

The Compliance Officer's Role in Risk Management: Insurance, Credit Unions, Gaming Board, Accountants, Lawyers etc.

By

Tanya C. McCartney

**Immediate Past- President, Bahamas Association of Compliance Officers
Regional Manager, Compliance (Retail Banking), RBC Royal Bank of Canada**

Friday, May 18th, 2007

BIFS Annual Week of Seminars

SALUTATIONS:

Good afternoon, it is certainly a pleasure to have been given the opportunity to make a presentation this 2007 annual Week of seminars hosted by the Bahamas Institute of Financial Service as the immediate past president of the Bahamas Association of Compliance Officers. I trust that you who are not members of BACO will complete membership forms and become active members.

I can honestly say that I look forward to interacting with you my colleagues in this setting. Hopefully I will leave you with more answers than questions

I have been asked to speak on the topic: ***The Compliance Officer's Role in Risk Management***

In my role as a Regional Manager for Compliance at The Royal Bank of Canada I must ensure not only that risks associated with financial services are mitigated with respect to my institution but that the reputation of The Commonwealth of the Bahamas as a premier financial services centre remains in tact. At the end of the day this is spirit of what we refer to as Compliance. Our role as compliance

professionals is to mitigate, that is to limit and minimize risks associated with the business that our employers offers in the financial services market place. Our role is to mitigate **“compliance risks”** a term that I will define a little later on.

From the outset it should be made clear that financial services are about so much more than banks and trust companies. Yes, it is. Just look at how these seminars and the Institute have evolved. It started as Bankers Week and the Bankers Institute. We now speak of the Bahamas Institute of Financial Services and its week of seminars. On behalf of BACO I wish to commend Mrs. Kim Bodie and her hardworking team of professionals.

So then,

Now to the topic at hand: “The Compliance Officer’s Role in Risk Management”. The first thing we must look at is the context within which compliance officer’s function – namely financial services and financial institutions.

WHAT DO WE MEAN BY A FINANCIAL INSTITUTION?

When we use the term “Financial Institution” traditionally we tended to think only of banks or trust Companies, however today we see that there are no longer just the traditional Financial Institutions but there are the non- traditional financial institutions. This concept has been broadened over the years and indeed some of the principles that originally only applied to banks have been developed to apply in a broad sense to “financial institutions”.

As, I am certain you all well now Under Sec 3(1) of the **Financial Transactions Reporting Act** the term “financial institution” includes any of the following:

1. **Bank** – a bank or trust company, being a bank or trust company licensed under the Banks and Trusts Companies Regulation Act 2000

2. **Insurance** Company– a company carrying life assurance business as defined in section 2 of The Insurance Act
3. **Casino** – a licensed casino operator within the meaning of the Lotteries and Gaming Act.
4. **A broker-dealer** within the meaning of section 2 of the Securities Industry Act;
5. **A real estate broker, but only to the extent that the real estate broker receives funds in the course of that person’s business for the purpose of settling real estate transactions** (Recently The Bahamas Real Estate Association expressed a desire that they be exempt from KYC due diligence verification requirements on clients who pay deposits for property transactions that are 10% or less than the purchase price. Currently being considered by parties concerned);
6. **A trustee or administration manager** or investment manager of a superannuation scheme;
7. **A mutual fund administrator** or operator of a mutual fund within the meaning of the Mutual Funds Act, 1995;
8. **Any person whose business** or a principal part of whose business **consists of** any of the following, **inter alia** -
 - (i) **borrowing or lending or investing money,**
 - (ii) **administering or managing funds on behalf of other persons,**
 - (iii) **acting as trustee in respect of funds of other persons,**

- (iv) dealing in life assurance policies,**
 - (v) providing financial services that involve the transfer ...**
9. **A counsel and attorney, but only to the extent that the counsel and attorney receives funds in the course of that person's business -**
- (i) for the purposes of deposit or investment,**
 - (ii) for the purpose of settling real estate transactions; or**
 - (iii) to be held in a client account;**
10. **An accountant, but only to the extent that the accountant receives funds in the course of that person's business for the purposes of deposit or investment.**

Indeed, a very broad definition is given to financial institution under the law and in the context of Anti-Money Laundering and the Counter - financing of Terrorism

Legal Recognition of the Compliance Function

The statutory footing for the role of compliance is found in the Financial Intelligence (Transactions Reporting) Regulations 2001. Regulation 5(e) where it states that:

“1) A financial institution shall institute and maintain internal reporting procedures which include reporting provision procedures.

identifying and appointing a senior officer as a compliance officer who shall ensure that a regulated institution is in full compliance with the laws of the Bahamas.

