An oversight framework to keep senior executives in control

Received (in revised form) 3rd August, 2020

Richard Pike
Founder and CEO, Governor Software, Ireland

Richard Pike

***Richard Pike** has extensive experience of working with financial institutions throughout the world, assisting companies in managing enterprise risk more efficiently while addressing local regulatory guidelines and standards. Richard is currently Chairman of Citadel Securities (Ireland) Ltd and an Independent Nonexecutive Director at, FBD Insurance plc, The National Cyber Security Society, JPMorgan fund administration, JPMorgan hedge fund administration and Citadel Securities Europe. He is also the founder and chief executive officer of Governor Software. Prior to these roles, Richard has worked in various senior banking, insurance, credit and market risk roles at Permanenttsb bank, Wolters Kluwer Financial Services, ABN AMRO, Bain, COMIT Gruppe and Quay Financial Software. He has analysed, designed and managed the development of core treasury and enterprise risk management systems for large financial institutions, including UBS, Citibank, Schroders and Unicredito. In 2009, Richard was recognised as a 'Top 50' Face of Operational Risk by* Op Risk & Compliance *magazine and was a contributing author to two books on risk management. He was also a founding board member of the Governance, Risk and Compliance Technology Centre, which focuses on research in the area of financial services governance, risk and compliance. He teaches on risk management at the Institute of Banking and at the UCD Smurfit Business School. Richard has also received the designation of 'Certified Bank Director' from the Institute of Banking.*

2C Avonbeg,
Long Mile Road,
Dublin, Ireland
Tel: (+44) 0800 047 0962
E-mail: richard.pike@mycomplianceoffice.com

Journal of Financial Compliance
Vol. 4, No. 2 2020–21, pp. 102–109

2398-8053

Abstract

Given the current regulatory focus on senior management responsibility and the resultant requirement for high-quality oversight of processes and controls, this paper sets out an approach to instantiating such an oversight process in the 1st line of defence. As most financial firms are subject to huge change, the paper then goes on to show how such an oversight process might dovetail with a regulatory change process. In order to more clearly explain the approach, the paper then describes a short case study from a large US bank who successfully ran such a project in 2019. Finally, the paper will set out the benefits to be accrued from taking this path to high-quality oversight.

Keywords: oversight, 1.5 line of defence, regulatory change, knowledge graph

BACKGROUND

The advent of responsibility regimes (eg SMCR (Senior Managers Certification Regime) in the United Kingdom, MICR (Managers in Charge Regime) in Hong Kong, SEAR (Senior Executive Accountability Regime) in Ireland) and the focus on operational resilience by regulators, are causing senior managers at financial firms to question their ability to effectively oversee their businesses. In many cases, they understand that relying purely on the 2nd line of defence for this oversight is not sufficient. The 2nd line of defence is designed as an assurance function that necessarily focuses on policies, frameworks and high-level risks and issues. They rarely get into the 'weeds' of the business unless they are doing specific testing or chasing the solution to issues. In fact, 2nd line functions that do get very close to the business too much tend to lose their ability to carry out their assurance function effectively.

So, if you cannot rely wholly on the assurance functions, what do you do? This, and other issues, have resulted in the advent of the 1.5 line of defence. This function reports to the business and has a core focus on risk, compliance and control management. It is often used to manage interactions with the assurance functions and regulators while also dealing with issue management and day-to-day fire fighting around business problems related to the control environment. Some firms are now realising that this unit is best positioned to provide oversight of the business processes and help assure the senior managers that all is well (or not as the case may be) within their areas of responsibility.

This new movement is akin to the change in the manufacturing industry to total quality management. In general, it was a move away from the quality assurance (QA) department being at the 'end of the line' and moving them to be an integral part of the process. Rather than focusing entirely on outputs and problems, they initiated monitoring of each stage in the process with the aims of stopping issues before they happened and helping to redesign processes to ensure quality.

SUMMARY

This paper sets out an approach to instantiating such an oversight process in the 1.5 line. As most financial firms are subject to huge change, the paper then goes on to show how such an oversight process might dovetail with a regulatory change process. In order to more clearly explain the approach, the paper then describes a short case study from a large US bank who successfully ran such a project in 2019. Finally, the paper will set out the benefits to be accrued from taking this path to high-quality oversight.

