



Association Luxembourgeoise
des Compliance Officers
du Secteur Financier



**ALCO Working Group 25:
ALCO-IACI Sub-Group 1
ALCO-PRIM Sub-Groups 2 & 3**

SUBMISSION PAPER

THREE FUNCTIONS IN THE FINANCIAL SECTOR

Compliance

Operational Risk Management

Internal Audit

This document reflects the conclusions of the working groups delegated by the three associations :
ALCO, IACI and PRIM.

Table of Contents

Introduction	4
1. The Regulatory Framework.....	4
1.1 Compliance.....	4
1.1.1 International.....	4
1.1.2 Luxembourg.....	4
1.2 Risk Management.....	5
1.2.1 International.....	5
1.2.2 Luxembourg.....	5
1.3 Internal Audit	6
1.3.1 International.....	6
1.3.2 Luxembourg.....	7
2. Compliance: role and scope	8
2.1 Compliance Role	8
2.2 Compliance Scope.....	8
2.2.1 Anti-Money Laundering / Anti-Terrorism.....	8
2.2.2 Banking Secrecy	8
2.2.3 Data Protection / Personal Data Protection	9
2.2.4 Insider / Staff Dealing and Market Abuse.....	9
2.2.5 Conflict of interest and Corruption - Investor Protection.....	9
2.2.6 Code of Ethics / Code of Conduct.....	10
2.2.7 New Products / Business Lines	10
2.2.8 Legal Risk	10
3. Operational Risk Management role and scope	11
3.1. Generic Mission	11
3.2 The Risk Framework	11
3.2.1 Identification.....	11
3.2.2 Assessment.....	11
3.2.3 Mitigation / Control.....	12
3.2.4 Monitoring and Reporting	12
4. Internal Audit : role and scope	13

4.1.	Internal Audit Role.....	13
4.2.	Internal Audit Scope.....	13
5.	Intersection between the functions	15
5.1	Requirements / Recommendations derived from the current legislation.....	15
5.2	Tasks by Function	16
5.2.1	Compliance	16
5.2.2	Operational Risk Management	17
5.2.3	Internal Audit	18
5.2.4	Special cases	18
5.3	General Functional Differences.....	20
5.3.1	Powers, delegations and access	20
5.3.2	Coordination and cooperation	21
5.3.3	Recommendations	22
5.3.4	Sanctions	22
5.4.	Functional Reporting Lines	22
5.4.1	General principle	22
5.4.2	Compliance Committee / Internal Audit Committee	23
5.4.3	Functional Reporting	24
6.	Conclusion.....	25

Introduction

The Third Capital Adequacy Directive in its article 22 states that :

“Every credit institution (must) have robust governance arrangements which include a clear organisational structure with well-defined, transparent and consistent lines of responsibilities, effective processes to identify, manage, monitor and report the risks it is or might be exposed to and adequate internal control mechanism including sound administrative and accounting procedures.”

IML Circular 98/143 defines the scope, role and mission of Internal Audit. Basel II defines the scope of Operational Risk Management and CSSF Circular 04/155 defines the mission of Compliance without explicitly defining its scope.

This paper aims to clarify the specificities; the commonalities; and the links between the functions of Risk Management and Internal Audit vis a vis Compliance.

In order to focus the results, the paper deliberately excludes the Financial and Credit aspects of Risk Management and concentrates solely on the Operational Risk aspect. The reason for this is that most financial institutions tend to have separate, well-established functions for Financial and Credit Risk due to the precise nature of those risks. Also, recognition of those risks is “older” than Operational Risk. Therefore, all references are to Operational Risk Management in this paper, unless specifically stated otherwise.

1. The Regulatory Framework

1.1 Compliance

1.1.1 International

On the international level, the reference is the April 2005 Bank for International Settlements paper: *“Compliance and the Compliance Functions in Banks.”*

1.1.2 Luxembourg

In Luxembourg, the regulatory framework applying to Compliance primarily consists of:

- the Law of 5 April 1993 on the Financial Sector which established the required “rules of conduct”;
- the Law of 12 November 2004 relative to the fight against money laundering and the financing of terrorism which established the obligation to know one’s clients, to have adequate internal organisation and to cooperate with the relevant authorities.
- CSSF Circular 2000/15 on Rules of Conduct in the Financial Sector (as amended by CSSF Circular 05/177);
- CSSF Circular 04/155 on the Compliance Function.

1.2 Risk Management

1.2.1 International

The Third Capital Adequacy Directive (article 4) defines Operational Risk as:

“Operational Risk means the risk of loss resulting from inadequate or failed internal processes, people and systems, or from external events and includes legal risks”

Although strategic and reputation risk are not included in the calculation of Operational Risk, some financial institutions do include those risks.

