**Audit points for other risks in connection with compliance issues**

**Overview**

|  |  |
| --- | --- |
| **Subject** | **Business risks – risk management / Other risks in connection with compliance issues** |
| **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)  Arts. 12 and 66-68 Financial Institutions Ordinance (FinIO)  Art. 12 para. 2bis BO in conjunction with Arts. 56 and 61a, FINMA Banking Insolvency Ordinance (BIO-FINMA)  FINMA Circular 2008/21 "Operational Risks – banks" (FINMA Circ. 08/21 / margin nos. 136.2-136.5)  FINMA Circular 2017/6 "Direct Transmission" (FINMA Circ. 17/6) |
| **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 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 methods/processes used to identify, measure, manage and monitor the other risks in connection with compliance issues were adequate and, in the case of the audit depth “audit”, were applied effectively. | ***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 work performed by Internal Audit relied on by the audit firm (including audit firm’s own assessment) | [Description] |

**Work programme – Other risks in connection with compliance issues** – Change management

| **No.** | **Topic** | **Procedures for audit depth  “critical assessment”:** | **Additional procedures for audit depth “audit”:** | **Procedures performed/findings** | **WP ref.:** |
| --- | --- | --- | --- | --- | --- |
| *Confirmation that methods/processes for identification, measurement, management and monitoring of other risks in connection with compliance issues were adequate and, in case of the audit depth “audit”, were applied effectively.*  *Bestätigung, dass die Methoden / Prozesse zur Identifikation, Messung, Bewirtschaftung und Überwachung von anderen Risiken im Zusammenhang mit Compliance-Fragen angemessen waren und im Falle der Prüftiefe „Prüfung“ effektiv angewendet wurden.*  *Confirmation que les méthodes / processus relatifs à l’identification, la mesure, la gestion et la surveillance des autres risques en lien avec les questions de compliance ont été appropriés et en cas d’étendue d’audit « audit » ont été effectivement appliqués.* | | | | | |
|  | **Legal and regulatory change management[[2]](#footnote-3)** | *Assess the adequacy of the methods/processes for the identification, measurement, management and monitoring of legal and regulatory developments as well as the changes to the business considering the size, business and organisational complexity and the compliance risk of the institution, specifically:* |  |  |  |
| Assess the adequacy of the institution processes for the:   * preparation, quality control and approval of a periodic overview of relevant legal and regulatory changes; * performance of a business impact analysis on the relevant legal and regulatory changes; * timely planning and initiation of action and measures to respond to the changes. | Verify the adequacy/comprehensiveness of the institution’s assessment of relevant legal and regulatory changes, and assess:   * the bank’s assessment of the resulting business impact; * the initiation of measures to respond to the change based on our own understanding of these changes. |  |  |
| Assess whether adequate expertise and know-how has been used by the institution in order to identify the legal and regulatory changes, including assessment of the way to obtain information about regulatory changes. |  |  |  |
| Assess the adequacy of reporting to and monitoring by the Executive Board and Board of Directors on legal and regulatory developments and the consequential changes and measures for the business. |  |  |  |
|  | **New activities, products and services** | *Assess the adequacy of the methods/processes for the identification, measurement, management and monitoring of impacts from introducing or changing activities, products and services considering the size, business and organisational complexity and the compliance risk of the institution, specifically:* |  |  |  |
| Assess the adequacy and comprehensiveness of the institution’s processes and controls to manage compliance risks regarding the introduction of new activities, products or services and to manage changes in activities, products or services. |  |  |  |
|  | **Risk policy** | *Assess whether risk policy, internal regulations, guidelines, manuals and job descriptions adequately define responsibilities, approval powers, reporting and escalation lines for the management of legal and regulatory change as well as changes in activities, products and services considering the size, business and organisational complexity and the compliance risk of the institution, specifically:* |  |  |  |
| Assess whether internal rules adequately assign responsibilities for the:   * continuous monitoring, identification and internal reporting to the Executive Board of legal and regulatory changes; * decision whether a business impact analysis is required for any particular legal or regulatory change; * approval of the business impact analysis and subsequent action/project plans for legal and regulatory changes. |  |  |  |
| Assess whether appropriate approval powers and procedures have been defined for the introduction of new activities, products and services and subsequent changes thereto. |  |  |  |
|  | **Compliance with existing risk policy** | *Assess whether an adequate process is in place to ensure that risk policy relating to the management of legal and regulatory changes and relating to new activities, products and services have been effectively applied and complied with, specifically:* | Select a sample of at least one major legal/regulatory change or of at least one significant new/changed activity, product or service and perform substantive testing of compliance with internal rules and limits. |  |  |
| Identify and document the internal controls relating to the management of legal and regulatory changes and to new/changed activities, products and services and assess their design and comprehensiveness. | Execute tests of controls to confirm the operating effectiveness of the internal controls performed for the management of legal and regulatory changes and to new/changed activities, products and services. |  |  |
|  | **Applicability of a stay on contracts subject to foreign law / a foreign place of jurisdiction** | *Assess if there is an adequate process to ensure compliance with Art. 12 para. 2bis BO in conjunction with Art. 56 and 61a of BIO-FINMA* |  |  |  |
|  |  | Examine the existence and appropriateness of internal instructions or directives ensuring that new contracts or amendments to existing contracts which are subject to foreign law or a foreign place of jurisdiction are only entered into if the counterparty recognises a stay on the termination of agreements as per Art. 30a BA, where these agreements are in the scope of application of Art. 12 par. 2bis BO in accordance with Art. 56 BIO-FINMA. | Select a random sampling of contracts governed by Art. 12 para. 2bis BO in accordance with Art. 56 BIO-FINMA and subject to foreign law or a foreign place of jurisdiction, and verify that the stay within the meaning of Art. 30a BA has been effectively agreed. |  |  |

