GLOBAL riskupdate
The quarterly independent risk review for banks and financial institutions worldwide
Q4 2014

Financial Crime Compliance:

A Brief Guide for Senior Bank Management, Compliance Officers and Internal Auditors

Also in this issue

- HR & Risk Management
- Derivatives: Limiting Market Change
- NEW BIS Bank Corporate Guidelines
- The Implications of Climate Change
- Client Money: Don't Be in a Bad Place
- The Value and Management of Intellectual Property, Intangible Assets and Goodwill
- MoneyScience Interviews Dennis Cox

Financial Crime Compliance:

A Brief Guide for Senior Bank Management, Compliance Officers and Internal Auditors

Recent events and penalties have resulted in Financial Crime moving to the forefront of financial industry concerns and this poses particular challenges for Senior Management, Compliance Officers and Internal Auditors who are all struggling to come to terms with this 'monster.' The author is currently engaged in a global AML CDD compliance project for a major bank.

Gamechangers

For a very long time banking was all about the extension of credit in one form or another—and thus a borrower's ability to repay. Regulators had guidelines for both capital and liquidity but within the industry these were only of secondary importance to the decisions on credit.

Then came the financial crisis of 2008 which tested the resilience and sustainability of not only individual banks but the entire financial system. The main issue here of course was the impact of poor credit decisions on bank capital and liquidity. Regulators have now responded to the financial crisis by significantly increasing said capital and liquidity requirements.

The impact of these increases has been such that they have changed the competitive nature of the industry. Consequently, strategy within banking and thus decisions on credit, are no longer about the business you want to do but what the regulatory capital and liquidity constraints will allow you to do.

There is no doubt that the Basel requirements on capital and liquidity have been a regulatory gamechanger. Just as banks have started to come to grips with the Basel requirements another set of regulations have emerged to take centre stage. They are the regulations in respect of Financial Crime and what in effect those regulations are saying is this: it is no longer good enough to know your sources of funding and liquidity, you also need to know where that money originally came from.

We have another gamechanger.

The Importance of Financial Crime Compliance

Financial Crime is defined broadly into six categories:

1. **Money Laundering**
2. **Bribery & Corruption**
3. **Terrorist Financing**
4. **Sanctions Evasion**
5. **Tax Evasion (Not Avoidance)**
6. **Fraud**

If there is any doubt as to the importance of Financial Crime and Financial Crime Compliance (FCC) then one has only to read the financial press to see the enormous fines levied against banks. Big Bank 1 (let's call them) paid $1.9 billion while Big Bank 2 has paid a whopping $8.9 billion in fines. In the case of Big Bank 1 the fines were levied for allowing that bank

to be used to facilitate the laundering of money by Mexican drug cartels. Big Bank 2 on the other hand got into trouble for facilitating payments to sanctioned countries including Iran.

... the FCC is easily one of the most significant challenges facing banks today

More importantly, the fines are not the end of the story. Big Bank 1 has been placed under a Deferred Prosecution Agreement (DPA)—meaning that criminal charges would follow if the bank did not undertake and effect significant improvements in FCC. For Big Bank 2, the landscape is even worse. The bank had been advised that criminal charges will follow and that it will not be allowed to clear any dollar transactions in 2015.

Then there is the case of Big Bank 3, a bank which utilised Swiss secrecy laws to help thousands of US citizens evade an estimated US$20 billion in taxes. The bank has since been fined US$980 million and is now also operating under a DPA, while the former Chief Executive of its Global Wealth Management division has been charged with conspiracy to defraud the IRS and is now under house arrest awaiting trial. Another Swiss bank, Big Bank 4, was fined US$2.6 billion and also faces criminal charges for aiding and abetting tax evasion by its US customers.

On a somewhat different note, a MENA bank has been held criminally liable for financing terrorism by a court in the US—because it provided bank accounts to individuals who were members of Hamas, the Palestinian militant group. The judgement was granted on behalf of US citizens who were victims of terrorist attacks for which they held Hamas responsible.

Huge and consequential fines, possible criminal convictions (both personal and corporate) and curtailment of business activities coupled with very negative reputational impacts all mean that FCC is easily one of the most significant challenges facing banks today.

The Industry Response to FCC

How have banks been responding to this immense challenge? How should they be responding? What should Senior Management, Compliance Officers and Internal Audit actually be doing about this?

Here are five ways banks have been responding:

1. Reviewing & Exiting of Certain Jurisdictions
There is no question that certain jurisdictions are more susceptible to Financial Crime than others. The Financial Action Task Force, an inter-governmental body also known as FATF (GAFI for some non-English speakers) regularly publishes lists of those countries which are either non-compliant or deficient in combating Financial Crimes.

Another very useful indicator of corruption is Transparency International's Corruption Perception Index (CPI). The CPI index ranks countries in accordance with the level of corruption on a scale of 0 to 100, with 0 being extremely corrupt.

Banks are using the information provided by the likes of FATF and Transparency International to determine jurisdictions they should be either reducing their business exposures or avoiding altogether.