Annex 7 of the Basel II Accord ¹ provides a detailed classification of operational risks which indicates that it covers legal risk, which is defined as “exposure to fines, penalties, or punitive damages resulting from supervisory actions, as well as private settlements.” A detailed loss event type classification further details the risks pertaining to this category of legal risks. It includes incidents arising from:

- unauthorised activity;
- theft and fraud;
- employee relations;
- safe environment;
- diversity and discrimination;
- suitability and disclosure; and
- improper business and market practices.

In particular, Annexe 7 outlines that loss events types belonging to operational risk arise from:

- fraud;
- tax non-compliance;
- insider trading;
- breach of privacy;
- misuse of confidential information;
- anti-trust; and
- money laundering.

1.2.2 Luxembourg

There is no similar Circular or Law in Luxembourg specifically relating to Risk Management or Operational Risk. However, Chapter III, Paragraph 10 of CSSF Circular 04/155 states:

“The expression compliance risk is defined as the risk of losses that an institution may suffer as a result of the failure to conduct its business in accordance with the rules in force. It can include a variety of risks such as reputation risk, legal risk, litigation risk, risk of sanctions, as well as certain aspects of operational risk, in relation with all the institution’s business activities.”

Also, Section 5 of IML Circular 98/143 states the system of internal control must:

¹ See also the Third CAD Directive, Annex X, Part 5, Table 3.

“... encompass a system of identification, of measurement, of control and of information on the risks of the bank or PSF, financial as well as operational ...”

1.3 Internal Audit

1.3.1 International

On the international level, the reference is the August 2001 Bank for International Settlements paper: *“Internal Audit in Banks and the Supervisor’s Relationship with Auditors.”*

In addition, the Institute of Internal Auditors also issues internal audit standards.

International Standards for the internal audit profession

The internal audit profession is regulated by the professional standards set up by the Institute of Internal Auditors (IIA).

In June of 1999, the IIA’ Board of Directors approved a new Professional Practices Framework (PPF) and a new definition of internal auditing:

“Internal auditing is an independent, objective assurance and consulting activity designed to add value and improve an organization's operations. It helps an organization accomplish its objectives by bringing a systematic, disciplined approach to evaluate and improve the effectiveness of risk management, control, and governance processes.”

The Professional Practices Framework (PPF) consists of three categories of guidance: Standards and Ethics, Practice Advisories, and Development & Practice Aids.

The first category (Mandatory Guidance) consists of core materials: the *Code of Ethics* and the *Standards for the Professional Practice of Internal Auditing (Standards)*.

The purpose of The Institute’s *Code of Ethics* is to promote an ethical culture in the profession of internal auditing.

Standards, as described within the PPF, are the criteria by which the operations of an internal auditing department are evaluated and measured. Within the new framework, three sets of standards have been developed: Attribute, Performance, and Implementation Standards.

- the Attribute Standards address the attributes of organizations and individuals performing internal audit services;
- the Performance Standards describe the nature of internal audit services and provide quality criteria against which the performance of these services can be measured.

The Attribute and Performance Standards apply to all internal audit services.

- the Implementation Standards expand upon the Attribute and Performance Standards, providing guidance applicable in specific types of engagements.

Compliance with the concepts enunciated in the Mandatory Guidance is essential before the responsibilities of internal auditors can be met.

As stated in the *Code of Ethics*, internal auditors shall perform internal auditing services in accordance with the *Standards*. All members of The Institute and all Certified Internal Auditors agree to abide by the *Standards* and *Code of Ethics*, and this guidance is intended to be applicable to all members of the internal auditing profession, whether or not they are members of The Institute.

In various countries, specific laws have been issued to clarify the Internal Audit function. These laws may affect Luxembourg banks with branches or subsidiaries in these countries, or with its head office located in one of these countries. In such cases, these banks must comply with the most stringent regulations applicable.

The members of the working group identified the following key texts:

- the recommendations issued by the US Sentencing Commission. (US Federal Guideline Manual, dated November 2004),
- the UK's FSA Handbook, dated January 2002,
- the French « Loi sur la sécurité financière » dated 1 August 2003 and the French decree dated 31 March 2005 modifying the 97-02 regulations related to the internal control of banks and investment funds,
- Belgium's Circular D1 –2001/13, dated 18 December 2001.

1.3.2 Luxembourg

In Luxembourg, the regulatory framework applying to Internal Audit primarily consists of:

- the Law of 5 April 1993 on the Financial Sector which establishes the required “rules of conduct”;
- Circular IML 98/143 on Internal Control clarifying the internal audit function and which states “The purpose of internal audit is to ensure that the system of internal control is operating effectively.”

In addition to all of the above, the forthcoming Markets in Financial Instruments Directive and the third Capital Adequacy Directive will expand definitions and requirements of the three functions.