**Work programme – Other risks in connection with compliance issues** – Risks from cross-border services

| **No.** | **Topic** | **Procedures for audit depth  “critical assessment”:** | **Additional procedures for audit depth “audit”:** | **Procedures performed/findings** | **WP ref.:** |
| --- | --- | --- | --- | --- | --- |
| *Confirmation that methods/processes for identification, measurement, management and monitoring of other risks in connection with compliance issues were adequate and, in case of the audit depth “audit”, were applied effectively.*  *Bestätigung, dass die Methoden / Prozesse zur Identifikation, Messung, Bewirtschaftung und Überwachung von anderen Risiken im Zusammenhang mit Compliance-Fragen angemessen waren und im Falle der Prüftiefe „Prüfung“ effektiv angewendet wurden.*  *Confirmation que les méthodes / processus relatifs à l’identification, la mesure, la gestion et la surveillance des autres risques en lien avec les questions de compliance ont été appropriés et en cas d’étendue d’audit « audit » ont été effectivement appliqués.* | | | | | |
|  | **Risk policy** | *Assess whether risk policy, internal regulations, guidelines, manuals and job descriptions adequately define responsibilities, approval powers, reporting and escalation lines for risks from cross-border services considering the size, business and organisational complexity and the compliance risk of the institution, specifically:* |  |  |  |
| Assess whether internal rules adequately define the business strategy and service model (including procedures for targeting, relationship management, doing business and communication) for target countries, excluded countries, non-target countries (those which are neither target nor excluded countries). |  |  |  |
| Assess whether the documented cross-border strategy is sufficiently detailed, clear and transparent to ensure that the governing bodies can take informed decisions on risk appetite and tolerance and whether it is adequate with regard to the institution’s business and organisational complexity (notably the selected target markets, the institution’s assessment of the compliance of its service models for the target markets and the obtained licences and approvals). |  |  |  |
| Assess whether internal rules adequately define target countries, excluded countries, non-target countries (those which are neither target nor excluded countries) consistently with the business plan and the effective commercial activities. |  |  |  |
| Assess whether internal rules adequately define roles and responsibilities, e.g. for:   * approval of cross-border strategy; * performance of sufficiently detailed and frequent country risk analyses; * approval of classification per specific country and frequency of new examinations and re-approvals; * definition, maintenance, update and approval of service models (incl. targeting, relationship management, doing business and communication) per target country and for all other types of countries; * approval, implementation and control of risk-based training programme; * controls, approvals and documentation before new customers are accepted; * periodic due diligence and (re-)approval of external asset managers and other intermediaries; * approval powers for travel plans to foreign countries; * timely preparation of travel reports and approval thereof; * internal ad-hoc reporting duties in case of observed increase of cross-border risks; * reporting duties if persons are contacted by foreign authorities. |  |  |  |
| Review the minutes of Board of Directors' meetings to assess whether the cross-border strategy, risk appetite and tolerance was discussed and approved by the Board of Directors. |  |  |  |
|  | **Country analyses/country manuals** | *Assess adequacy of methods/processes for identification, measurement, management and monitoring of risks from cross-border services considering the size, business and organisational complexity and the institution's compliance risk, notably* |  |  |  |
|  |  | Assess whether the target countries defined in the institution’s internal regulations are consistent with the existing business of the bank, e.g. cross-border service model, type of clients, products, services or intermediaries. |  |  |  |
| Assess whether country-specific analyses were performed for all target market countries with consideration of all arising material risk types (e.g. legal risk, civil law risk, regulatory risk, etc.) by experts who are familiar with the territories. | Select a sample of country manuals and test whether the high-level business strategy and service models have been consistently defined in line with the results of the country-risk analyses performed. |  |  |