2. Reviewing & Exiting Certain Industries & Relationships
Banks are also busy identifying industries where the risks of money laundering are considered greatest because of the amounts of cash involved and where there is an increased risk of disguising and integrating legal and illegal funds. Another consideration is whether or not an industry lends itself to bribery and corruption.

Examples of the industries/categories which are now being targeted by banks for either exiting relationships or enhancing due diligence includes:

a. Charities
b. Jewellery, Gems, Precious Stones
c. Arms and Munitions
d. Casinos
e. Shell Companies
f. Offshore Banking Institutions
g. Money Service Businesses (MSBs)
h. Transactions Involving Bearer Shares
i. Politically Exposed Persons (PEPS)

3. Reduction in Correspondent Banking Relationships
There was a time when the major international banks had as many relationships with other smaller banks in as many jurisdictions as they possibly could. The fees earned from correspondent banking were of secondary importance—the general rule was that the more correspondent banking relationships a bank had the more it would attract deposits from those other banks and the greater its importance within the global financial system.

However, having finally realised that banks that reside in poorly regulated jurisdictions, offshore centres or those with less than transparent ownership structures are highly susceptible to Financial Crimes, the major international banks have been busy exiting a large number of correspondent banking relationships.

4. Greatly Increased Customer Due Diligence
Customer Due Diligence or CDD is at the heart of the new regulatory environment. The general principle is that the more an organisation knows about its customers the better it can avoid and reduce the incidents of Financial Crime. The concept of CDD goes well beyond simply identifying the name and residence of a customer—it actually requires an in-depth knowledge of their business including their customers and suppliers, as well as the source of their wealth and capital.

The amount of resources being required for devotion to CDD, Know Your Client (KYC) and the onboarding of customers is now both exhaustive and exhausting—yet many banks feel that in light of the risks involved they simply have no other option.

5. Increased Investment in Compliance & Financial Crime Intelligence

The onerous and apparently unforgiving nature of FCC is such that it is vitally important that banks invest in both the requisite people and systems in order to ensure that they manage their business within the vast and ever-changing guidelines with a focus on both detecting and deterring Financial Crime.

In FCC, failure is simply not an option.

As such, as Financial Crime regulations are constantly being updated and new individuals, countries, groups and activities are constantly being added plus watch lists for money laundering and sanctions, the investment in IT and systems required to maintain pace is both immense and ongoing.

What This Means for Senior Management, Compliance Officers & Internal Auditors?

In the case of Financial Crime salespersons, relationship managers and others either in direct contact with customers or processing customer transactions and data represent the first line of defence.
Financial Crime Compliance is the second line of defence as it falls to this group to develop the knowledge, knowhow and capabilities to deter and detect Financial Crime.
Internal Audit represents the third line of defence and the independence of its role in assessing and evaluating FCC is specifically recognised in the FATF guidelines.

Within this context there are several issues which Senior Management, Compliance, FCC and Internal Audit must focus on if banks are to reduce the very significant risks of getting it wrong. The most important of these issues are outlined below.

1. The Adequacy & Effectiveness of Financial Crime Resources

FCC regulations and guidelines are vast given the number of bodies involved in developing them. In addition to the transnational and multilateral entities such as the UN, EU and FATF, every single country will each have its own Financial Crime regulations. For banks that operate in several jurisdictions the task of interpreting, responding to and acting appropriately on these regulations is thus extremely demanding.

Consequently, Senior Management has the primary responsibility for ensuring that FCC has all requisite skills, systems and other resources necessary for executing their tasks and that these resources are consistent with the nature of the business, the jurisdictions in which it operates, the customers it will target and the products which it intends to offer.
In this regard, Chief Compliance Officers are responsible for ensuring that they develop, obtain management approval for and execute FCC plans that are comprehensive, sufficient and fully reflecting of both the business and regulatory environments.

Internal Audit should review and assess the adequacy, efficiency and effectiveness of the FCC strategy and

plans. Internal Audit should also ensure that said plans are reviewed, approved by Senior Management and where appropriate revised on a periodic basis—in accordance with the demands of the operating environment.

2. Establishing Standards – Policies, Procedures, Documentation

Given the legal and regulatory requirements of FCC it is vitally important that suitable policies and procedures are established in order to consistently apply the appropriate standards. Having such standards is critically important in respect of demonstrating to regulators and if required the courts, precisely how the institution is fulfilling its obligations—including the determination of whether a Financial Crime is being committed or not.

Consequently, there is a need to ensure that not only are policies and procedures properly documented but that customer records, correspondence and employee workflows all fully reflect the onboarding and other decision making processes as they relate to Financial Crime.

It is the responsibility of the Chief Compliance Officer, working in conjunction with FCC, to ensure that standards are suitably implemented and that they are consistent with the nature of the business and the legal and regulatory environment.

In this instance the role of Internal Audit is one of ensuring that there is consistency in the application of standards and that that they are subject to regular review in accordance with changes in both the business and the legal and regulatory environments.