2. Compliance: role and scope

2.1 Compliance Role

CSSF Circular 04/155 provides that the Compliance function be independent and aimed at protecting the financial institution from any prejudice that might result from the failure to comply with the rules in force and to assist senior management in managing and monitoring this risk. It reports to senior management and, where applicable, to the board of directors and can act as advisor to senior management. The expression compliance risk is defined as the risk of losses that a financial institution may suffer as a result of the failure to conduct its business in accordance with the rules in force. It can include a variety of risks such as reputation risk, legal risk, litigation risk, risk of sanctions, as well as certain aspects of operational risk, in relation to all the financial institution's business activities.

The compliance function performs regular controls linked to the ongoing and close controls of the operations of a financial institution, with regard to Compliance risk.

2.2 Compliance Scope

The authors of this paper have performed a detailed review of the practice of the Compliance functions in several financial institutions. The outcome of this analysis indicates that the obligations faced by the financial institutions, regarding compliance with norms, rules and regulations, can be broadly classified in the following categories (this may vary by institution).

2.2.1 Anti-Money Laundering / Anti-Terrorism

Money laundering is any process, using the financial system, by which persons or entities attempt to conceal the true origin and / or the true ownership of the monetary proceeds of activities considered by law as criminal.

Terrorist financing constitutes the gathering or supply of any funds or proceeds intended for use in the commission of terrorist acts or the activities of terrorist groups.

2.2.2 Banking Secrecy

Professional secrecy is the legal obligation for any depositories of secrets, by status or profession, to keep secret or confidential information they obtained pursuant to their professional activity.

Financial professionals, due to the very nature of their work in being recipients of confidential information, are under a legal obligation of professional secrecy. Any breach of this professional obligation is a criminal offence.

This obligation applies equally to directors, managers, employees and any service providers who, in the course of their working practice, receive confidential customer information.

2.2.3 Data Protection / Personal Data Protection

The processing of personal data is fundamentally forbidden by the law, except in certain situations where special permission for collection, processing and use of such data is granted contractually by a data subject, or by law.

Personal data means any information concerning the personal or material circumstances of an identified or identifiable data subject.

“Data Subject” is any specific or identifiable individual whose data is subject to data processing (according to Luxembourg law, legal persons are also data subjects).

“Data Processing” is any operation or set of operations performed upon personal data, whether or not by automatic means, such as collection, recording, organisation, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction.

2.2.4 Insider / Staff Dealing and Market Abuse

Insider Dealing means using Insider Information in order to make a profit or avoid a loss, disclosing such information to a third party except in the normal course of working practice or making a recommendation to a third party on the basis of such information.

Insider Information means non-public information concerning the financial institution as well as third parties that may considerably affect market price in the trading of securities or derivatives if the information were released into the public domain.

Information is deemed public once it is publicly disseminated, e.g. when it is reported on an ad-hoc publication service, a major wire service or in a newspaper of general circulation. Limited disclosure, such as a private wire service for institutional investors only, is not sufficient.

Market abuse means intentional actions aiming at influencing the supply of, demand for, or price of financial instruments. Irrespective of whether or not there is a material impact on the supply, demand or price of financial instruments, intention is the decisive factor.

2.2.5 Conflict of interest and Corruption - Investor Protection

Corruption is defined as the offering or receipt of benefits to/from existing or prospective customers and suppliers, by employees of a financial institution, with the objective of influencing a decision.

Conflict of interests are defined as situations where employees of a financial institution who either take decisions or have an influential role in any decision-making process can have private interests which may influence the business decisions being taken.

In all its dealings, Compliance takes into account the interests of the investors to ensure their protection under the laws and regulations.

2.2.6 Code of Ethics / Code of Conduct

Apart from the existing laws, rules and regulations with which they have to comply, financial institutions may find it necessary to identify a certain number of values which should serve as references to the staff in any kind of situation. These values may be translating into more concrete recommendations aiming at providing guidelines for staff's professional behaviour.

2.2.7 New Products / Business Lines

It is important for Compliance to be formally consulted on proposed new products and / or business lines, from the earliest stages of the proposals. This is to ensure that the proposals take into account compliance issues and investor interests such as suitability etc.

2.2.8 Legal Risk

The authors believe that the Compliance areas identified above should be considered by the financial institutions of the Luxembourg market place as the minimum scope of any Compliance function.

The decision on whether other areas related to rules and regulations (corporate law, labour and social laws, environment regulations...) should be partially or totally attributed to the Compliance function should be left to the discretion of the financial institutions.

In particular, while Legal Risk is properly the domain of the Legal department, Compliance may participate in the assessment of the impact of new laws and regulations on the operations of the financial institution, particularly for smaller institutions.