|  | **Organisation** | Assess the adequacy of the organisation model for cross-border business (e.g. dedicated desks per country/groups of similar countries, dedicated unit for intermediaries, organisation model for non-target countries, segregation of duties, market purity (maximum number of target countries a client advisor can acquire and service clients from) and the support by internal or external experts. |  |  |  |
|  | **Asset managers and intermediaries** | Assess the adequacy of policies, processes and documentation maintained for external asset managers and other intermediaries, for example:   * + - * policy for the management of external asset managers;       * process to select, instruct and monitor external asset managers in general and regarding adherence to the institution’s cross-border strategy/rules;       * documented analysis of business activities, financial conditions, risk policy, organisation and regulatory status of intermediaries;       * written contract with intermediaries incl. scope of permitted / prohibited services and products by country, applicable rules, remuneration. | Verify acceptance, re-approval and monitoring of the collaboration with external asset managers and other intermediaries (incl. clients managed by them) on a sample basis.  Test a sample of external asset manager client relationships for conformity with the institution’s internal policies and directives including adherence to the institution’s cross-border strategy/rules. |  |  |
|  | **Monitoring** | Assess whether periodic adequate management reports are provided to the Executive Board and to the Board of Directors (e.g. top risks, customer volumes by market, volumes by intermediaries, progress made against strategic plans, maintenance of country manuals, training statistics). |  |  |  |
|  | **Training and education** | Assess the adequacy of cross-border training procedures (extent and scope, frequency, instructors, up-to-dateness, internal controls) for employees exposed to cross-border activities of the bank. | Test on a sample basis that the employees have effectively attended the training sessions defined mandatory by the financial institution and passed respectively tests, if applicable. |  |  |
|  | **Compensation models (margin 136.3 FINMA Circ. 08/21):** | *Assess the adequacy of the compensation model with regard to incentives for client advisors and other personnel for client acquisition and retention in connection with cross-border risks, specifically:* |  |  |  |
| Assess through inquiry and review of relevant documents the adequacy of the institution’s:   * compensation model regarding cross-border risks, notably in preventing wrongful incentives for client acquisition and retention, penalties for violations and promotion of good compliance and whether it complies with the general framework of the institution’s compensation policy. | Test on a sample basis and with focus on cross-border aspects that the compensation models have been adhered to and no objectives were set that contradict the defined internal policies. |  |  |
|  | **Compliance with existing risk policy** | *Assess whether risk policy relating to risks from cross-border services has been effectively applied and complied with, notably* | Assess whether customer relationships which are no longer desired are terminated in line with the institution’s strategy, policy and/or directives. |  |  |
| Identify and document the internal controls relating to:   * acceptance, management and monitoring of customers; * monitoring of the conduct of relationship managers (e.g. regarding travel reports, contact memo based on visit at the point of sale, education, etc.); * acceptance and periodic review of external asset managers and other intermediaries;   and assess the adequacy of their design effectiveness/comprehensiveness with regard to the size and complexity of the cross-border activities of the institution. | Execute tests of controls to confirm the operating effectiveness of the internal controls performed and perform substantive testing relating to:   * acceptance, management and monitoring of customers; * monitoring of the conduct of relationship managers (e.g. regarding travel reports, contact memo based on visit at the point of sale, education, etc.); * acceptance and periodic review (resubmission) of external asset managers and other intermediaries. |  |  |

