institute of internal auditors luxembourg

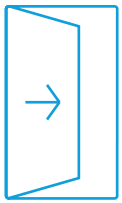
1996 - 2016

Sponsored by

Deloitte.

Institute of Internal Auditors, Luxembourg

2018 internal audit planning priorities for Luxembourg banking institutions



Dear members and friends of the IIA Luxembourg,

The leadership team of our Banking Working Group is delighted to share with you its publication on internal audit planning priorities for Luxembourg banking institutions.

The banking industry continues to operate in a complex environment, with internal audit functions under pressure and high expectations from internal and external stakeholders. In today´s world, aside from covering the regulatory baseline, internal audit is also meant to add insights on the hot topics that stem from regulatory and industry trends. At the same time, the International Professional Practices Framework (IPPF) continues to evolve, putting further emphasis on internal audit´s role as a trusted adviser within organizations beyond the traditional function of assurance provider.

This document is the result of a joint collaboration between the IIA Luxembourg and Deloitte Luxembourg. It provides views of internal audit leaders and experts, bringing together a great wealth of knowledge and experience. The objective of this piece was to offer real value to banking internal auditors and their organizations, with the aim of improving the efficiency of the 2018 annual planning process and ensuring enhanced audit coverage.

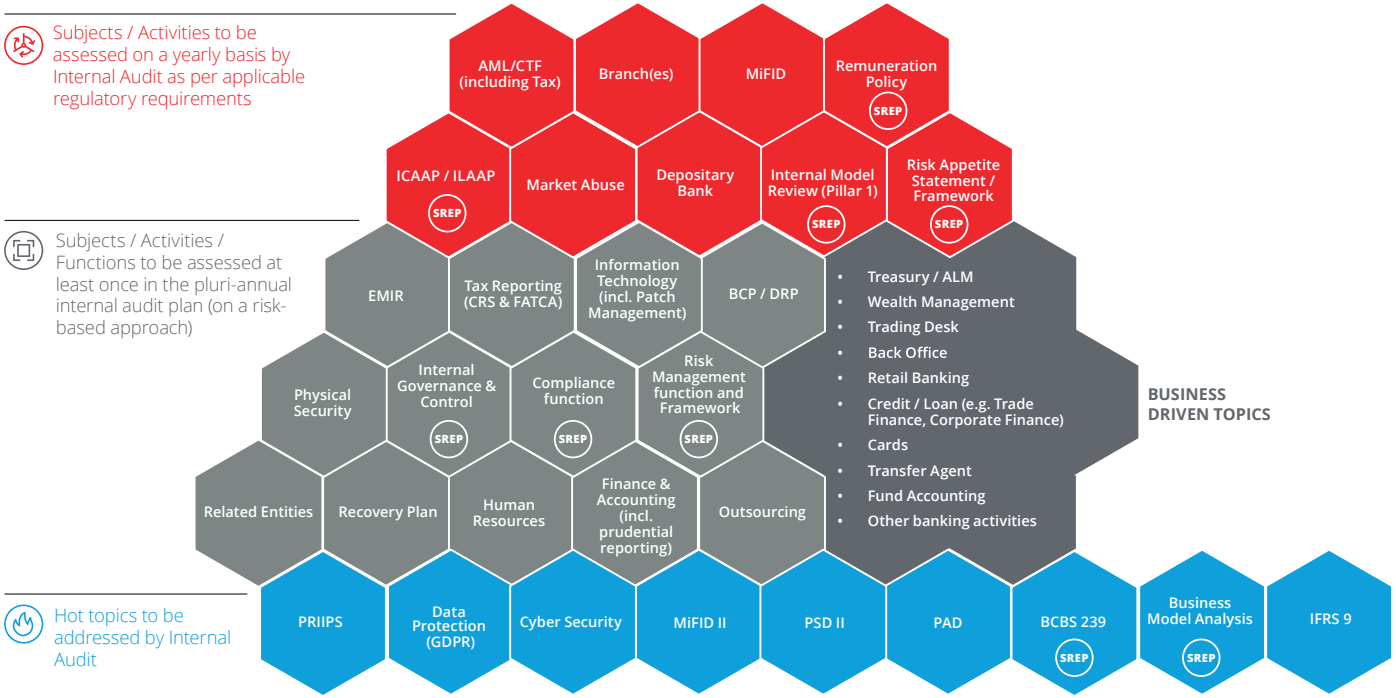
We would like to thank all the members of the Deloitte project team and the IIA Luxembourg Banking Working Group leadership team for their contributions and making this happen.

