Risk-Based Resource Planning and Allocation

Introduction
Since the financial crisis, banks and other financial services institutions have increased Compliance resources significantly. In 2014, the Financial Times claimed that Compliance roles accounted for some of the hottest areas of financial recruitment, calling it “the age of the Compliance Officer”. In another FT article, just a year later, it said that JP Morgan hired 4,000 Compliance Officers in 2013, whereas HSBC hired 3,000 in the same year and an additional 2,000 in the following two years. These are staggering numbers of additional resources deployed to a cost centre. For Compliance professionals, this is good news, and many regulators commend the much needed investment in controls functions within banks, but how are these additional resource requirements calculated, justified and eventually allocated?

What has led to this increase in resources?
Before we begin, let’s define the term “resource”. In the context of this article, I will talk about human resource in the main, but will also make reference to other resources embedded in operational structures, such as IT systems.

There are two key reasons for such a large investment in Compliance resources. Firstly, there has been wholesale regulatory change around the world, driving the need to hire more Compliance professionals to interpret, design and implement controls to meet changing regulations. Secondly, we have seen unprecedented financial sanctions levied by regulators, which appear to have provoked a knee-jerk reaction amongst the financial institutions subject to these regulatory actions. Certainly for the second reason, there is a considerable risk that the increased resources have not been logically justified, which is not good for those employed, the companies employing the resources, or the investors in those companies.

With regulatory control costs running in some occasions, over an additional $1 billion per year in the large global banks, Boards must surely be asking the questions, “are compliance costs appropriately justified?”. Perhaps they are, perhaps they are not, but it is crucial that financial services organisations have a clear, logical process in defining resource requirements, both human and system, before proceeding to hire or deploy.

How should companies assess their resource requirements?
Heads of Compliance must employ a risk-based strategy in quantifying and qualifying the required resources in their organisation. Without this risk-based strategic approach, it is difficult to provide assurance to the Board or regulators that the allocation of resource is pertinent to the nature, scale and complexity of your organisation, and indeed manages the risk appropriately.

The cycle in Figure 1 outlines how the process should work. It is not a “one-off” activity, but should be a living process that identifies changes in business risk and environmental risk brought by changes in regulation.

Define the Regulatory Risk Universe
To begin the process, a regulatory risk map should be developed, which defines the regulatory risk universe. This is done by mapping business activities to specific regulatory rules that apply to the organisation and to those activities. To do this for the first time is quite time and resource intensive, and it can often be more efficient and economic to employ a consultancy to advise and help complete the risk universe.
Measure the Risk

Once the regulatory risk universe has been defined, the identified risks must be measured in terms of likelihood of the risk occurring, and the impact it could have on the organisation in that event. Risk measurement occurs at two stages: firstly, the inherent risk, which is calculated without consideration of any controls that may be in place and secondly, the residual risk, which considers the effectiveness of existing controls in mitigating the risk.

The risk measurement stage of the process should be underpinned by a consistent scoring methodology, so that risks are measured in a reliable and comparable way. Furthermore, a numeric scoring system enables risk to be categorised into risk level groups such as High, Medium or Low. This allows firms to prioritise risks, and create a heat map of where the greatest regulatory risks reside within the organisation’s activities.

Finally, escalation and approval thresholds should be defined, which are driven by the organisation’s risk appetite. For example, low risks may represent acceptable risks that are just part of doing business, whereas high risks may require escalation to the Board.

Design the Control Framework

In this context, the control framework involves assigning resources, both human and system, to mitigate the regulatory risks to the Board-mandated risk appetite of the organisation. As mentioned above, it might be reasonable to leave some low risks without any specific controls in place, if the inherent risk is deemed to be low enough to tolerate.

When assessing the controls required for each risk, it is important to consider the efficacy and efficiency of each of the control options. For example, in a financial institution that deals with thousands of customers and transactions per day, it is far more efficient to deploy a transaction monitoring system rather than employ numerous employees to monitor the transactions on a daily basis. Conversely, for an organisation that deals with few clients and a small number of transactions, a transaction monitoring system would be disproportionate to the risk, and competent human resources could mitigate that risk quite effectively.

It is important to consider the size, nature and complexity of business areas when designing the most appropriate controls to include within your framework. For a retail bank with a large branch network, some of the major regulatory risks are decentralised across the branch network. It may not be viable to deploy 2nd line Compliance staff across the network, so embedding compliance controls into the first line of defence in the branch is a better solution. It is common to assign a Compliance or AML champion within each branch or region, who has a role within the business, but who can ensure that compliance is maintained by acting as a knowledge and escalation point. These individuals form an important directive control.