|  |
| --- |
|  |

**Work programme – Other risks in connection with compliance issues** - Serious violations of compliance

| **No.** | **Topic:** | **Procedures for audit depth  “critical assessment”:** | **Additional procedures for audit depth “audit”:** | **Procedures performed/findings** | **WP ref.:** |
| --- | --- | --- | --- | --- | --- |
| *Confirmation that methods/processes for identification, measurement, management and monitoring of other risks in connection with compliance issues were adequate and, in case of the audit depth “audit”, were applied effectively.*  *Bestätigung, dass die Methoden / Prozesse zur Identifikation, Messung, Bewirtschaftung und Überwachung von anderen Risiken im Zusammenhang mit Compliance-Fragen angemessen waren und im Falle der Prüftiefe „Prüfung“ effektiv angewendet wurden.*  *Confirmation que les méthodes / processus relatifs à l’identification, la mesure, la gestion et la surveillance des autres risques en lien avec les questions de compliance ont été appropriés et en cas d’étendue d’audit « audit » ont été effectivement appliqués.* | | | | | |
|  | **Methods/processes for identification, measurement, management and monitoring of risks** | *Assess adequacy of methods/processes for identification, measurement, management and monitoring of serious violations of compliance considering the size, business and organisational complexity and the compliance risk of the institution, specifically:* |  |  |  |
| **\*** Assess the adequacy of the procedures of the compliance function to:   * identify serious violations of compliance with applicable laws and regulations; * receive, assess, document and evaluate allegations and suspicions. |  |  |  |
| Assess the appropriateness of the processes and controls with respect to dealing with identified compliance violations and how the next steps are defined or initiated including escalation procedures. |  |  |  |
| Assess the appropriateness of the defined procedures for the interaction with Board of Directors, Audit Committee and Internal Audit regarding suspected and incurred serious violations of compliance and subsequent measures taken. |  |  |  |
|  | **Risk policy** | *Assess whether risk policy, internal regulations, guidelines, manuals and job descriptions adequately define responsibilities, approval powers, reporting and escalation lines as well as sanctions for serious violations of compliance considering the size, business and organisational complexity and the compliance risk of the institution, specifically:* |  |  |  |
| Assess whether there is an adequate framework in place to instruct all persons of the institution how to deal with violations of compliance, including the designation of a point of contact for serious violations of compliance (e.g. compliance function or whistleblowing helpline). |  |  |  |
| **\*** Assess whether responsibilities have been appropriately assigned to compliance function to:   * notice and investigate serious violations of compliance; * assist the executive board in the selection of instructions and measures; * inform Internal Audit about serious violations of compliance and significant developments regarding compliance risks; * escalate any violation to appropriate governing bodies or committees, if the executive management refuses any treatment or sanction. |  |  |  |
| Assess reasonableness of assignment of approval powers for instructions and measures relating to serious violations of compliance, incl. approval of investigator and post investigation measures (e.g. to the Executive Board, respectively to Board of Directors or one of its committees). |  |  |  |
|  |  | Assess the adequacy of the procedures to consider compliance objectives in performance appraisals. |  |  |  |
|  |  | **\*** Assess the appropriateness of the general sanctioning framework of the institution with regard to compliance with prudential rules and regulations. |  |  |  |
|  | **Compliance with existing risk policy** | *Assess whether risk policy relating to serious violations of compliance has been effectively applied and complied with, specifically:* |  |  |  |
| Obtain an overview of serious violations of compliance during the audited period. Enquire and assess how management ensured compliance with internal policies, directives and limits. | Perform substantive testing on a sample basis whether internal policies, directives and limits have been complied with for the treatment of serious violations of compliance. |  |  |

