

Designing a Comprehensive Compliance Risk Management Framework

By

Kenneth L. Bryant

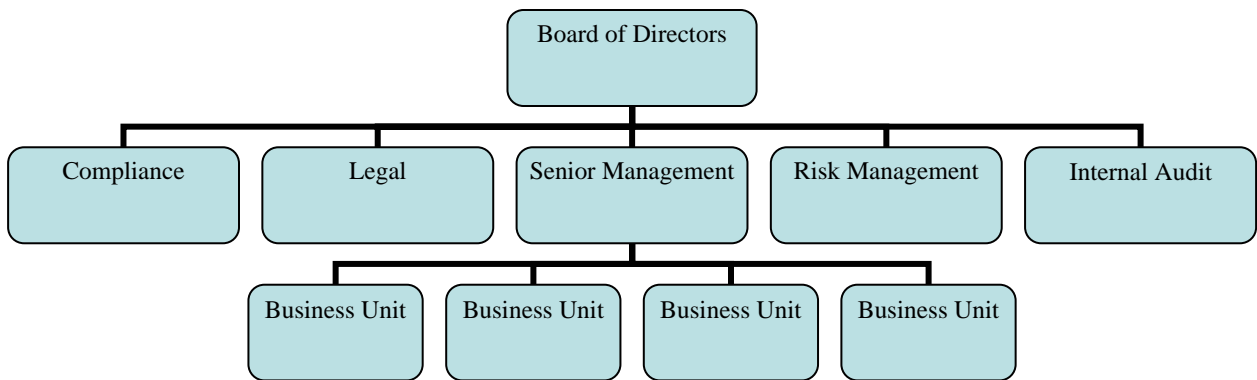
MSCJ, CPP, CFE, CRP, CAMS, ACoI

www.amlcft.com

June 2004

With the advent of several corporate and financial industry scandals over the past few years, there has been an increased focus on the need for effective internal controls. In order to ensure compliance and prevent breaches, a Financial Services Provider (FSP) should consider adopting a comprehensive compliance risk management framework. Best practices and the predominant thinking in the field is that such a risk management framework consists of at a minimum the following four internal control functions: Internal Audit, Legal, Risk Management, and Compliance.¹ The roles of each of the respective functions along with the Board of Directors, Senior Management, Compliance Staff and Business Unit personnel, all have a part to play in contributing to the overall success of the four internal control functions as they form an effective and comprehensive compliance risk management framework.

A suggested organizational structure of the four internal controls functions and their relationship to the rest of the organization is illustrated in the following diagram:



In this model, the information flows would be from “top down,” “side to side” and to “bottom up” as appropriate along structural lines. In general, the internal controls functions are “auxiliary” to Senior Management (“staff”) and each other and directly report to the Board of Directors, who are ultimately responsible for the compliance risk management framework.^{2,3,4} It should be noted that under the proposed structure, the internal control functions are on par, and are placed at the highest senior management level in the organization. This gives the internal control functions the necessary prominence and stature in the organization and designates to all personnel their importance. For the purposes of day to day operations, the four internal control functions should report to senior management (e.g. Managing Director) but have access to the board when an appropriate issue arises as well as for quarterly, semi annual, and annual reporting. This structure provides the necessary support to the internal controls functions within the organization to accomplish critical tasks. The individual business units represent the “line” function of the organization. It is useful to examine the suggested typical duties and responsibilities of each of the above functions in turn: Board of Directors, Senior Management, Business Unit, Internal Audit, Risk Management, Legal, and Compliance.