An often misunderstood element of assigning human compliance resource is the competence of the resources. Heads of Compliance need to define the level of competency required for each role. The heat map created in the Measuring stage of the cycle, should inform the business of the core competencies required to mitigate the risks effectively. Competency manifest itself in a number of ways: years of experience in compliance, years of experience in a jurisdiction, years of experience in a particular type of institution, years of experience in a particular financial product etc. It is quite common to see a Compliance Officer, with compliance experience in credit cards, for example, working in a very technical area such as trade finance. In this instance, it may be more sensible to hire someone with less compliance experience, perhaps even none, but with plenty of trade finance experience. This is due to the operational knowledge required when monitoring trade finance activity.

Implementing Controls

Following the design stage of the cycle, resources can be deployed and implemented. Depending on the resources opted for, this can involve a project plan, in the case of an IT system implementation or revised working procedures. In the case of human resourcing implementation, appropriate hiring, induction, training and supervision strategies should be in place to ensure an effective deployment of staff.

With regards to staff recruitment, it is important to hire adequately skilled resources, as discussed previously, in order to deliver the controls required. When hiring new staff, job profiles and minimum levels of experience should be clearly communicated to the HR function and recruitment agency. Again, it may be more effective to hire a resource with strong operational knowledge, rather than individuals that understand general compliance.

As described in the Measuring stage of the cycle, controls do not have to lie with 2nd line Compliance: employees within the 1st line of defence are often the most effective directive control to mitigate risks. These employees are often not direct compliance cost to the organisation, as they have a functional operational role as well. Using 1st line operational employees makes the implementation of compliance control a lot less costly, more efficient, and often more effective, because these individuals understand their business area better than most.

Monitoring

Once the controls are implemented, their effectiveness should be assessed to ensure that the controls are working as expected, and that the control environment is managing regulatory risk in line with the company’s risk appetite. Compliance Employees, as part of their role in the 2nd line of defence, should be tasked to carry out independent assurance work on the effectiveness of these front line controls. This may include adequacy of advice, appropriate decision making and appropriate escalation of issues on in timely manner. Assurance work should also be carried out on the effective use of system resources, such as transaction monitoring systems, to ensure that these controls are utilised properly, and are delivering control to the risk appetite of the organisation.
Human resource deployment should also be reviewed as part of the monitoring element of the cycle. Examples of such reviews could include assessment of the workload of control staff, and whether they have sufficient bandwidth to deal with BAU as well as reactive work. Skills needs analysis should be carried out to demonstrate where the strengths and weaknesses of skills and knowledge lies. This analysis should also consider planned business activities, and whether there is sufficient compliance expertise to effectively manage the risk of a new business line or regulatory jurisdiction.

**Other Considerations**

I have discussed 1st and 2nd lines of defence in the regulatory risk management cycle, but it is important to consider the role of the 3rd line of defence also. The Internal Audit function has its own risk universe, which drives its assurance activity, typically over a three year cycle. It is important for Internal Audit and Compliance to discuss planned assurance activity, because there may be an overlap, and essentially a duplication of work, which does not add value to the organisation or its controls. Likewise, other 2nd line of defence functions such as Risk, may also duplicate assurance work, so again, it is important to cooperate, and possibly collaborate with other control functions to drive a more efficient, cohesive and more risk-based allocation of resources.

**Conclusion**

The process outlined in this article may be resource intensive, it may take time to begin and take time to complete. However, without a risk assessment behind the allocation of resources, it is difficult to justify to Board of Directors or a regulator that the allocation of resources is appropriate to the nature, scale and complexity of the organisation. Historically, we have seen under resourced Compliance functions, which naturally causes a concern for regulators. Currently, there may be a risk that Compliance functions are over resourced and poorly coordinated, which should also cause concern for regulators. Without a risk-based rationale behind your resourcing justification, an effective Board of Directors should not approve the increase and / or deployment of resources. Without a risk-based rationale behind your resource allocation, a regulator would be entitled to question an organisation’s grasp of the risks it faces and appropriate allocation of controls to mitigate those risks.

**Author:** Carwyn Evans, Director, Consultancy  
E CEvans@cclcompliance.com  
T +971 4 323 0800