Best regards,
IIA Luxembourg

2018 internal audit planning priorities for Luxembourg banking institutions

The regulatory environment is in constant evolution, bringing new challenges every day for internal control functions including internal audit.

Internal audit, more than ever, has to play a critical role in the success of the organisation by detecting regulatory or internal control breaches that could impair the robustness of the Bank's internal control mechanisms and to a certain extent its reputation. In this context, we have highlighted below key and common regulatory and business topics we believe should be addressed within the internal audit plan of Luxembourg banking institutions with an emphasis on subject / activities that are required to be reviewed on an annual basis by the internal audit function in light of the applicable regulatory requirements and EU guidelines. This list does not intend to be exhaustive but rather to give a sound basis to internal audit practitioners in the preparation of their 2018 internal audit plan.



SREP Key components

Supervisory Review and Evaluation Process. The key purpose of SREP is to ensure that banking institutions have adequate arrangements, strategies, processes and mechanisms as well as the capital and liquidity to ensure sound management and coverage of the risks to which they are or might be exposed, including risks revealed by stress testing and any risks that banking institutions may pose to the financial system internal audit function in light of the applicable regulatory requirements and EU guidelines.

Issues to be assessed on a yearly basis by internal audit as per applicable regulatory requirements

This section addresses the applicable regulatory requirements (e.g. local regulation, circulars, EU directives or ECB guidelines) where internal audit should assess a subject/activity on a yearly basis. These references do not constitute an exhaustive list of texts.

AML/CTF
(including tax)

CSSF Regulation 12-02

Section 4 Internal audit control

Article 44 (1) ***The control of the AML/CFT (Anti-Money Laundering/ Counter Terrorism Financing) policy shall be an integral part of the mission of the professional's internal audit function.***

(2) The ***internal audit shall*** *assess the management and control of the risks on an independent basis and report to the authorised management and board of directors (or specialised committees) by providing them,* ***at least once a year, with a summary report on the compliance with the AML/CFT policy.*** *He shall show due diligence by ensuring that his recommendations or corrective measures are acted upon.*

CSSF Circular 17/650

2. Internal organization

This new framework must be implemented by the AML/CFT compliance officer and ***be controlled by the professional's internal audit.*** *The professional's authorised management must closely monitor the implementation of the framework and regularly report thereon to the Board of Directors or to the Supervisory Board.*

Key areas of concern

- Assess the internal governance arrangements covering AML/CTF, including the roles and responsibilities of the board of directors/ authorized management/chief compliance officer/MLRO, internal committees, reporting, AML/CTF policy and procedures;
- Assess the customer due diligence process: risk-based approach (including tax assessment), AML/KYC documentation, blocked account conditions;
- Assess monitoring of business relationships: name screening, transaction monitoring, periodic review of client accounts;
- Assess cooperation with the Luxembourg authorities;
- Assess the AML/CTF training program.

Branches

CSSF Circular 07/326 as amended

II.4 Risk management function, compliance function and internal audit function of the branch

30. At least once a year, the internal audit function of the head office shall audit representatively every aspect of the activities performed on the premises of the branch. *The summary report drawn up for the purpose of internal audit in accordance with "points 116 and 156 of Circular CSSF 12/552 on central administration, internal governance and risk management" (CSSF Circular 13/568) and to be submitted annually to the CSSF, shall include a chapter relating to the controls performed on the premises of every branch.*

Key areas of concern

- Assess the organization, oversight, and internal governance covering branches;
- Assess the level of reporting made by branches to head office;
- Assess the internal control framework covering the main activities of branches, in a representative manner, including an onsite inspection at least once a year.