It is noteworthy that The Basle Committee on Banking Supervision in April 2005 issued a high level paper on compliance and the compliance function in banks. It basically outlined that banking supervisors must be satisfied that effective compliance policies and procedures are followed and that management takes appropriate action when compliance failures are identified. This emphasizes the importance of the compliance function.

All financial institutions, as previously defined, must have a compliance officer.

Let us then for a moment consider this in a little detail,

**WHAT EXACTLY DO WE MEAN BY COMPLIANCE? IS THERE
REALLY A DEFINITION?**

The term compliance appears to have originated in the United States, referring to the need to comply with the 1930s securities laws that were enacted there. Within the United Kingdom, the term compliance first appeared around 1985 when the Financial Services Bill was proceeding through parliament, to be enacted in 1986 and eventually coming into force in 1988 as the Financial Services Act.

Financial Services firms began to realize that this new legislation would have a significant impact upon their various operations. The more far-sighted senior management identified executives to review this impending legislation in order to understand what it would mean for their business.

For those pioneer UK compliance officers, as they quickly became known, this role was focused initially, largely upon understanding the new legislation, the new regulations of the various Self Regulatory Organizations and in particular obtaining authorization for their firm. In the same way, here in the Bahamas, the compliance function has evolved as a result of legal and regulatory developments.

What then are the Core responsibilities of the compliance function as it relates to financial services?

Well, Compliance professionals:

- Ensure that a regulated institution is in full compliance with the laws of the Bahamas
- May serve as Money Laundering reporting officer
- Ensure that the financial institution complies with its own internal controls, policies and procedures
- Advise on legal and regulatory developments
- Train staff
- Vet Documentation (account opening etc.) to ensure adherence with legal and policy requirements;
- Lead in the AML and Anti-Terrorist Financing Fight
- Serve as a Link between Regulators and Institution
- Serve as a Link Between the Business and external legal Counsel
- Ensure that anti-fraud arrangements are in place
- Ensure that corporate governance requirements are adequate.
- Monitor and Manage “Compliance Risk”. Compliance risk has been defined as:

the risk of legal or regulatory sanctions, financial loss, or damage to reputation and franchise value that arises when a financial institution fails to comply with laws, regulations or the standards or codes of conduct of self regulatory

organizations applicable to its business activities and functions.

That is certainly a lot, and this list is not exhaustive, AS MANY OF YOU KNOW FULL WELL.

Ladies and Gentlemen, colleagues:

Traditionally compliance was seen as having solely an Anti-Money Laundering focus, however today we see that Compliance is not **ONLY AML COMPLIANCE** but it encompasses what I refer to as **REGULATORY COMPLIANCE**. In fact, AML Compliance may very well be embodied in this concept of REGULATORY COMPLIANCE.

What do we mean by AML Compliance?

Our local Framework for ensuring AML Compliance, unlike the UK for example which has the FSA (Financial Services Authority) is spread among many regulators. These regulators include:

- **The Central Bank of the Bahamas** – regulates its Licensees namely banks and Trust Companies
- **The Securities Commission of The Bahamas** – powers to regulate the securities market
- **The Compliance Commission** – statutory authority responsible for enforcing compliance with the anti-money Laundering rules and regulations FOR THE NON-TRADITIONAL FINANCIAL INSTITUTIONS;
- **The Registrar of Insurance** – regulates and supervises entities and persons involved in the insurance industry

- **The Inspector of Financial and Corporate Service Providers** – regulates companies engaged in the provision of financial and corporate services
- **The Gaming Board** – responsible for the licensing and regulating of casinos which are FI for the purposes of AML/CFT Supervision in The Bahamas; **and**
- **The Financial Intelligence Unit** – an agency responsible for receiving, analyzing obtaining and disseminating information which relates or may relate to the proceeds of offences under the proceeds of crime act 2000.