The Board of Directors should have responsibility for approving and periodically reviewing the overall business strategies and significant policies of the FSP; understanding the major risks run by the FSP, and setting acceptable levels for these risks.⁵ “The Board of Directors is ultimately responsible for ensuring that an adequate and effective system of internal controls is established and maintained.”⁶ Given the increasing nature of the emphasis placed on the Board of Directors for effective corporate governance, the creation of a separate audit committee without proper board involvement may well cause problems.^{7,8,9} The fear is that there will be a natural tendency for the Board of Directors to delegate away too much power, authority and decision making to the audit committee. Although Non-Executive or External Directors (independent from the daily management of the FSP) can “enhance independence and objectivity” there should be a primary concern that such Directors “are not overextended” and “avoid conflicts or interest in their activities with, and commitments to, other organizations.”¹⁰ It is particularly helpful if Non-Executive Directors possess financial services experience, and/or expertise in financial reporting and internal controls.¹¹ The Board of Directors should ensure “that Senior Management takes the steps necessary to identify, measure, monitor, and control these risks” and ensure “that Senior Management is monitoring the effectiveness of the internal control system.”¹² In the final analysis, the Board of Directors “provides governance, guidance and oversight to senior management.”¹³

“Senior Management should have responsibility for implementing strategies and policies approved by the Board of Directors; developing processes that identify, measure, monitor and control risks incurred by the bank; maintaining an organizational structure that clearly assigns responsibility, authority and reporting relationships; ensuring that delegated responsibilities are effectively carried out; setting appropriate internal control policies; and monitoring the adequacy and effectiveness of the internal control system.”¹⁴ Senior Management should assume an oversight role with respect to the various line managers and their respective business units.¹⁵

In addition to the mandate of carrying out the day to day operations of the FSP, Business Units should be responsible for ensuring compliance amongst all line personnel. From a compliance risk management framework perspective, typically this is the objectives and internal and external rules of the compliance function pertaining to the regulatory obligations of identification, monitoring, training, reporting and recordkeeping. Best practice would be for the FSP to establish a “Compliance Handbook” to outline, prescribe and establish the above compliance objectives, rules, policies and procedures.¹⁶ From experience, care must be taken for FSPs to avoid the common mistake of creating a stand alone compliance manual or a section in an operations manual that is not cross referenced to “the various procedures that must be applied throughout” an FSP.¹⁷ This is often a review comment of Federal Reserve Board (FRB) Examiners. Without this roadmap, Business Units will find it difficult to apply compliance procedures to the daily activities conducted by line personnel which often serve as the first line of defense in the internal controls process.

Adequate internal controls within FSPs should be supplemented by an effective internal audit function that independently evaluates the control systems within the organization by conducting detailed testing.¹⁸ Typically, this internal control function is carried out by Internal Audit. In addition, “there should be an effective and comprehensive internal review of the internal control system carried out by operationally independent, appropriately trained and competent staff.”¹⁹ However, the value of external auditors, on the other hand, can provide an important feedback on the effectiveness of this process.²⁰ With respect to the detection of money laundering (as compared to breaches of compliance), it should be noted that in January 2002, the International Federation of Accountants published a discussion paper on anti-money laundering in which it explains why money laundering is unlikely to be detected in the context of a financial audit. Since most money laundering methodologies do not involve the type of fraudulent activity (e.g. misappropriation of assets) that is likely to effect financial statements, accountants are never likely to detect an instance of money laundering within the confines of generally

accepted accounting standards and practices. Moreover, the Association of Certified Fraud Examiners released a report on fraud in 2002 and discovered that incidents of fraud were detected more often by mere chance than by internal audit teams conducting financial audits. Thus, Internal Audit has limitations (as recent corporate industry scandals have pointed out) and as a result should be only one of the internal control functions. This also serves to point out the importance of Internal Audit conducting operational audits as well as financial audits. Since the Internal Audit function should not be directly responsible for operational risk management,²¹ Risk Management was purposely delineated as a separate function in the above proposed organizational diagram.