MiFID

CSSF Circular 07/307

3.2 Responsibility of the authorised management

17. The authorised management defines the human and technical resources to be implemented to ensure the correct application of the policies and rules. It ensures that compliance with these policies and relevant procedures is checked by its compliance function and its internal audit function on a regular basis. To this end, ***it requires that written reports are submitted by the aforementioned functions on a regular basis and at least once a year.*** *In particular, these reports shall describe the deficiencies observed, the corrective measures taken and the follow-up on these measures.*

18. On a regular basis, and at least once a year, the authorised management submits reports on the issues covered by the internal audit function, the compliance function and, where required, the risk management function, to the board of directors.

Key areas of concern

- Assess the client classification process (categorization).
- Assess the suitability and appropriateness methodology and its implementation;
- Assess the adequacy and effectiveness of the banking institution's systems and internal control framework for identifying, preventing, and managing conflicts of interest to ensure fair customer outcomes;
- Assess whether the best execution and broker selection process is effectively designed and monitored;
- Assess the client-order handling rules process;
- Assess the list of inducements and the related governance and monitoring process;
- Assess the information provided to clients and potential clients (reporting).

Remuneration Policy

CSSF Circular 06/273

Annexe 1: Lignes directrices du CEBS du 10 décembre 2010 pour la conduite de bonnes politiques de rémunération:

2011/61/EU/Directive 2014/91/EU

49. The supervisory function should ensure that the remuneration policy of the institution will be reviewed on an annual basis at a minimum. *Such central and independent reviews should assess whether the overall remuneration system:*

- operates as intended (in particular, that all agreed plans/programs are being covered; that the remuneration payouts are appropriate, and that the risk profile, long-term objectives and goals of the institution are adequately reflected); and
- is compliant with national and international regulations, principles and standards.

The relevant internal control functions (i.e. internal audit, risk management, compliance functions, etc.) as well as other key supervisory function committees (i.e. audit, risk, and nominations committees) should be closely involved in reviewing the remuneration system of the institution.

The implementation of the remuneration policy is, ***at least annually,*** *subject to* ***central and independent internal review*** *for compliance with policies and procedures for remuneration adopted by the management body in its supervisory function.*

CSSF Circular 17/658

EBA guidelines on sound remuneration policies - EBA/GL/2015/22

36. The ***internal audit function should carry out an independent review*** *of the design, implementation and effects of the institution's remuneration policies on its risk profile and the way these effects are managed in line with the guidelines provided in section 2.5*

Key areas of concern

- Assess the organization, structure, and internal governance of the remuneration policy in light of the applicable regulatory requirements (e.g. establishing the list of identified staff, performance measurement, instruments and deferrals, malus/clawback, proportionality principle, transparency and disclosure);
- Assess the operational effectiveness of the remuneration policy.

ICAAP/ ILAAP

CSSF Circular 07/301 as amended

Sub-chapter II.4. General principles applicable to the ICAAP

*12. The **ICAAP is subject to a periodic review** in order to ensure that (...) This review shall take place **at least once a year.** It shall be carried out with the necessary objectivity and be subject to **an independent internal control.***

Sub-chapter II.7. ICAAP review by the internal audit and compliance function

27. The ICAAP, as any internal process, must be included in the scope of intervention of the internal audit.

28. Being a regulatory requirement, the ICAAP also falls under the competences of the compliance function.

*29. **The internal audit and the compliance function contribute to realising the integrity and effectiveness objectives** referred to under point 12, considering the organisation of these functions within the institution.*

Key areas of concern

- Assess the governance framework around the ICAAP, including the roles and responsibilities of the board of directors/authorized management/chief risk officer;
- Assess the risk identification process;
- Assess the risk assessment and measurement process;
- Assess the capital and liquidity planning;
- Assess the robustness of the stress testing program, including sensitivity analysis, reverse stress testing, and scenario analysis.