THREE-STAGE APPROACH

Best practice is still emerging in this area but what is set out subsequently has been seen to work at firms of various types and sizes. A clear three-stage approach is starting to become the de facto standard.

Understand your obligations

The business is given various obligations through regulation, policy, strategy and risk appetite. Those obligations then require processes and controls to ensure they are carried out correctly. So a vital first step is for the business to clearly map those items together to understand the linkages and relationships and get a library of the 'business as usual' situation. This effort results in a full map from regulations to tests as shown in Figure 1.

This process may seem like a huge lift (and it often is) but if one thinks about the logic, it is impossible to oversee a process/policy if one does not know its constituent parts. Teams often find that a lot of this data is already available in the firm within the GRC (Governance Risk and Compliance) systems or even the multitude of process mapping or other systems in an institution. It is also not a requirement to take a Big Bang approach to this effort. Firms can tackle the areas with the most risk or the most potential for benefit. A tier 1 US firm has taken five years to do this on a global scale whereas another large bank in the United States recently used the cyber risk arena as a first step due to the regulatory focus and the fact that it was a relatively clean slate.

One key challenge in this process is the interconnectedness of the data; if one tries this in a spreadsheet, one will realise that the many to many nature of the links between policies and regulations will quickly overwhelm the technology that is very table based. Firms that have succeeded in these projects (for example a large tier 1 US bank) have utilised graph technology (as used by Amazon and LinkedIn) to store the complex network of regulations, policies and controls. This creation of what is called a knowledge

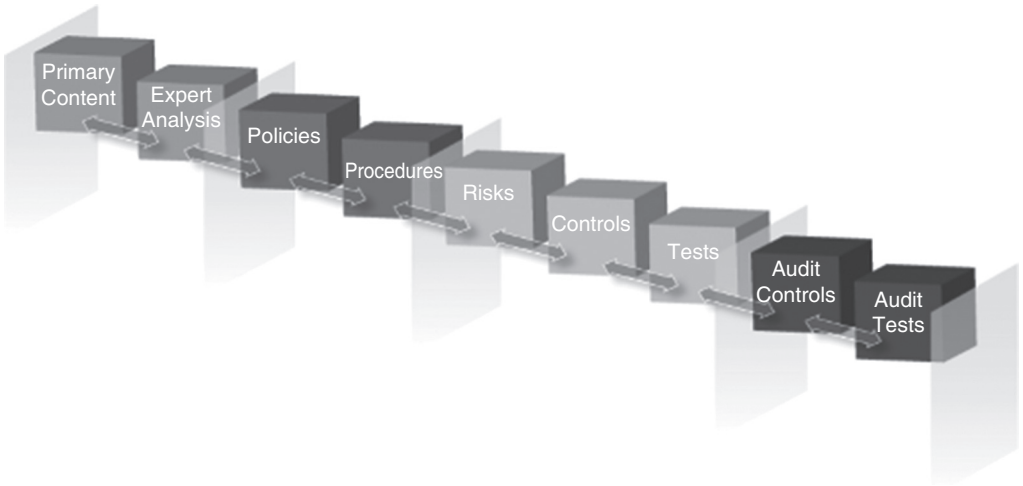

Figure 1 Linkage between the Primary Content (obligations) and business processes and controls

graph also enables firms to leave a lot of the detailed data in original systems that are just pointed to by items in the graph. So the firm is not creating yet another system of record but instead creating a map of how all of the items relate to each other.

Another challenge is to decide what data points need to be recorded. The advice here is to err on the side of less data items; otherwise, the project will quickly end up in a sea of complexity. Key data points around roles and responsibilities are required but other metadata about the policies or controls might be best left outside the scope.

While the map set out earlier may seem like a large unnecessary overhead to some financial firms, if one talks to a life sciences firm or medical device manufacturer, one would find that they are not be able to survive without such a map. Given the current regulatory scrutiny and focus on personal responsibility, many executives are realising that it is a required overhead and, as this paper shows, actually a real benefit to the firm in the long term.

Utilise continuous monitoring to understand the status of processes

Once there is a map of the business, the 1.5 line can instantiate a monitoring programme.