3. Operational Risk Management role and scope

3.1. Generic Mission

Basel II assigns the following mission to the Risk Management Function:

- Designing and implementing the risk management framework aiming at identifying, assessing, controlling and reporting Operational Risk
- Codifying firm level policies and procedures concerning Operational Risk management and controls
- Designing and implementing the firm's Operational Risk measurement methodology
- Designing and implementing a risk-reporting system for Operational Risk

Moreover, the Third Capital Adequacy Directive III, Annex X (part 2-4) states that credit institutions should meet qualifying criteria and particularly:

- a) *“Credit institutions shall have a well-documented assessment and management system for operational risk with clear responsibilities assigned for this system. They shall identify their exposures to operational risk and track relevant operational risk data, including material loss data. This system shall be subject to regular independent review.”*

3.2 The Risk Framework

The Risk Management function is in charge of designing and implementing the risk framework. The latter consists of following four key processes which can be performed by different entities within the financial institution, depending on the size of the business and the geographic area covered by the financial institution.

3.2.1 Identification

The essential pre-requisite for the risk management process is Risk Identification. This involves – to the most complete extent possible – the identification of all threats to the financial institution, as well as the causes of loss and potential disruptions. Risks may arise as a result of internal activities or external factors. The risk examination must be performed with regard to existing or new processes when concluding new business or entering new service areas.

3.2.2 Assessment

The Risk Assessment phase is usually carried out by the Risk Management function. It consists of assessing the impact that a given threat may have on the financial institution. The risk assessment can be based on quantitative methodology or on a qualitative approach. In the quantitative approach, the various components of risks are quantified in financial terms using the Value at Risk (VaR) methodology, performing stress tests with a defined interval of confidence.

In the qualitative approach the assessment produces risk ratings to be applied.

3.2.3 Mitigation / Control

The development of a single risk, or a combination of them, must be constantly monitored according to the previous steps in the risk management process. Changes to previous periods must be analysed. When necessary, a decision on the development of mitigating actions must be taken by the company. The mitigating actions may have two objectives:

1. reducing the source of risk (e.g. the threats) through the implementation of extra controls; or
2. reducing the impact of incidences. For example, the development and testing of business recovery plans, reinforcing redundant systems etc.

3.2.4 Monitoring and Reporting

It is essential that the executive management of a financial institution is informed about current risks and potential future risks, enabling it to take suitable measures and to monitor the risks as well as the effectiveness of the mitigations. The reporting should provide a global view of the risk profile of the company, including an aggregated financial countervalue of the risk exposure, as well as a detailed analysis of critical events which have significantly impacted the risk profile of the financial institution during the reporting period. It is the core responsibility of the Risk Management function to ensure that this obligation is fulfilled in a regular, transparent and objective manner.

4. Internal Audit : role and scope

4.1. Internal Audit Role

Circular 98/143 defines Internal Audit as an independent function which verifies the effectiveness and the efficiency of the Internal Control system. Thus, Internal Audit carries out *a posteriori* controls and it is located on the fourth level of the Internal Control set-up of an institution. Internal Audit may also provide consulting services, as well as reassurance, to management.

Internal Audit reports to the highest level of management and has direct access to the Audit Committee.

It is important to note that, in large organisations, there are still Inspection functions, generally co-ordinating with Internal Audit, but sometimes with Compliance. The role of Inspection is normally to take the lead in investigations, mainly in the accounting field, aimed at the detection of internal fraud, and of weaknesses in physical security.

4.2. Internal Audit Scope

CSSF Circular 98/143 (§ 5.4.6.) confirms the scope of Internal Audit as follows:

“The field of Internal Audit covers all the activities and functions of the bank or the FSP (Financial Sector Professional), and cannot be restricted.

Generally, the Internal Audit department goes through the administrative and accounting organisation of the institution, and make an evaluation. It checks as well if the planned Internal Controls are adequate and efficient. Internal Audit takes into account rules and recommendations set up by the IML in the present circular, as well as in the following IML Circulars: 93/101, 93/102, 95/119, 96/126, and, in addition, the individual guidelines that may have been given by the IML to an institution.

More particularly, the Internal Audit department has to check, amongst other things:

- *The good functioning of the risk identification system, the risk measures, the limitations and alert systems,*
- *The validity of value and good administration,*
- *The good functioning of task division,*
- *The good execution of operations,*
- *The correct and complete registration of operations, together with the production of a fast and reliable information,*
- *The execution of decisions taken by the management and by the delegates, and with respect to the regulatory framework of the banks, or the FSP.*
- *The availability of data provided to senior management in order to support its control function in conformity with § 5.3. here-above.”*

If a separate department is in charge of control or surveillance of a specific activity or function within the institution, the Internal Audit department is still responsible for controlling this specific field.

5. Intersection between the functions

5.1 Requirements / Recommendations derived from the current legislation

Besides the definition of the Internal Control framework to be implemented by a financial institution, IML Circular 98/143 identifies four levels of controls:

- 1st level controls: Ongoing controls performed by the operators
- 2nd level controls: Ongoing critical controls performed by the persons in charge of administrative operations
- 3rd level controls: Controls performed by executive management over activities which are under their responsibility
- Audit control: Aiming at ensuring that the overall control framework of the financial institution is adequate.