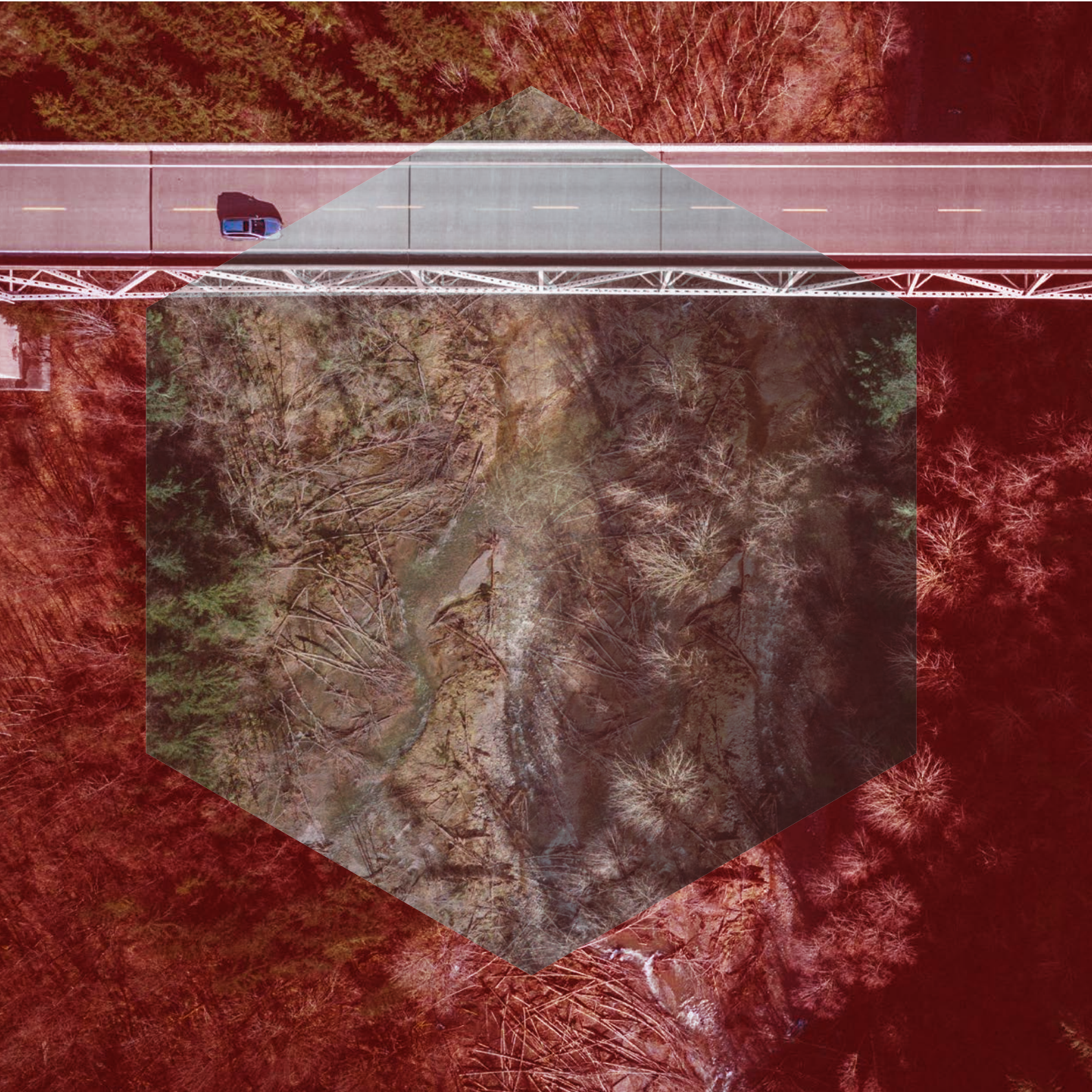
Market Abuse

Commission Delegated Regulation (EU) 2016/957 – 9 March 2016

Article 2 - General requirements - 5. Persons professionally arranging or executing transactions, market operators and investment firms operating a trading venue shall ensure that the arrangements, systems and procedures referred to in paragraphs 1 and 3: (a) are appropriate and proportionate in relation to the scale, size and nature of their business activity; (b) are regularly assessed, ***at least through an annually conducted audit and internal review,*** *and updated when necessary; (c) are clearly documented in writing, including any changes or updates to them, for the purposes of complying with this Regulation, and that the documented information is maintained for a period of five years.*

Key areas of concern

- Assess the organization, structure, and internal governance of the market abuse prevention and detection processes in light of the applicable regulatory requirements;
- Assess the internal control mechanisms in place for preventing, detecting, and reporting abusive practices or suspicious orders/ transactions.