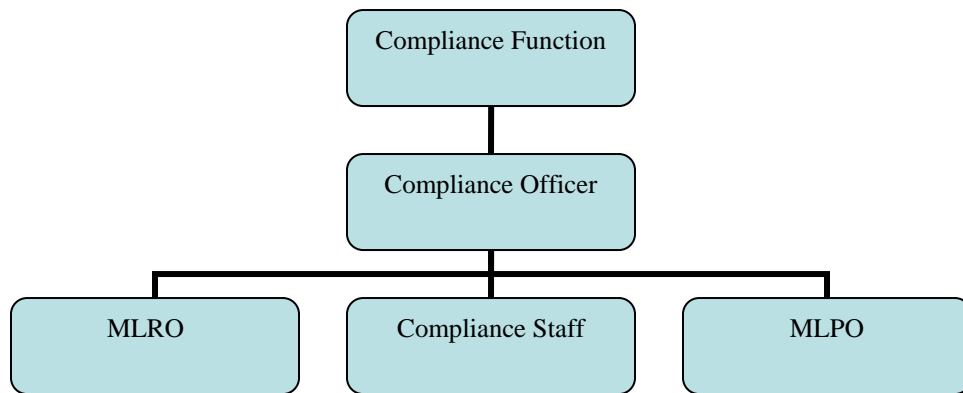
The importance of a risk based approach can not be understated from either a resource allocation or prioritization point of view. To that end, Risk Management becomes a critical function in the internal controls process. As such, the Risk Management function should aim to “integrate fully the management of risk into the business culture and practices.”²² It does this by identifying risks (e.g. types of clients, accounts, products and service lines), quantifying risks, prioritizing risks, managing risks, monitoring risks and then “advises on reporting systems and controls to minimize the risk” and provide for future early warning.^{23,24}

“The in-house legal function is responsible for implementing a coherent approach to the management of legal risk” within the FSP.²⁵ Legal should perform audits and identify risk associated with agreements, contracts, lawsuits, adverse judgments, and regulatory enforcement. Legal should routinely advise Senior Management and the Board of Directors on the significance of legal risks facing the FSP and suggest possible remediation measures for mitigation.

Lastly, and most importantly, we come to the Compliance function. The compliance function should facilitate the implementation and maintenance of the compliance culture, arrange for or provide compliance training, advise on regulatory matters, conduct

monitoring, maintain lines of communication with the regulator, handle regulatory issues, conduct reviews, provide reports and guidance to management, assist in identifying, assessing and managing regulatory risk, manage internal, external and inter-relationships, and turn regulatory burden into competitive advantage (e.g. such as recommending IT solutions which in some cases may be the only way for an FSP to effectively comply with local legislation, regulation and guidance).^{26,27,28} In general terms, the inter-relationships for the Compliance function are: the Board of Directors has the responsibility for overseeing the management of the compliance function;²⁹ Senior Management is responsible for establishing a compliance policy and a permanent and effective Compliance function;³⁰ Legal provides legal guidance to the Compliance function; Risk Management impacts and provides input to the risk based approach the Compliance function takes; and the “Compliance function should be subject to periodic review” by Internal Audit.³¹

A suggestion relationship and organizational structure for the Compliance function can be observed in the following diagram:



The delineation of the Money Laundering Reporting Officer (MLRO) and Money Laundering Prevention Officer (MLPO) as separate job functions reporting to the

Compliance Officer is based on experience where in most average sized FSPs Compliance Officer duties and obligations are ever increasing and as such the Compliance Officer can no longer effectively manage the workload. We will look at each of the four positions in turn: The Compliance Officer, the MLRO, the MLPO, and the Compliance Staff.

The Compliance Officer should serve as the Head of Compliance and should be “responsible for the day-to-day management activities of the compliance function.”³² The Compliance Officer position should be responsible for overseeing all types of regulatory compliance and not necessarily those involving anti-money laundering or combating the financing of terrorism. This is a more comprehensive approach consistent with developing international practice (e.g. advertising and investment rules pertaining to insurance, securities investment, and mortgage markets in the US and UK).

The MLPO was added to the suggested organizational structure because certain jurisdictions are beginning to impose a requirement for this specific position and because the position itself has taken on specialist importance internationally.³³ The MLPO should have oversight over all activity specifically related to anti-money laundering and combating the financing of terrorism.

