Reducing cost of regulatory compliance

February 9, 2012

This post is not meant for the average company which has to worry about SOX and standard privacy laws. It post is based on my experiences of working for a large international bank which did a lot of outsourcing, but did not know well how to translate the large amount of national and international laws and regulations into a manageable and cost effective control and monitor framework.

What does regulatory compliance cost?
A study of the Work Bank in 2005 shows that in the Netherlands, the United Kingdom, Belgium, Sweden and Norway on average 8 to 11% van the total expenditures by the government goes towards regulation of the business. Figures from the United States over 2004 indicate that there a total of 14.9% of the Gross National Income is spent on laws and regulation (11.2% on national regulation and 3.7% on regional and local regulation). In 1947 this was 4%.

The figures do not show what percentage was covered by financial institutions but research from Australia does give an indication. In this country, banks spent A$1.02 billion (€630 million) on complying to new anti-laundry and terrorism laws and regulations in 2007. This was A$50 (€31) calculated per capita. These figures combined with the increase attention by regulators and government for the financial sector means that the cost related to compliance is likely to increase even further.

Overall objective: look at compliance more from a financial perspective
The most important prerequisite to structurally reduce the compliance cost is to teach the (senior) compliance officers to approach regulation from a more business economic perspective. The typical compliance officer is used to shouting 'Federal Deposit Insurance Corporation' (FDIC) or 'Federal Reserve Board' (FDB) in the United States or 'Autoriteit Financiële Markten' (AFM) or 'De Nederlandsche Bank' (DNB) in the Netherlands as being enough to get a new control measure implemented. Hardly ever are direct and indirect costs taken into consideration. Although it is up to a business manager responsible for a product, market or activity to implement a measure or not, the advice of the compliance officer is important in such a case.

Learning as a compliance officer to look more from a financial perspective to its work and being able to make cost-benefit analysis and subsequently talk to the responsible business manager in both risk and finance terminology is to me a key driver to a) optimize the resource usage for compliance (regardless of the topic outsourcing) and b) improve the alignment between the compliance risk discipline and the business managers. The rest of the post will look more into how this overall aim can be achieved.

Sub objective one: look beyond the regulation; look at the risk
Being able to create a lean and mean regulatory compliance framework for an outsource

contract starts with understanding the scope and nature of the outsource contract. Understanding it to such an extent that that compliance officer is able to:

1. Define the ‘compliance risk drivers, and
2. Define a lean and mean scope for the compliance chart

1. Compliance risk drivers
The so-called ‘compliance risk drivers’ are parameters which have a negative or positive influence on the compliance risk the organization runs related to the contract. A simple example is the maturity of a financial product. A recently introduced ´green´ investment product scores higher on this point than a standard product that has been invested on the stock exchange for twenty years. So if part of the product selling and/or administration has been outsourced is it important to know that more partner/supplier oversight is required related to this risk driver. Three other examples are the amount of personal data in scope of the contract, the maturity of the vendors’ processes and attention of regulators regarding the outsourced activities or outsourcing in general.

Weighting and then subsequently scoring the risk drivers for the portfolio of outsource contracts provides insight in how outsource contracts relate to each other regarding their compliance ‘heat maps’. The compliance officer should at the end of this activity thus have a risk profile for every individual contract plus insight in how contracts score compared to each other. This insight will later on be an important driver for resource allocation and control/monitor effort

Two attention points here: a) ensure the risk drivers are defined in an adequate level of detail to prevent the outcome of a risk assessment to be too subjective and b) the score of a risk driver changes over time (e.g. the risk appetite changes) and has thus to be updated regularly.

2. Compliance Chart
The risk profile drives the scope of the Compliance Chart which has to be created for the outsource contract. The compliance risk profile regulates the selection of relevant regulations and the underlying themes and requirements (also called ´obligations´). For example, an object can score high on a compliance risk driver called ´presence of personal data records´. In that case several themes from the Dutch Wet bescherming persoonsgegevens (Wbp) will have a prominent place in the Compliance Chart. The design of the Compliance Chart will thus consist of a minimal base set of regulatory requirements completed with specific add-ons derived from the characteristics of the risk profile.

The cost advantage is in leaving out the non-relevant regulation and in prioritizing themes and requirements that do belong in the Compliance Chart. Additional efficiency gains are captured later on when defining the control and monitoring strategy based on the lean-and-mean compliance chart.

The regulator on risk-based compliance management
Research by the Basel committee from 2008 shows that the compliance function is given an important role when managing risks. The responsibilities mentioned in Basel II have been implemented in the Netherlands within the Wet financieel toezicht (Wft) in articles 3:17 en 21 Bpr. These articles have a direct link with articles 13 of the Markets in Financial Instruments Directive (Mifid) and article 6 in which the implementation and measures are discussed: 'Member States shall ensure that investment firms establish, implement and maintain adequate policies and procedures designed to detect any risk of failure by the firm to comply with its obligations under Directive 2004/39/EC, as well as the associated risks, and put in place adequate measures and procedures designed to minimise such risk.'