Depositary bank

CSSF Circular 16/644
(only available in French)

Chapitre 2. Procédures internes et procédures écrites ou contrats avec des personnes externes relatives à la fonction de dépositaire d'OPCVM

31. Il relève de ***la responsabilité de l'audit interne ou du département de contrôle interne du dépositaire*** *de vérifier l'existence et le caractère approprié de ces procédures internes et des procédures écrites ou contrats avec les personnes externes ainsi que leur mise à jour périodique* ***et ce au moins une fois par an.*** *L'audit interne ou le département de contrôle interne doit également vérifier l'application effective de ces procédures internes et procédures écrites ou contrats avec les personnes externes. Cette obligation est notamment applicable aux procédures internes et procédures écrites ou contrats avec les délégués et sous-traitants du dépositaire*

Sous-chapitre 3.3 : Dispositions organisationnelles à mettre en place par rapport aux actifs dont la garde est assurée par un délégué au premier niveau en dessous du dépositaire

43. La procédure de diligence doit être réexaminée régulièrement, ***au moins une fois par an,*** *et mise à la disposition de la CSSF sur demande. Il relève de la* ***responsabilité de l'audit interne ou du département de contrôle interne du dépositaire*** *de contrôler l'existence, la mise à jour périodique et l'application effective de cette procédure.*

Key areas of concern

- Assess the organization and internal governance of the depositary bank function (e.g. organization chart, internal procedures, systems, depositary agreements/contracts, segregation of duties);
- Assess the design, implementation, and operational effectiveness of key controls applicable to the onboarding of investment funds, safekeeping, and record keeping (e.g. ownership verification), depositary oversight (e.g. registrar and transfer agent, fund administration), processing of investment transactions and related instructions, dividend distributions, custody operations (e.g. income and corporate action events), reconciliation of financial assets, cash flow monitoring, and the escalation process;
- Assess the selection and monitoring of sub-custodians, brokers, and prime brokers, including performance standards.

Chapitre 7. Dispositions organisationnelles en matière de rapprochements

*75. Il relève de la **responsabilité de l'audit interne ou du département de contrôle interne du dépositaire** de contrôler l'existence, la mise à jour périodique et l'application effective de ces procédures en matière de rapprochements et de s'assurer d'une résolution dans un délai raisonnable de toute différence de rapprochement constatée.*

Partie IV. Obligations spécifiques du dépositaire Chapitre 2. Missions de surveillance et de contrôle

*82. Le dépositaire est investi de missions de surveillance et de contrôle sur base des articles 18(2), 34(1) et 39 de la loi de 2010 et des articles 3 à 8 du règlement délégué. Les modifications apportées par la loi de 2016 et le règlement délégué sont relativement limitées, et s'articulent essentiellement autour du fait que les 5 types d'obligations de surveillance sont à effectuer par rapport à tous les OPCVM, quelle que soit leur structure juridique et par des précisions apportées dans le règlement délégué sur les tâches à accomplir par le dépositaire pour se décharger de ses obligations par rapport à ces missions de surveillance. En ce qui concerne ces missions de surveillance et de contrôle, il relève de la **responsabilité de l'audit interne ou du département de contrôle interne** de l'établissement agissant comme dépositaire de contrôler l'existence, la mise à jour périodique et l'application effective des procédures en relation avec les missions de contrôle.*

Internal model review (Pillar 1)

European Central Bank - Guide for the Targeted Review of Internal Models (TRIM)

16. The first two options are possible for all banks classified as significant institutions (SIs). When using the second option (two different units reporting to the same member of senior management), the institution should ensure that the additional requirements specified in Article 10(3) of the Final Draft RTS on assessment methodology for IRB and Article 22(1)(e) of the Final Draft RTS on assessment methodology for IMA and significant shares are fulfilled.14 They should also ensure, in particular, that the ***internal audit regularly assesses the fulfilment of these additional requirements.***