CSSF Circular 04/155 indicates that the Compliance Function is responsible for:

- The identification and the assessment of the risks of compliance;
- The procedures and instructions supporting the implementation of the compliance policy; and
- The controls ensuring that the compliance policy is applied.

It is understood that Compliance forms part of the 3rd level controls, and effectively Operational Risk Management also.

CSSF Circular 04/155 also indicates that any of the tasks which are under the responsibility of the Compliance function can be delegated to other departments within the financial institution, provided that such delegations are clearly documented in the Compliance Charter, and provided that the Compliance function remains responsible for the delegated tasks.

In particular, the Circular indicates that the Compliance function must perform regular controls vis a vis procedures and instructions, but it does allow for the Compliance function to rely on the Internal Audit function to do so.

Basel II indicates that the Risk Management function is responsible for designing and implementing the risk management framework aiming at identifying, assessing, controlling and reporting Operational Risk, while the Third Capital Adequacy Directive III, Annex X (part 2-4) states that:

- b) *“The operational risk assessment system must be closely integrated into the risk management processes of the credit institution. Its output must be an integral part of the process of monitoring and controlling the credit institution’s operational risk profile.*
- c) *Credit institutions shall implement a system of management reporting that provides operational risk reports to relevant functions within the credit institution. Credit institutions shall have procedures for taking appropriate action according to the information within the management reports”*

However, these texts do not provide any recommendation on whether any particular department of a financial institution should be specifically or exclusively in charge of performing the tasks belonging to any of these processes.

5.2 Tasks by Function

It should also be noted that financial institutions have “Control” areas within them that are linked e.g. Internal Control, Risk Control, Compliance Control, Quality Assurance etc. The authors of this paper believe that it matters not so much who carries out the controls, but that they are carried out. For this reason, the following tasks were identified:

- where the law or regulations state what tasks must be done by a particular function (“Compulsory Tasks”);
- where tasks cannot be carried out by a particular function due to conflicts of interest (“Conflicting Tasks”); and
- Tasks/areas that should be covered as a matter of sense but where it is irrelevant which function carries it out (“Optional Tasks”);

5.2.1 Compliance

Scope: Covers compliance risk of the financial institution arising from failure to comply with laws, regulations, Circulars relating to access to, and conduct of, business within the financial sector, as defined in each financial institution’s Compliance Charter.

Role: Required by CSSF Circular 04/155.

Compulsory Tasks:

- must assess the compliance risk arising from failure to comply and also relating to professional obligations (including anti-money laundering, rules of conduct etc);
- must identify “rules in force”, maintain an up-to-date list and make this available to staff;
- ensure rules in place to guide staff in the performance of their duties across all business lines;
- must be consulted at the time of drafting and implementing internal control procedures;
- must centralise all information on Compliance issues;
- must analyse, provide recommendations and follow up on remedial actions agreed, where appropriate for corrective measures in all compliance-related incidents;
- must develop and implement a compliance training programme; and
- must fulfil all reporting obligations to the CSSF and other relevant authorities regarding anti-money laundering etc.

Conflicting Tasks:

- may not report to a department or unit within the financial institution but to senior management.

Optional Tasks:

- may delegate tasks to other departments/units/divisions, in which case it must act as a coordinator; and

- may rely on Internal Audit work in the course of monitoring compliance risk procedures and instructions.

Other:

- must be an independent function; and
- is subject to internal audit.

5.2.2 Operational Risk Management

Scope: May cover entirety of operations within a financial institution. The extent to which institutions define the breadth of this scope varies, although the defining references are found in Basel II and in the Third Capital Adequacy Directive.

Role: Not defined by any Circular. However, Basel Operational Risk recommendations (Sound Practices), while not of the same force, are used by regulators (to ultimately be replaced as a basis by the Third Capital Adequacy Directive). In Basel II ², the core role is expected to cover the design and roll-out of the following key aspects:

- Risk management framework
- Enterprise-wide operational risk policies and high-level procedures
- Operational risk measurement methodology
- Operational risk reporting systems and processes

Ultimately, the operational risk function is expected to provide assessments on the magnitude of the risks arising from a failure of processes, whether they be caused by people, processes, systems or external events.

Tasks:

While not compulsory, Operational Risk Management generally carries out those tasks arising from the execution of the Operational Risk framework detailed above:

- Risk Identification
- Risk Assessment
- Risk Mitigation / Control
- Risk Monitorings / Reporting

The question of independence:

The issue of operational independence is often different from Compliance functions, since there may be functions carrying out operational risk tasks which report directly into the business. Operational Risk staff can, and often are, involved in the resolution of risk issues and may be seen (depending upon the culture of the Group) as a support function as well as a control function. Nevertheless, this does not eliminate the need for ultimate independence of judgement at the enterprise-wide level.

Other:

The operational risk function and framework must be subject to internal audit.