For each policy, process and/or control, the team can define one or more indicators that tell them about the correct performance of the item (policy, control etc). These indicators can be either quantitative; a set of metrics that are recorded and have thresholds set to identify when these items are out of tolerance, or qualitative; an assessment from a process/control owner as to the state of the performance of their items. These indicators might range from automated control failure data points to the results of manual control tests or audits. They can also include attestations from staff/third parties that are used for other processes like Service Organization Control (SOX) or Sarbanes Oxley (SOC2) reporting.

Again, this might sound like a huge project, but teams actually find that most of these indicators are already in place for other reasons like management and/or compliance reporting. So it is often a matter of reusing those same indicators for this purpose. The key is to focus on capturing the performance of the controls/processes rather than being drawn into trying to assess risk or design considerations. That data may be captured but the focus of this exercise is on oversight, and projects often get drawn off course by trying to be forward-looking

risk processes as well. Risk data is useful to help teams decide where to focus initial efforts or to drive out more status information but not as the key deliverable of the project.

A key pointer here is to ensure clarity. Failures at this stage most often are due to the indicators being too nebulous, resulting in the reader not understanding what is being indicated or the inputter not understanding how to gather the data. Another common problem is the differing frequency of data. How to merge daily, weekly and annual data into a monthly attestation. In both cases, the best approach is to utilise processes and indicators already proven and being relied upon for other uses.

The result of this stage will be a continuous understanding of the status of one's performance against the obligations of regulations, policies and strategy. If stage 1 has been completed correctly, this will enable reporting of status against regulations, policies, strategic objectives etc.

The other benefit of this approach (as was found in Total Quality Management in manufacturing) is that issues are picked up before they become large problems and resources can be directed towards failing processes before they get the attention of external stakeholders like customers or regulators.

So, one can think of this as a continuous monitoring process that sits above the actual processes and constantly flashes warnings when things start to go awry. It is similar to the traditional picture of a factory owner standing on a gantry above the 'shop floor' watching and listening for problems with the manufacturing line.

Many senior executives in financial services firms will tell you that they already have far too many monitoring processes and spend hours in front of various dashboards and reports. The problem seems to be that these individual processes exist for different reasons and look at different parts of the problem, which results in 'monitoring spaghetti'. The aim here is to have one monitoring process that, when well designed, provides all of the monitoring outcomes required in a unified approach. The subsidiary benefit of a unified monitoring approach is that the entire monitoring process can be streamlined and efficiencies can be found.

Retaining one's data as evidence

Finally, firms are recording the results of the first two stages and any associated documentation. In the current regulatory landscape where 'if you don't have the evidence of a process, it didn't happen', it is vital to be able to show a regulator/auditor that one has understood the obligations and controls and one knew what their status was. Even where one has issues, if they can show that they had identified the issues and have programmes in place to close them, they will be in a much better place with the regulator/auditor. What firms who have implemented this process realise is that they find it much easier to respond to regulatory or audit data requests. This is currently a large overhead for many businesses and so this process is the source of some clear efficiencies as well as a regulatory necessity.

As set out in the first stage, the knowledge graph does not have to be another system of record for this evidence data, but instead it can simply point to it in other systems.

RELATIONSHIP TO OTHER PROCESSES

This three-stage process set out earlier will result in a powerful standardised oversight process run by the business 1st line to ensure that the obligations of the business are met and senior executives can attest to that in an effective and efficient manner.

Obviously, this process would interact with and encompass many other processes within the business and will therefore require strong senior executive sponsorship. As stated earlier, the project can and should utilise processes and systems already in use

in the firm and act, in the main, as a collator rather than a creator of data. A key benefit of being a 1st line function for the 1.5 line is that business support when coming cap in hand for data or resources. It can be more complex when discussing these needs with 2nd line colleagues. It helps to explain that the project will result in a clear understanding of the business that the 2nd line can use as a key pillar of their work. It also acts as a common language that the 1st and 2nd lines (and even regulators and auditors) can use to communicate.

In cases where the assurance functions understand the benefits of the approach, firms have redesigned processes involving those functions to gain extra benefits. There is no template for these interactions, but many firms have worked through the issues and come out the other side with smooth results.

Regulatory change example

Let us look at how it might work in the context of a regulatory change-management process.

Line of sight from obligations to policies

What if the compliance team were to map out a new or amended regulation when they first receive it? This mapping would involve breaking down the requirements into specific obligations and for each obligation defining what proof points they need for good compliance oversight. These items might be metrics, audits, assessments, outcomes etc.