The above given quote indicates that the regulator not only expects the financial institution to implement the regulation, but also that it has to comply to the regulation's exceeding goal that undesirable activities and behaviours have to be prevented. In short, the management of the underlying risk.

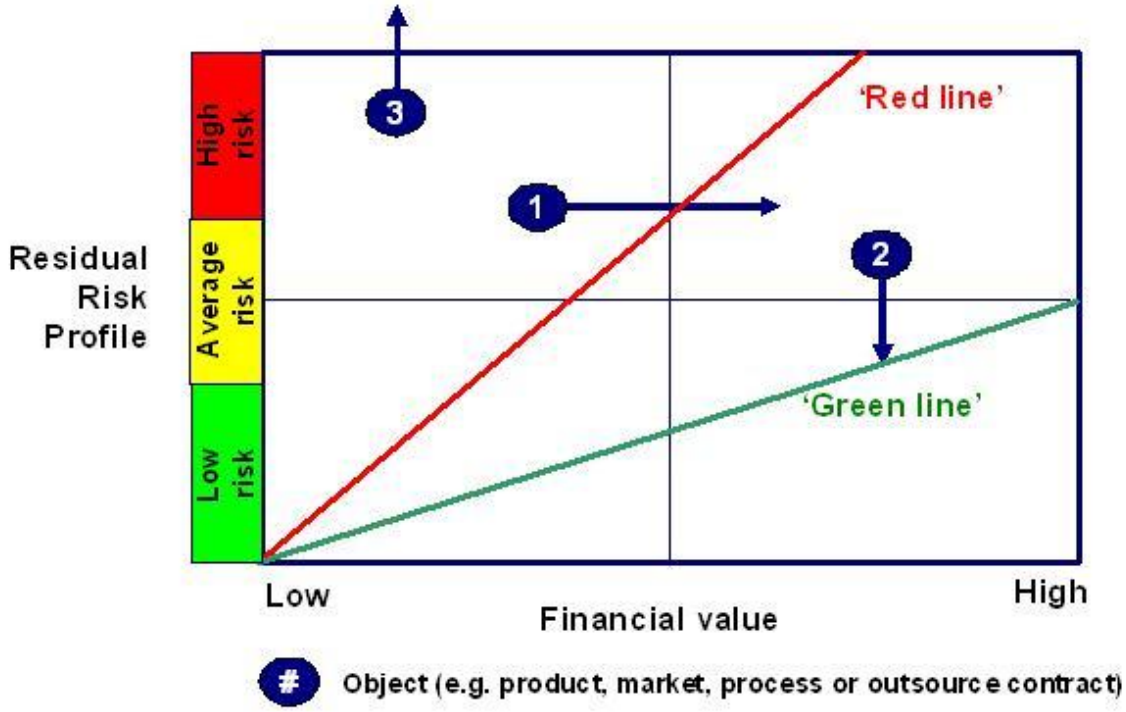
The approach applied to practise
At the compliance department of the financial institution I worked with, applying this methodology meant first of all more prominent involvement by compliance officers in new projects. This turned out to be a difficult task as outsourcing was regarded as a subject that was initiated by the business and compliance was not seen as a relevant stakeholder. The situation improved however when the compliance departmenr described clearly how and when they wanted to be involved and by formally incorporating the compliance function within the project governance

But being at the table was only one of the challenges. In the past the business case for several outsourcing deals got scuttled by the cost of the control framework desired by the Compliance department. An organization active in the field of payment traffic wanted to outsource part of its IT because the initial business case predicted lower costs. However, the requirements the supplier had to comply with regarding, amongst others, security were so costly that the entire outsourcing was cancelled two weeks before the planned sign date. In this case too, the compliance department was involved very late in the project, causing the expensive bunny to come out of the hat only just before the planned signing date.

On the one hand, this example is an argument to involve the compliance function early in de process, while at the same time it also underlines the necessity for compliance officers to become better informed in the financial implications of compliance. Understanding it to such an extent that that compliance officer is able to:

- Determine the financial risk (impact x probability) of the regulated object (e.g. outsource contract);
- Gwet a feeling for the financial value (return minus cost) of the regulated object.
- Being able to engage in a discussion trading off risk, compliance cost and value.

To enable the compliance office to get a more sophisticated view portfolio management concepts were introduced within the bank. An outsource contract can have a high compliance risk and a low financial value, but the situation can be completely different in two years time. This is illustrated in the figure in which object 1 currently has an unacceptable risk-value distribution (the object is above the red line). For example by increasing the volume of the contract and/or lowering the compliance risk, the ratio between risk and value can shift to an acceptable level.



The green line in the figure represents the desired ratio the financial institution has defined for compliance risk versus the related value. Based on the position in the portfolio the best improvement strategy for a outsource contract can be determined: lowering the risk profile (object 2), raising the value of cancelling the contract (object 3).