17. The third option is only possible for SIs which are not classified as globally significant institutions (G-SIIs) or other systemically important institutions (O-SIIs).15 When using the third option, institutions should ensure that the additional requirements specified in Article 10(4) of the Final Draft RTS on assessment methodology for IRB and Article 22(2) of the Final Draft RTS on assessment methodology for IMA and significant shares are fulfilled,16 and especially that the ***internal audit regularly assesses the fulfilment of these additional requirements.***

49. ***Pursuant to the existing regulatory requirements, the internal audit or another comparable independent auditing unit should review the rating system and its operations at least annually.*** *The areas for review should include compliance with all applicable requirements.*

Key areas of concern

- Assess the robustness of the governance process surrounding the setup and maintenance of the models;
- Assess the calibration process of the models;
- Assess the validation process of the models;
- Assess the back testing process implemented and maintained by the banking institution;
- Assess how the results of the back testing are embedded in the adjustment of the model calibration;
- Assess the existence of systematic reporting mechanisms about the status of the models to the Chief Risk Officer and the Authorized Management;
- Assess the regular thematic review on specific models (e.g. corp, mid corp, bank, retail).

Risk appetite statement and framework

European Central Bank – SSM supervisory statement on governance and risk appetite – June 2016

An independent review *of the Risk Appetite Framework ("RAF") should be performed regularly by the internal audit function to assess its effectiveness. Institutions, which perform such reviews generally, do this on* ***an annual basis,*** *including an assessment of the overall framework and of the adequacy of the limit breaches identification, escalation and reporting.*

Key areas of concern

- Assess the risk appetite framework, including key risk indicators (global and business), internal limits, early warnings and threshold in the light of the ECB requirements;
- Assess the completeness of the risk appetite framework (including financial risks and non-financial risks);
- Assess the consistency of the risk appetite framework with the business strategy of the banking institution and the consistency of the indicators with elements disclosed in the recovery plan;
- Assess the regular review of the risk appetite framework in the context of sound internal governance mechanism;
- Assess the internal governance over the periodic review and validation of the risk appetite framework.

Issues /activities/functions to be assessed at least once in the internal audit plan (risk-based approach)

This section lists the main issues/activities/functions that should be part of the audit universe of the Luxembourg banking institutions to be assessed at least once in the internal audit plan using a risk-based approach.

European Market Infrastructure Regulation (EMIR)

- Assess the completeness of contracts with all counterparties;
- Assess the implementation of risk mitigation techniques (non-cleared instruments) to reduce the operational risk of bilateral (non-centrally cleared) OTC derivatives transactions (including timely confirmation, daily valuation, portfolio reconciliation, dispute resolution, portfolio compression, collateral requirements);
- Assess the quality and timeliness of the monitoring of EMIR reporting (reporting of OTC and ETD contracts and collateral and valuation/ collateral reporting);
- Assess the implementation of clearing obligations.

Tax reporting (FATCA & CRS)

- Assess the organization and internal control environment for tax reporting: FATCA and CRS;
- Assess the organization, structure, and internal governance of the tax reporting process in light of the applicable FATCA regulatory requirements (e.g. registration on the IRS portal, US indicia process to detect eligible clients, classification of new clients/pre-existing accounts, closing accounts and reporting) and CRS requirements (e.g. reporting).

Information Technology (including patch management)

- Assess the organization and internal governance of the IT function (e.g. reporting lines, committee, appointment of information security officer/IT officer);
- Assess the internal control framework for information security (e.g. logical access, change management, backup management, job scheduling, patch management*).

* *In accordance with the provisions of CSSF Circular 12/552 as amended by CSSF Circular 17/655: "The institutions shall have a monitoring process in place in order to be quickly informed of the emergence of new security vulnerabilities, as well as a procedure to manage patches allowing the correction of these vulnerabilities, within a short period of time, if they can significantly impact their IT systems. Internal audit shall include the review of the monitoring process and the management of patches in its multi-annual audit plan; it shall notably state any failures in the launch of production of a patch while this patch is widely known and shall document such failure in an audit finding".*

Business Continuity Plan (BCP)/Disaster Recovery Plan (DRP)

- Assess the organizational processes in place for the BCP/DRP aimed at avoiding, preventing, handling, and recovering from planned and unplanned outages;
- Assess the operational resilience of the banking institution (end-to-end technology architecture and its relative importance).

