-ref-2)
2. Banks in the small banks regime must at the very least conduct scenario analyses. [↑](#footnote-ref-3)