Looking at outsource contracts in this way originates from the portfolio management theory. This is a structured method for categorizing, evaluating and prioritizing objects based on an acceptable balance between risk and value. The objects in the portfolio (for example all outsource contracts) are scored by comparing them to each other and the location within the portfolio directs the amount of resources to be spent on compliance activities.

In the customer example that was discussed earlier, the existing portfolio of outsourcing contracts was analyzed and the contracts with the maximum score (high risk and value) were the first to be assigned to compliance officers. The goal was determining if the existing control and monitoring strategy was in balance with the contract. Amongst others, this entailed determining whether the (gross/inherent) risk already had been reduced to an acceptable level (´residual risk´ lower or equal to the risk appetite). If not,

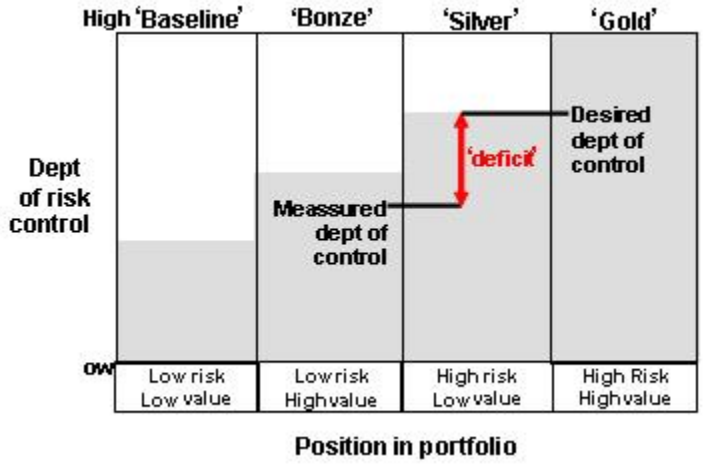
which additional control and monitoring activities could accomplish this in the most efficient manner.

The control and monitor activities are typically described in a so called Compliance Program which is the overarching framework that encompasses the different activities and responsibilities performed by the compliance function.

Compliance cost can be reduced by applying only a ´golden´ control and monitoring approach when it is really necessary (for example at high risk and value) and select a ´silver´ or ´bronze´ approach elsewhere (see figure).

By strengthening the collaboration of the so called 'three lines of defence' and other risk disciplines (for example, operational and information risk departments) even more efficiency gains may be achieved. For example, the department Operational Risk Management (ORM) is usually responsible for controlling the risk related to business and IT continuity. Within the Dutch banking regulation Wft, requirements are stated regarding IT continuity. To comply with this regulation the compliance department may choose to come up with new controls or look into existing assurance measures and add where necessary.

The desired end result is a cooperation in which the lines of defence and risk disciplines make use of a shared set of procedures, risk-control matrices, control measures, reports etc. However, this requires the willingness to put the needs of the group above ones own.



In the figure, the translation is made from the position a regulated object has within a portfolio (see first figure) to the corresponding control and monitor strategy. The strategy can be defined in terms of the lines of defence that are involved in the monitoring. This way, the choice can be made only to have the first and second line monitoring in case of a ´bronze´ control and to only give the third line a prominent role in case of a ´silver´ and ´gold´ control.

Removing the discrepancy between the current and desired control maturity can be done by means of an improvement plan or by including actions in the monitoring plan.

Optimize the expenses by first of all implementing those improvement actions that have the highest risk reducing effect at the lowest (in)direct costs.

What are the results that can be achieved?
At the compliance department which implemented this methodology a minimum base set has been defined consisting of requirements to which external suppliers have to comply and future suppliers will tested against during the due diligence process. Besides that, together with the retained organization (which acts on behalf of the business as the first line of defence) and existing suppliers, there are talks on creating control frameworks in which a balance is sought between the best practises of the supplier and the requirements and wishes of the bank. Among others, this is a way to try to limit the check related to compliance the supplier submits each month.

In principle all objects (for example products, markets and activities) that are regulated and over which the financial institution runs a reputation risk, can profit from the described approach. The compliance program can be designed both more effective and more efficient than is currently often the case and besides that, by means of continues documenting the steps, a risk-based ´compliance dossier´ for regulated objects is being constructed.

This dossier can be used to indicate to internal and external stakeholders that the organization is ´in control´ and that the organization is acting not only within the law but also in the spirit of the law. Eventually (also in the law) it is about adequately controlling the risk underlying the requirements demanded by the legislator.

The most added value however, is the insight that is gained between the financial value of, for example, a pension product, the compliance risk an organization has and the money that is spent on compliance. This insight will enable management to make a well-informed decision based on possible scenarios that can further optimize the relation between risk and value. No one is waiting for the situation ABN Amro found itself in during 2005 when it had to pay $80 million to the US government because of involvement in money transactions to Iranian and Libyan entities.