² See also CEBS – Guidelines - 20 January 2006

5.2.3 Internal Audit

Scope: Must cover the entirety of activities carried out by the financial institution.

Role: Required by IML Circular 98/143

Compulsory Tasks:

- a three year audit plan and execution of that plan;
- management control of external experts used to assist in areas where Internal Audit does not have the necessary knowledge or experience; and
- issue recommendations, where appropriate.

Conflicting Tasks:

- may not report to a department or unit within the financial institution but to senior management;
- an auditor may not audit functions in which he has worked in the recent past; and
- may not draw up implementation plans for, or manage implementation of, controls or action plans.

Optional Tasks:

- may be consulted on matters of internal control, particularly in the light of reorganisations or the introduction of new products.

Other:

- must be an internal, independent function for the regular control of the internal control system;
- must be independent of functions audited; and
- audits must be carried out in an objective manner.

5.2.4 Special cases

The authors of this working paper summarised below the results of discussions on some specific assignments. The CSSF clarified the Internal Audit and Compliance functions but has not issued detailed guidance on the other internal control functions that may exist within Luxembourg banks. For this reason, the authors did not refer to these additional control functions but only mentioned below, as applicable, some incompatibilities. The authors believe however that each Luxembourg bank should clarify in a memorandum the function in charge of each of the assignments below, based on the various factors (resources available, the technical knowledge, etc.).

Fraud:

The Compliance function is mainly involved in this area through the provision of training etc. The actual investigation of fraud cases is usually carried out by either the Inspection or Compliance functions.

Extensive discussions took place on this subject. Based on the analysis performed, it appears that most banks consider that internal auditors have the required technical expertise to carefully review fraud cases. However, taking into account the specific risks related to these cases, the use of an expert is highly recommended. These experts have the technical and legal background to perform the related investigations. In Belgium, a specific institute was set up in 2001 –

the Institut of Forensic Auditors (asbl). The main objective of this new entity is to make sure that the specificities of fraud enquiries are fully recognised. In Belgium, in some cases, fraud enquiries are conducted by the Compliance function. In France and Luxembourg, fraud investigations are normally carried out by the Inspection function.

The members of the working group agree that each bank in Luxembourg should assign fraud enquiries to a responsible group, based on:

- the types of fraud (counterfeit bank notes, staff fraud, money laundering etc);
- the victims (internal or external); and
- the specific knowledge required to analyse the particular case.

The members of the working group highlighted the fact that specific methodologies are required to perform these enquiries.

Anti-Money Laundering :

The Compliance function is definitively involved in anti-money laundering issues, as this is explicitly mentioned in the Basel Committee texts and in the CSSF Circular. Compliance is particularly involved in the following tasks regarding anti-money laundering:

- the **adequacy of the internal organisation**, as provided in article 4 of the Law of 12 November 2004 on the prevention of money laundering;
- **training staff**, under the same obligation.

Complaints:

The Compliance function is normally consulted on client complaints which have been sent to CSSF, and those which are linked to a compliance matter. However, it's generally considered inadvisable that Compliance or Internal Audit be in charge of complaints – that is best undertaken in the operational area where the complaints arose. Compliance ensures the adequacy of responses to complaints. Internal Audit remains responsible for evaluating the adequate management of complaints. Finally, Risk Management and Compliance tend to spot trends in complaints and suggest changes to processes.

Control Monitoring:

The Compliance function is required to organise controls within the areas which are under its responsibility. However, CSSF Circular 04/155 does not require that the controls are made directly by Compliance, but permits the possibility of delegation. For instance, the 2nd or 3rd level controls regarding account opening documentation may be delegated to the department in charge of managing client files - to the extent that Compliance has previously given clear instructions on what has to be controlled, and on the measures to be taken if the file is not complete.

The periodic review of the functioning of the department may be enough to make sure that these controls are adequate. However, Compliance must make some regular checks as well, on the basis of activity reports and exception reports. Internal Audit expects that Compliance can demonstrate actual oversight of delegated controls.

Relations with the Authorities:

It is agreed that, certainly for anti-money laundering issues, Compliance is naturally in charge of relation with the relevant authorities. However, on other issues, relations with the authorities can vary according to each institution's organisation.

5.3 General Functional Differences

Basically, Compliance ensures that people and the financial institution comply with all the relevant internal and external policies, regulations and laws; Operational Risk Management draws up the financial institution's risk framework and standards as well as providing input on policies, thereafter monitoring the processes in place that could contribute to any breach; and Internal Audit provides an independent verification and risk assessment of the other two areas.

Compliance is more likely to be involved in the "before" of events, and Internal Audit "after", whereas Operational Risk Management will be involved in both.

5.3.1 Powers, delegations and access

Power

The Compliance function has no hierarchical authority on the areas which it controls but it does have the power of recommendation which can go as far as a veto, depending on the institution.