Although there is the Group of Financial Services Regulators which collaborates we have no single super-regulatory body. AML Compliance is about ensuring adherence to our AML laws, regulations, guidelines and best practice. But we will all admit that this is only one aspect of compliance. The other facet of compliance is what I refer to as:

REGULATORY COMPLIANCE

Now let us consider the concept of Regulatory Compliance. Today, we must take a holistic approach to the management of compliance risks because money laundering is not the only activity that poses a risk to a financial institution.

You may ask yourself what is Regulatory Compliance and additionally what does this term entail? When I speak of RC I am focusing on what some financial institutions refer to as an Enterprise Compliance Management Program (ECMP). It is a concept introduced by many large multi-jurisdictional FIs to deal with compliance matters, and designed to minimize or avoid compliance risks.

To use the words of Federal Reserve Governor Mark W. Olson in the context of banks but which can be equally as useful to all types of financial institutions:

“Because of the nature and levels of risks inherent to their business activities, complex banking organizations should have in place a compliance-risk management framework that makes it possible to identify, monitor, and effectively control the compliance risks facing their entire organization. Of course, such a framework needs to be commensurate with the nature and level of the organization's compliance risk. It should evolve with the ever-changing product lines and business activities of any growth-oriented organization. And, of course, it needs to stay on top of regulatory developments.”

End of quote

Colleagues,

A successful compliance-risk management program starts at the top of the organization; and

A sound and effective enterprise-wide compliance-risk management program has strong board and senior management oversight.

What elements are likely to fall within such an Enterprise Compliance Management Program, you may ask? There are 8 key components for the proper management of compliance risks, in my view.

1. Liaison with Regulators

Firstly, Compliance serves as the liaison to maintain positive relationships with regulators by providing key points of contact. Relationship management include:

- (a) Responding to regulator requests for information; and
- (b) Responding to specific examinations or other on-site activities

2. Risk Assessment

Secondly, The approach to financial services is largely risk based. Identifying the risks associated with the business and putting controls in place to mitigate those risks. Hence, Regulatory compliance involves the risk assessment of applicable Regulatory Requirements associated with the FIs business activities and the ongoing maintenance, knowledge and documentation of applicable Regulatory Requirements. What regulations pose the most serious risk for the financial institution if not complied with?

The business must clearly understand their role in owning risk management, including compliance risk. The Compliance function should partner with the business units to ensure adequate compliance risk mitigation.

3. Control Design and Oversight

Thirdly, this is a fancy way of saying drafting and ensuring implementation of policies and procedures. Yes, this is a key element in sound compliance risk management.

4. Training and Education

Fourth on my list - Training and Education: Compliance must ensure that there is a documented process to ensure that employees have the skills and knowledge they need to manage compliance risk effectively. This involves the initial and ongoing training of new employees. Such training should be customised for the roles and responsibilities of the employees. Records of who have completed training should be kept.

5. Compliance Execution

Fifth, It is not enough for the compliance function to ensure that policies and procedures are in place which are consistent with the legislative and regulatory regime. There is a crucial next step – compliance execution. This involves:

- o Day to day controls to manage compliance with regulatory requirements at the business level;
- o Policies, procedures, processes and appropriate compliance staffing in all operations;
- o The fulfillment of action plans created to address identified Compliance Issues;
- o The referral to head office (where applicable) of any situation where the FI is unable to immediately meet a Regulatory Requirement.

6. Monitoring and Testing

Sixth on my list - Monitoring and Testing: The goal posts continue to change. International pressures, new laws and new risks dictate continued monitoring. This involves the Continuous review of the operation of controls to mitigate Regulatory Risk in the context of a financial institution. Monitoring is the means of identifying and communicating compliance breaches to the appropriate points within the organization.

Independent testing should be conducted to verify that compliance-risk mitigation activities, including training and internal controls, are in place and functioning as intended throughout the organization.

7. Issue Tracking

Seventh – Issue Tracking, Compliance cannot be seen as dropping the ball. The Compliance Function entails remaining on top of live issues (such as Regulatory Recommendations and Internal Audit findings) until their favourable resolution.

Issue tracking which involves the tracking of action plans, from initiation to resolution.