Physical security

- Assess the implementation and monitoring of physical security processes (e.g. emergency drills, building evacuations, contingency arrangements, internal policy, insurance, training);
- Assess the controls in place to restrict physical access to authorized individuals and detect any unauthorized access;
- Assess the protection of and access to sensitive physical information.

Internal governance and controls

- Assess the internal governance arrangements at the board of directors and authorized management level (e.g. composition, agenda/minutes), including oversight of any branches and subsidiaries, where relevant;
- Assess the appointment and revocation procedures for key function holders;
- Assess the fit and proper criteria applicable to key function holders;
- Assess the composition, functioning, and mandates of specialized committees;
- Assess the banking institution's internal control mechanisms.

Compliance function

- Assess the organization, nature, and purpose of the compliance function, including the compliance policy and the compliance code;
- Assess the methodology used to create the compliance monitoring plan incorporating a risk-based approach (compliance risk assessment);
- Assess the regulatory oversight (e.g. identification of laws, regulations, circulars, guidelines, standards applicable to the organization) performed by the compliance function and the information circulated within the organization (e.g. education, training);
- Assess the operational effectiveness of the complaints handling policy and related procedures*;
- Assess the periodic reporting of the compliance function to the authorized management, the board of directors, and the CSSF.

Risk management function and framework

- Assess the organization, nature, and purpose of the risk management function (role, responsibilities, and duties);
- Assess the risk strategy and policy;
- Assess the risk monitoring program that is part of the risk appetite framework;
- Assess the risk inventory and measurement process;
- Assess whether the interest rate risk for the banking book has been measured in line with EBA and CSSF requirements, and is appropriately managed.

* *In accordance with the provisions of CSSF Circular 17/671 (only available in French): "Le directeur responsable détermine les moyens humains et techniques à mettre en oeuvre pour appliquer correctement la politique et les procédures en question. Il fait contrôler régulièrement le respect de cette politique et des procédures y relatives par la fonction compliance du professionnel et par sa fonction d'audit interne".*

Related entities

- Assess the related entities of the banking institution falling into the scope of the supervision;
- Assess the organization, oversight and monitoring over the related entities;
- Assess the reporting lines existing between the banking institution and the related entities.

Recovery plan

- Assess whether any comments made to the bank by the Luxembourg regulatory authorities (CSSF) or European Central Bank (ECB) in relation to the recovery plan have been addressed.

Human resources

- Assess the organization and structure of human resources;
- Assess the internal control framework over key processes (e.g. recruitment, employment contracts, payroll, overtime, vacations, training programs and development, performance evaluation, remuneration packages).

Outsourcing

- Assess the organization, structure, and internal governance of the outsourcing framework in light of the applicable regulatory requirements;
- Assess whether the outsourcing policy addresses key regulatory expectations as well as roles and responsibilities;
- Assess whether all outsourced services are underpinned by relevant contracts (e.g. service level agreements, operating memorandum) and related terms and conditions;
- Assess whether the monitoring process for outsourced activities is based on relevant indicators (e.g. key performance indicators, key risk indicators);
- Assess whether adequate procedures support the application of the outsourcing framework, in particular the escalation procedure;
- Assess whether initial and ongoing due diligence is performed (including onsite visits to service providers).

Finance and accounting

- Assess the organization and governance of the finance and accounting functions;
- Assess the daily and monthly closing process;
- Assess the governance arrangements and internal controls of internal/transitory accounts;
- Assess the monitoring and documentation of manual transactions;
- Assess the invoice validation process and release of the related payments;
- Assess the financial control framework;
- Assess the budget preparation and monitoring process;
- Assess the internal control framework for reporting (including regulatory, prudential, BCL and internal reporting);
- Assess the banking institution's process for preparing financial statements.

Hot topics to be addressed by internal audit

Internal audit plans for 2018 need to reflect the new regulatory requirements that will have an impact on banking institutions. The internal audit function will therefore be required to adapt to the new regulatory framework while at the same time managing emerging risks, meeting ever-expanding stakeholder expectations, and keeping abreast of developments in technology.

Packaged Retail and Insurance-based Investment Products (PRIIPs)

- Assess the preparation and monitoring of the requirements linked to PRIIPS including Key Information Documents (KIDs).