Delegation

In principle, Compliance cannot delegate to Internal Audit for the following reasons:

- Internal Audit carries out 4th level controls while Compliance carries out 3rd level controls. Since Internal Audit is responsible for evaluating the internal control set-up of an institution, it cannot carry out the 3rd level controls itself.
- Monitoring carried out by Compliance, which is of a permanent nature, cannot be delegated to a function that carries out periodic monitoring.
- Internal Audit cannot carry out monitoring for a function which it controls e.g. Compliance.

However, this delegation principle may be adjusted according to the size of the firm and complexity of the business.

It should be noted that the Compliance function may use the reports of Internal Audit, both as information and as a guideline (for instance, in detailing corrective actions). In this case, it is advisable and necessary that the Compliance Officer systematically receives reports sent by Internal Audit to the Audit Committee (or equivalent body), and be informed of any recommendation linked to a compliance matter.

Right of Access:

In addition, tests made by Internal Audit following strict norms have an actual value which are useful for Compliance. Compliance has to be in a position to request access to these tests, to the extent that an audit recommendation is related to a compliance matter.

5.3.2 Coordination and cooperation

Coordination:

If Compliance cannot delegate to Internal Audit, coordination is possible and advisable in order to establish synergies and to strengthen each of the functions. This is particularly true for “cross” proposals, in terms of audit missions on the one hand, and improving controls or procedures on the other hand.

The monitoring role of the Compliance function could be supplemented, not only by Internal Audit, but also by other control functions, such as Risk Management, Internal Control and the Complaints department.

Cooperation:

CSSF Circular 04/155 provides that contacts have to be organised through regular meetings between the Compliance and other control functions. Discussions and decisions taken during those meetings must be minuted.

Practically, in Luxembourg, the division of tasks remain strongly influenced by the history of each institution, and by the availability of the necessary competences and resources for investigations.

The coordination role mostly belongs to Compliance in order to cover all the fields where Compliance has a monitoring mission, without creating overlaps. If it's considered impossible that Compliance may delegate to Internal Audit, then it is advisable that a Compliance Officer be a member of, or invited to, the Audit Committee (or other relevant committee). In this way, weaknesses observed by Compliance could be incorporated into the Audit plan, for example.

The two functions – Internal Audit and Compliance – make use of risk assessment. In fact, Internal Audit has to use risk assessment in drawing up its Audit plan. Compliance must permanently measure the risk linked to operations, with the help of Risk Management.

Another major difference between the two functions lies in the fact that the Compliance function may sometimes intervene directly in operations, such as the approval of sensitive clients. Within some institutions, for example, the Compliance function supervises the opening of all new accounts.

The Internal Audit function has built up, over many years, a very strict methodology, based on test documentation and results, ending in formal recommendations. By contrast, in some institutions, the Compliance function is still relatively new and in the process of developing its own methodology.

It is important that Compliance controls and opinions are clearly documented and capable of audit. Indeed, Compliance is not a mere “help desk” or “breakdown” department, but the function must bring about permanent presence and firmly assert itself. In addition, in order to train an institution, Compliance opinions must be continuous and coherent.

5.3.3 Recommendations

Internal Audit and Compliance essentially have powers of recommendation.

In contrast to the Internal Audit function, Compliance may be requested not only to make recommendations, but also to coordinate (and even lead) the necessary corrective actions, as can Risk Management.

Recommendations made by Compliance – by definition – target legal, regulatory, and ethical norms. As such, they carry a higher constraint for the management than the recommendations made by Internal Audit, which – generally speaking – target an improvement of internal controls. Of course, sometimes Internal Audit recommendations are also concerned with legal norms.

Faced with a breach of a legal, regulatory or ethical provision, management has no choice but to act to correct the breach. By contrast, when presented with an Internal Control weakness, management has the choice to continue without taking corrective measures, provided there is a valid risk assessment carried out.

5.3.4 Sanctions

Compliance is sometimes consulted for its opinion regarding facts in a situation that may lead to a sanction. Of course, the right of sanction belongs to management. However, soliciting Compliance's opinion involves more than just consulting in this area – the level of seriousness of the failure is linked to the seriousness of the sanction. Of course, senior management can take into account all the elements which allow for an assessment of the individual. But once Compliance has been approached to provide an opinion on the seriousness of a failure, Compliance must use its right of investigation and gather all the facts and circumstances. As a result, its opinion may very well be decisive in the application of sanctions.

For this reason, and in order to avoid Compliance being viewed as repressive, it is quite important to qualify facts rather than individuals and to reach a high level of objectivity.

If Compliance observes serious and repeated failures through its monitoring, it might be led to directly suggest sanctions. In such case, Compliance should try to have more a training role than a repression role. Facts will be brought to the senior management for action, together with the issuance of recommendations, according to the degree of seriousness.

5.4. Functional Reporting Lines

5.4.1 General principle

CSSF Circulars state that the two functions (Compliance and Internal Audit) are independent functions. However, there is a difference in terms of reporting lines:

Compliance reports to senior management and, where necessary, has access to the Board of Directors.