8. Reporting

The last element to a holistic enterprise wide compliance concept is – reporting. At the core of Compliance is ensuring good corporate governance. Ultimately Compliance ensures that the mind (the Board of Directors) of the financial institution is privy to all relevant information to make sound decisions and has the necessary information to make accurately informed decisions. Information regarding regulatory risk issues should be presented to the necessary operating committees, senior management or the Board of Directors formally and on a regular basis.

These eight (8) elements comprise a sound compliance management program and facilitate the mitigation of compliance risks and other risks associated with the business.

Well then let us focus in briefly on,

WHERE AND HOW DO COMPLIANCE AND RISK MANAGEMENT PRECISELY INTERSECT?

There are different types of risk as you are all aware. As previously mentioned, the compliance professional is charged with managing “compliance risk.

Hence, compliance professionals must ensure that systems, policies, procedures and internal guidelines are in place to avoid ***of legal or regulatory sanctions, financial loss, or damage to reputation and franchise value.*** This however is not the sum total of all risk that must be managed in a

financial institution – as I alluded to earlier. Each unit in a financial institution poses unique risks. Hence, we must ask – how does compliance fit in to the general or overall risk management function in an institution?

Ladies and Gentlemen,

Quite honestly, the lines tend to be rather gray in some instances surrounding the role of compliance and the role of the risk management function. In fact in some institutions this function is merged and in others it falls under two separate units. I have worked in institutions where both approaches have been taken. Is one better than the other? Is there a right way and a wrong way? There are differing schools of thought.

Bill Sharon, CEO and Founder of Strategic Operational Risk Management Solutions (SORMS) put it this way in an article entitled ***Operational Risk Management: The difference between risk management and compliance:***

“The Operational Disciplines which support a business...(IT, HR, Finance, Legal) all have professional standards, are benchmarked by best practice and are subject to laws and regulations that govern their activities in part or in whole. Comparing the level of adherence to these regulations, laws and best practices is an essential compliance activity...”

He goes on to state;

“Risk management has the responsibility of coordinating all of the risk assessments of all the operational disciplines (IT, HR, Finance, and Legal) along with options to address the identified issues... Risk management is about assessing both quantitatively and qualitatively the opportunity for success of the business initiatives. It is composed of methodologies and

processes which are designed to develop information critical to achieving the strategic objectives of the organization...

The Compliance function is essential to ensure that those methodologies and processes are being followed in the manner intended. Merging the two together essentially means that there is no oversight of the risk management function. Losing the compliance function in an activity that has become as complex as risk management is not an acceptable outcome.”

What lessons can we take from this? What conclusions can we draw?

1. **Risk management** is about devising the best plan to achieve business objectives. Best meaning – the plan that does not expose the institution to loss (financial, reputational or otherwise), damage or regulatory sanction – that will yield the desired results for the financial institution or business. It is not only about identifying all the things that could go wrong but requires a solid understanding of the business and all the things that need to go right for success of the business; and
2. **Compliance** is about ensuring that the institution stays on plan and achieves its business objectives in accordance with the rules set out in various laws, regulations and policies that apply to the business – avoiding or limiting exposure to compliance risks.
3. **Compliance and Risk Management intersect** – and are not mutually exclusive.

Risk Management draws the map, identifying risk indicators and assessing the level of those risks. Risk management in the broad sense outlines what the safest and most efficient route is to achieve the desired result. **Compliance is the backseat drive** that ensures that the business – the driver stays on the right

course and does not fall foul of the rules, take a detour that could lead to regulatory sanction, reputational damage or get lost along the way to its destination of achieving business objectives which tend to be heavily financial and bottom line focused in our profit driven world.

CONCLUSION

Risk Management is about assessing all the things that must go right and considering all those things that may go wrong and putting a plan or measures in place to minimize the exposure of the financial institutions – whether it is a bank or a real estate company, insurance company, casino, credit union, accounting or legal firm.

Compliance has the equally awesome task of ensuring that once the risks to avoid have been identified and business objectives put in place that all parties concerned adhere to that plan in a manner consistent with legal and regulatory requirements.

Compliance has an important role to play in risk management. Although the business owns the risk, and is ultimately responsible for determining its risk appetite: Compliance must always be the watchful eye reminding of the laws, regulations internal policies and controls to ensure that the strategic objectives of the business are met but always within the legal parameters.

I am now open to your questions and comments. **The end...**