Data protection (GDPR)

Assess the internal framework put in place by the bank in the light of the EU General Data Protection Regulation (GDPR) on the data privacy of EU citizens in terms of:

- Strategy: does the organization have a clearly defined data protection strategy?
- Organization and accountability: has an effective privacy strategy been implemented, and have roles and responsibilities concerning data protection been defined (e.g. role of the data protection officer)?
- Policies, processes and data: is data protected, governed, managed, and utilized effectively in line with the organization's strategy through the effective implementation of organizational (e.g. policies and procedures) and technical controls (e.g. access segregation controls)?
- Culture, training, and awareness: has a high level of organizational awareness around privacy been created (e.g. awareness training)?
- Privacy operations: has privacy been embedded into the organization's project methodology (e.g. systems should be "privacy" friendly by design and by default)?
- Data processing inventory: has a personal data processing inventory been prepared as per GDPR requirements?

Cyber security

- Assess the organization and internal governance of the cybersecurity framework.
- Assess whether a comprehensive third-party risk assessment has been conducted by the banking institution in order to develop a third-party cybersecurity plan.
- Assess whether security standards have been adequately incorporated into third-party contracts and include a "right to audit" clause.
- Assess the cybersecurity monitoring process (particularly vulnerability and patch management activities).

MiFID II

- Assess the advisory model and quality of enhancement for non-independent advisory (inducement);
- Assess product governance (product complexity, product approval, and target market definition/monitoring);
- Assess the methodology for suitability and appropriateness (client profiling and classification);
- Assess the client information and reporting process (client agreement/contracts, information provided to clients, marketing documentation, reporting to clients);
- Assess the transaction process (transaction reporting);
- Assess the trading process and best execution (e.g. investment research, trading obligation, best execution, and selection and order handling policy);
- Assess the organization and internal governance (client assets' safekeeping and intra-group deposits, record keeping, business continuity, compliance policy, conflicts of interest policy, management body organization).

Payment Services Directive II (PSD II)

- Assess the organization and internal governance of payment services;
- Assess the process for authorizing and recording payments (cut-off and value dates);
- Assess the process for managing access to the payment system and nostro accounts;
- Assess the transparency of the conditions and information requirements for payment services.

Payment Accounts Directive (PAD)

- Assess whether fee transparency is sufficient and compliant with regulation 2014/92/EU to ensure comparability between service offers;
- Assess the process for switching payment accounts, and whether payment account switching offers to consumers are clear, quick, and safe (as specified by the regulation);
- Assess whether all EU customers (nationality or residence) have equal payment account access.

BCBS 239

- Assess the organization and internal governance infrastructure (e.g. risk data architecture, IT infrastructure);
- Assess the risk data aggregation capabilities;
- Assess risk management reporting;
- Assess the suitability of the banking institution's independent valuation framework design and operational model;
- Assess that first-line-of-defense monitoring is in place and that any incidents are duly reported.

Business Model Analysis

- Assess the viability of the banking institution's current business model on the basis of its ability to generate acceptable returns over the following 12 months;
- Assess the sustainability of the banking institution's strategy on the basis of its ability to generate acceptable returns over a forward-looking period of at least 3 years, based on its strategic plans and financial forecasts;
- Assess the analysis of the banking institution's financial projections and strategic plan to understand the assumptions, plausibility and riskiness of its business strategy.

IFRS 9

- Two elements are critical to this topic including accounting and internal model for loan loss provisioning. Such elements can be separately addressed respectively in the audit units "Finance & Accounting" and "Internal Model Review (Pillar I)".

About IIA Luxembourg
IIA Luxembourg is the local institute of the Institute of Internal Auditors (the IIA), the driving force in internal audit-related research and the promoter of the code of ethics and regulations guiding the profession.
Since its foundation in 1996 as the local chapter of IIA Global, the IIA Luxembourg has grown to become one of the leading professional organisations in Luxembourg, bringing together around 590 members employed by some 100 Luxembourg-based corporations across all economic sectors.

Contact Us
IIA Luxembourg
Tel: +352.26 27 09 04
Email: iialux@pt.lu
Web: www.iia.lu