Internal Audit reports directly to senior management.

On its side, Risk Management, which historically tended to be part of the Finance Department, is now emerging as a separate function and is starting to report to senior management.

5.4.2 Compliance Committee / Internal Audit Committee

Each institution is free to set-up the structure most suitable to its needs. For example, some institutions merge these two committees. Indeed, some larger institutions also have Risk Committees. These Risk Committees are often run in a similar fashion to the Compliance Committee (with a risk focus) as outlined below.

Regarding institutions of a significant size, the creation of a Compliance Committee is not only justified for its reporting of Compliance weaknesses and incidents. It is also the body which gathers people representing several parts of the internal control set-up (Legal, Risk Management, Executive Committee chairman etc) thus improving coordination and actions.

A Compliance Committee can be a useful forum, for example, for raising any difficulties met by Compliance in terms of resources and/or means. This should be reported whether or not these difficulties involve the structure of the Compliance set-up, the training, the following-up of regulatory developments, contact with external control bodies, non-compliant aspects regarding AML, ethics, other norms, etc.

The Compliance function must both centralise compliance matters and report on them. These elements, formalised in a regular report, ensures that the Compliance Committee takes corrective measures and follows up. This Compliance report should also be presented to the Executive Committee and the Audit Committee. It remains, however, that the functioning of the latter committee will, in Luxembourg, often reflect the organisation of the whole Group.

- Within some groups, there is sometimes a Compliance Committee at the Group level. The reports requested by the parent company's Compliance Officer normally formalises the information necessary to the management of the compliance function on a Group-wide basis. In addition to this reporting, the Compliance Officer of each subsidiary should make his own annual report for this Compliance Committee, about the subsidiary. In fact, it is important that some topics are discussed at the Committee level – for example, the question of resources and means attached to the Compliance function, especially during the function's set-up.
- Theoretically, when the Compliance function wants to involve Internal Audit on a specific issue, it should go through the Compliance Committee (or the Audit Committee acting as Compliance Committee).

In reality, the best practice is that Internal Audit consult Compliance before drawing up its annual audit plan. Then, Internal Audit can check the possibility of including specific reviews or important control items at

Compliance's request, within the limits of its resources, and of its own risk assessment.

At any time, such suggestion might be made by Compliance but, of course, Internal Audit retains the authority to follow the suggestion or not.

Within each institution represented on the working group, the hierarchy and the functional links of the three functions are specific to each organisation. The Compliance and Internal Audit functions are necessarily separated, following CSSF Circular 04/155, however they are sometimes supervised by a common, coordinated body. In such cases, it is recommended to obtain approval from the CSSF for this approach.

In the past, Internal Audit has often covered part of the areas now included under the Compliance function, as well as taking a role in the field of fraud prevention and investigation. It is therefore advisable that the missions of the Compliance and Internal Audit functions include reviews of the Inspection missions.

5.4.3 Functional Reporting

Where an issue arises across functions, e.g. a case of fraud with Compliance and Operational Risk implications, it can be that Internal Audit would write the ultimate report but with the independent review of Compliance and Operational Risk.

6. Conclusion

The defined responsibility of Compliance to “identify and assess the compliance risk of an institution, as well as to assist senior management in managing and monitoring this risk” is clear, while the manner in which this is achieved is left to interpretation. Some financial institutions see this as a day-to-day control and advisory role related to the need “to conduct its business in accordance with the rules in force.” Others believe that in order to achieve this, greater involvement in the operational processes and environment that can contribute to failures is integral to an effective function.

In parallel, in some financial institutions, Operational Risk reporting to executive management is in charge of coordinating the Risk Framework, with some of the tasks belonging to the four processes being delegated to other units. In other financial institutions, Operational Risk, located within the business lines or with local oversight and reporting to senior management, can perform specialist Operational Risk controls.

This diversity prevents the authors from prescribing one or other solution. From the review performed, it appears that the following responsibilities can be allocated:

- Compliance to ensure that the rules in force to which the financial institution is subject are identified, policies and procedures adapted to norms, and control performed to ensure that the latter are applied.
- Risk Management to assess that the magnitude of the risk arising from non-compliance is assessed, in conjunction with other Legal and Operational risks, and to ensure that the executive management is regularly provided with an overall view of the risk profile of the financial institution encompassing both Financial and Operational risk.
- Internal Audit to ensure that the overall control, compliance and risk framework of the financial institution is adequate and effective.

However, in terms of internal organisation, financial institutions should have the discretion to define the optimum approach within the constraints of existing Circulars to allow them to best perform the three levels of controls described in IML Circular 98/143.

Finally, there should be efficient communication between each of the three functions. Such communication should be aimed at coordinating work, consultation when setting recommendations, and informing each other of the result of investigations. This coordination should be reflected in reports to senior management and the board of the institution.