3. Developing a Culture of Compliance

The best operating standards will prove inadequate if they are not accompanied and supported by an appropriate culture of adherence and behaviours. The implementation and success of a suitable Culture of Compliance is dependent on the actions of both Senior Management and FCC.

Senior management has the primary responsibility for engendering a culture that both respects and exemplifies the Financial Crime governance framework. It can achieve this by:

A. Ensuring that the overall strategic approach, in terms of the types of jurisdictions, customers and products being targeted, are consistent with stated cultural and behavioural objectives e.g. if the target markets include casinos in Macau or mining in the Congo then this would be sending the wrong message
B. Communicating and reinforcing very clear messages in respect of what is considered as 'good' and 'bad' behaviours supported by appropriate training (see below)
C. Providing Compliance and FCC in particular with the necessary resources and operational independence to fulfil all its obligations
D. Ensuring that rewards and promotions are based on the right ('good') behaviours
E. Ensuring that 'bad' behaviours are sanctioned and punished
F. Ensuring that absolute remuneration levels do not negate cultural objectives
G. Establishing an appropriate whistleblower policy

The Chief Compliance Officer in conjunction with FCC must ensure that:

H. It has properly identified the universe of Financial Crime risks to which the institution is exposed and develops an appropriate strategy for addressing them

I. Resources notwithstanding, adequately and effectively implementing the stated strategy and programmes
J. It provides consistent and proactive support to the business units
K. It develops suitable risk-based programmes and approaches to:
   i. CDD and the onboarding clients
   ii. When, where and under what circumstances higher levels of due diligence and/or approvals are required
   iii. The active monitoring and surveillance of customer accounts, data and transactions
   iv. The escalation of FCC issues
   v. Reporting suspicious transactions and activities
   vi. Client reviews and exit
L. There is an active, ongoing and consultative relationship with the relevant regulatory authorities as well as industry professional bodies

The role of Internal Audit in this instance is to ensure that:

M. Compliance and FCC have properly documented programmes in support of the above
N. Such programmes have been approved at the highest levels
O. That said programmes have and are being implemented in accordance with the stated plans and business strategy
P. That such programmes are regularly reviewed and approved in accordance with the changes in the business and legal and regulatory environment
Q. That any variations or alteration is programmes or procedures are properly documented and approved

4. Financial Crime Education

As noted above Financial Crime education is a key and integral aspect of developing the right cultures and behaviours—but that is only part of the story. FCC is a complicated, ever changing and continuously expanding subject. It is therefore vital that all members of staff are aware of and know their specific responsibilities in respect of FCC. That awareness can only be achieved by way of a comprehensive and ongoing programme of education.

In addition, given that in most jurisdictions all employees working in regulated sectors are responsible for being aware of and taking the appropriate steps where necessary to prevent Financial Crime—from a legal perspective it is absolutely vital that staff are made fully aware of their specific responsibilities under the law.

Given the above, the **Chief Compliance Officer in conjunction with FCC** must ensure that the training programme is consistent with needs of the business and the legal and regulatory environment. Such a programme of education must:

A. Have the full support of Senior Management, who should also participate when and where relevant
B. Make all members of staff aware of their specific responsibilities in respect of FCC
C. Consist on online learning, classroom sessions and other learning resources such as websites and regular journals or newsletters
D. Form part of each employee's annual review and assessment
E. Form part of the employee onboarding process

In this instance the role of **Internal Audit** will be to:

F. Ensure that the scope of the programme is adequate
G. That the areas covered by each employee, business or operational unit is consistent with their roles and responsibilities
H. That the programme is run in accordance with a predetermined schedule
I. That attendances, non-attendances and test scores (if any) are properly recorded in employee records
J. That the programme is continuous and thus reflective of ongoing changes

Summary

Financial Crime Compliance has moved to the forefront of the list of matters that financial institutions must get right as the possible penalties, both personal and corporate, are now so severe that failure is clearly not a good option. Senior management, Compliance, FCC and Internal Audit all have a vital role to play and it is important that they all perform well.

As the third line of defence, Internal Audit is tasked with ensuring that the other areas of the business and governance framework are performing at optimum levels. This is the ultimate backstop and safeguard to the business.

The author invites your comments via email to JL@riskrewardlimited.com

RISK REWARD
GLOBAL BANKING & FINANCIAL SERVICES EXPERTS

Risk Reward Limited

part of Risk Reward Group of Companies

Global Headquarters

Risk Reward Ltd
60 Moorgate, 1st Floor,
London EC2R 6EL
United Kingdom

Office hours: London (GMT)
09.00 – 18.00 Monday – Friday

tel: +44 (0)20 7638 5558
fax: +44 (0)20 7638 5571

Risk Reward Americas

Office hours: (EST)
09.00 – 18.00 Monday – Friday

tel: +1 (917) 310-1334 New York
+1 (305) 831-4913 Miami

email:info@riskrewardlimited.com

www.riskrewardlimited.com

designed by mfp
info@mfp.me.uk