The MLRO has long since been required by most offshore jurisdictions such as Cayman. The MLRO should specifically deal with the receipt of internal unusual activity reports, evaluate, investigate and substantiate them, make external suspicious activity or transaction reports as necessary, keep required files, logs and registers, provide management information on reporting trends, supporting the regulatory visit and inspection process, keep abreast of new and emerging money laundering typologies, provide input to training, and serve as the point of contact for law enforcement, the financial intelligence unit and the regulator concerning disclosures and requests for information.^{34, 35} An often unrealized and underutilized value to the FSP of the MLRO is

the analysis of under, over and defensive reporting along with feedback to staff on the current patterns and trends of money laundering and terrorist financing.

Compliance staff should simply assist in the support duties for the compliance function personnel as required by the needs of the FSP (size dependent). This may either be the Compliance Officer, the MLRO and/or the MLPO. Typically, this may be reviewing files, assisting in compliance monitoring, and assembling information for reports, etc. “Staff exercising compliance responsibilities should have the necessary qualifications, experience and professional and personal qualities to enable them to carry out their duties effectively.”³⁶ Moreover, the Guidance Notes for the Cayman Islands specifically state that the MLRO (Compliance Officers and MLPO’s are not statutorily required in Cayman) should be “a suitably qualified and experienced person” and “it is generally expected that the MLRO would be a senior member of staff carrying out a Compliance, Audit or Legal role within the Financial Services Providers' business.”³⁷ This standard for the MLRO should equally be applied to the Compliance Officer and MLPO positions. From observation, identifying such a candidate has been a problem for FSPs in Cayman and Cayman Islands Monetary Authority (CIMA) personnel have repeatedly commented on this. It appears this is a recurring problem, especially in the Caribbean Region where the compliance function is relatively new on the world scene in a formal sense. An FSP should endeavor to attract, recruit and hire compliance staff with the appropriate seniority, background, experience and qualifications for the specific position they will hold within the Compliance function. As Andrew Newton rightly points out, “the compliance role is not a job for amateurs.”³⁸

An area of concern for the Compliance Officer and MLPO positions in terms of duties and responsibilities is where the FSP must be careful not to allow the organization to delegate compliance production work to the Compliance Officer and/or MLPO. This is especially true with smaller institutions where the Compliance Officer or MLPO is often seen conducting due diligence on files. It is important to note that it is a fundamental

precept that a Compliance Officer and/or MLPO should never be placed in a position to review their own work (similar to the principle of dual control).

In conclusion, “there are two distinct elements to every effective and comprehensive compliance risk management framework. The first is the creation of the framework itself” and the second is the creation of a compliance culture.³⁹ The first distinct element has been addressed in this paper with a particular sensitivity to the prominence, stature, support, professional qualification and workload distribution necessary for the compliance function to be successful. However, experience has shown that the creation of an effective compliance culture is far more difficult and indeed may overshadow the very framework itself. For this reason, it is critical that “the Board of Directors and Senior Management are responsible for promoting high ethical and integrity standards, and for establishing a culture within the organization that emphasizes and demonstrates to all levels of personnel the importance of internal controls. All personnel at a banking organization need to understand their role in the internal controls process and be fully engaged in the process.”⁴⁰ In fact, history has shown that without an effective compliance culture, a comprehensive compliance risk framework could easily be rendered ineffective.

Word count: 2384

¹ The Handbook of Compliance: Making Ethics Work in Financial Services, Andrew Newton, p. 78. For simplistic purposes and for practical reasons of length, I have excluded Credit (or Concentration Risk per the Basel Customer Due Diligence Paper) although I do acknowledge it as per pages 160 and 267 in the ICA Course Book. All others I consider related to Operational or Reputational Risk and excluding System or Jurisdictional risk as it is not relevant for our purposes here in terms of an internal compliance risk management framework.