|  |
| --- |
|  |

**Work programme – Other risks in connection with compliance issues** – Direct transmission

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **No.** | **Topic:** | **Procedures for audit depth  “critical assessment”:** | **Additional procedures for audit depth “audit”:** | **Procedures performed/findings** | **WP ref.:** |
| *Confirmation that methods/processes for identification, measurement, management and monitoring of other risks in connection with compliance issues were adequate and, in case of the audit depth “audit”, were applied effectively.*  *Bestätigung, dass die Methoden / Prozesse zur Identifikation, Messung, Bewirtschaftung und Überwachung von anderen Risiken im Zusammenhang mit Compliance-Fragen Risiken angemessen waren und im Falle der Prüftiefe „Prüfung“ effektiv angewendet wurden.*  *Confirmation que les méthodes / processus relatifs à l’identification, la mesure, la gestion et la surveillance des autres risques en lien avec les questions de compliance ont été appropriés et en cas d’étendue d’audit « audit » ont été effectivement appliqués.* | | | | | | |
|  | **Compliance with FINMA Circular 17/6** | Assess the compliance with the requirement of the Circular, in the context of the transmission of information to foreign supervision authorities and other foreign entities responsible for supervision, specifically: |  |  |  |
|  |  | Assess if the transmission of information is of little or no relevance for the institution.  If so, assess if the institution has implemented instructions for avoiding any transmission before escalation and issuance of instructions, internal guidelines and formalised procedures.  If not, assess the adequacy of the instructions respectively of the internal guidelines and formalised procedures dealing with the transmission of information to foreign supervision authorities and other foreign entities responsible for supervision. |  |  |  |
|  |  | Assess if the transmission of non-public information considered the precondition (margin no. 19 FINMA Circ. 17/6) or – if the relevant conditions have not been met from a requesting authority – the institution made additional clarifications (margin nos. 22-25 FINMA Circ. 17/6) and refused the transmission in case of doubts relating to the confidentiality and speciality (margin nos. 27-29 FINMA Circ. 17/6) | Test with a sample the adherence to the preconditions (margin no. 19 FINMA Circ. 17/6), the adequacy of required additional clarifications (margin nos. 22-25 FINMA Circ. 17/6) and thus the appropriateness of the transmission or non-transmission (margin nos. 27-29 FINMA Circ. 17/6). |  |  |
|  |  | Assess whether the institution adhered to the rules regarding preserving the rights of clients and third parties (margin nos. 30-31 FINMA Circ. 17/6) |  |  |  |
|  |  | Assess whether the transmission of information is only related to the business activities of clients and supervised parties (in application of Art. 42c para. 2 FINMASA; margin nos. 39-41 FINMA Circ. 17/6) | Test with a sample the compliance with the rules regarding the transmission of information (margin nos. 39-41 FINMA Circ. 17/6) |  |  |
|  |  | Assess whether the institution complied with its information and reporting duties in favour of FINMA (margin nos. 43-57 FINMA Circ. 17/6) | Test with a sample the compliance with the information and reporting duties in favour of FINMA (margin nos. 43-57 FINMA Circ. 17/6) |  |  |

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

1. Margin nos. 33 and 34 FINMA Circ. 13/3. [↑](#footnote-ref-2)
2. This audit involves ensuring that the institution or a third party has set up a framework for monitoring the legal and regulatory changes in Switzerland and abroad relevant and significant for the activities of the audited institution. [↑](#footnote-ref-3)