² ICA Course Book Appendix 22: Basel Committee on Banking Supervision – The Compliance Function in Banks, p. 658

³ ICA Course Book Appendix 3: Basel Committee on Banking Supervision – Framework for Internal Control Systems in Banking Organizations, p. 60

⁴ The terms “auxiliary,” “staff” and “line” are used in the organizational sense.

⁵ ICA Course Book Appendix 3: Basel Committee on Banking Supervision – Framework for Internal Control Systems in Banking Organizations, p. 60

⁶ Ibid. pp-60-61.

⁷ ICA Course Book Appendix 12: OECD – Principles of Corporate Governance

⁸ ICA Course Book Appendix 15: Basel Committee on Banking Supervision – Enhancing Corporate Governance for Banking Organizations

⁹ U.S. Sarbanes-Oxley Act

¹⁰ ICA Course Book Appendix 15: Basel Committee on Banking Supervision – Enhancing Corporate Governance for Banking Organizations, p. 474

¹¹ Ibid. p. 475

¹² ICA Course Book Appendix 3: Basel Committee on Banking Supervision – Framework for Internal Control Systems in Banking Organizations, p. 60

¹³ Ibid. p. 61

¹⁴ Ibid. p. 62

¹⁵ ICA Course Book Appendix 15: Basel Committee on Banking Supervision – Enhancing Corporate Governance for Banking Organizations, p. 475

¹⁶ ICA Course Book, Module 6: Designing an Internal Compliance System, p. 158

¹⁷ ICA Course Book, Module 6: Designing an Internal Compliance System, p. 159

¹⁸ Basel Committee on Banking Supervision - Internal Audit in Banks and the Supervisor's Relationship with Auditors, August 2001

¹⁹ ICA Course Book Appendix 3: Basel Committee on Banking Supervision – Framework for Internal Control Systems in Banking Organizations, p. 71

²⁰ Basel Committee on Banking Supervision - Internal Audit in Banks and the Supervisor's Relationship with Auditors, August 2001

²¹ ICA Course Book Appendix 4: Basel Committee on Banking Supervision - Sound Practices for the Management and Supervision of Operational Risk, p. 90

²² The Handbook of Compliance: Making Ethics Work in Financial Services, Andrew Newton, p. 78.

²³ Ibid.

²⁴ ICA Course Book, Module 11: Risk Management, p. 271

²⁵ The Handbook of Compliance: Making Ethics Work in Financial Services, Andrew Newton, p. 78.

²⁶ Ibid. pp. 75-76

-
- ²⁷ ICA Course Book, Module 4: The Role of the Compliance Officer, p. 58
- ²⁸ Ibid. p. 63
- ²⁹ ICA Course Book Appendix 22: Basel Committee on Banking Supervision – The Compliance Function in Banks, p. 658
- ³⁰ Ibid. pp. 658-659
- ³¹ Ibid. p. 664
- ³² Ibid. p. 663
- ³³ ICA Course Book, Module 7: Managing the Risk of Money Laundering and Terrorist Financing, p. 193
- ³⁴ Ibid. pp.-194-195
- ³⁵ Cayman Islands Monetary Authority, Guidance Notes of the Prevention and Detection of Money Laundering in the Cayman Islands, September 2003, pp. 42-43, 49
- ³⁶ ICA Course Book Appendix 22: Basel Committee on Banking Supervision – The Compliance Function in Banks, p. 663
- ³⁷ Cayman Islands Monetary Authority, Guidance Notes on the Prevention and Detection of Money Laundering in the Cayman Islands, September 2003, p. 39
- ³⁸ The Handbook of Compliance: Making Ethics Work in Financial Services, Andrew Newton, p. xv.
- ³⁹ ICA Course Book, Module 6: Designing an Internal Compliance System, p. 160
- ⁴⁰ ICA Course Book Appendix 3: Basel Committee on Banking Supervision – Framework for Internal Control Systems in Banking Organizations, p. 63