Collaboration to piece the policy puzzle together

The policy-writing team would then take these regulatory maps and match their individual policy elements to these obligations. At this stage, they should also include in their policies the items that will make for good policy oversight. For each of those items, they may also define the appetite or tolerances that will cause the policy to be in 'breach'.

Seamless transition from agile project delivery straight to BAU (Business as usual) oversight

When regulatory requirements are presented to the business as the input to the change programme, there will be a clear understanding of what information is needed to record and store for compliance oversight to do their job. If this is done well, then those items should be the same regardless of the oversight function that needs them (compliance, audit, regulators etc) although it is worth noting that operations teams may rely on differing approaches, systems and machine intelligence to ensure their own processes.

Documentation/evidence management

With the earlier-mentioned tenets followed, a financial institution would have a new regulation mapped to its obligations and then a set of policy statements that map to those obligations. For each item, there will be a well-defined set of metrics and/or assessment points that are required for oversight. As those data points are recorded, the process should also require the attachment of evidence data lineage so that overseers can easily track back to the source.

Ability to see demarcation zones between 1st and 2nd line activities

Within the earlier-mentioned 'Oversight Map', each item can also have a clear statement of responsibility to ensure that both 1st and 2nd lines clearly understand what their roles are in the process.

Complete record over time

The finish line is a map of the regulatory obligations, linked to a set of internal policy statements, linked to a set of internal

proof points (metrics, assessments, reviews) all of which record and store all changes in real–time, thus allowing anyone to go back to a point in the past to see the state of compliance.

CASE STUDY

NYDFS Cyber 500 Compliance Certification (2019) at US$180bn US bank

Background

The NYDFS Cybersecurity Regulation (23 NYCRR 500) is a new set of regulations from the NY Department of Financial Services (NYDFS) that places cybersecurity requirements on all covered financial institutions. The rules were released on 16th February, 2017, and includes 23 sections outlining the requirements for developing and implementing an effective cybersecurity programme, requiring covered institutions to assess their cybersecurity risks and develop plans to proactively address those risks.

The board of each covered institution must annually attest to their firm's compliance with the regulation.

The challenge

Like many of its peers, this bank was utilising a mix of Microsoft tools and SharePoint for the governance and oversight of the underlying processes required to support the annual NYDFS Cyber 500 compliance certification. As a result, it was a struggle for the bank to

- fully understand and communicate the consolidated status of the firm's compliance against each relevant domain of the NYDFS Cyber 500 regulation;
- provide senior management with a central point where they could self-serve real-time data on NYDFS Cyber 500 compliance;
- track and oversee in real-time the progress of individual attestations within its review/approval workflow processes; and
- retrieve and collate data for supporting NYDFS Cyber 500 compliance reporting/certification.

The solution

To address this challenge, the bank sought to create a 'live' NYDFS Cyber 500 oversight map. This map would contain

- the 'live' NYDFS Cyber 500 regulation broken down to individual obligations;
- the bank's individual compliance activities (eg policies, controls) connected to the relevant regulatory obligation(s);
- scheduled attestations for key obligations (supported by workflow, notifications, dashboards, commentary, evidence and performance key indicators); and
- history and robust audit trail.

The aims of the project were:

- to fully understand the consolidated status of the firm's existing compliance to NYDFS Cyber 500;
- to communicate and self-serve information to senior management via customised reporting and file packages;
- to retrieve historical information for track and trending purposes; and
- to facilitate gap analysis and project management of corrective actions.

The results

The project results in a set of clear responsibilities for different staff members. Each manager made an assessment of their controls/procedures and recorded supporting commentary and evidence documentation — all within a secure, audit trail environment. This meant senior managers, with the appropriate access, could see the explanation behind status approvals (in real-time). Overall, it allowed the board to get comfort in regard to their compliance with the regulation and make

the appropriate certification. The return on investment for the project was achieved through operational efficiency gains (aggregating status, reporting and audit preparation) and increased effectiveness (situational awareness, agility and line of sight).

FTE (full time employees) Operational efficiency gains

1. Average time taken to attest/review/approve compliance status (for a NYDFS regulatory obligation) was reduced.
2. Time taken to collate data and produce the NYDFS Cyber 500 compliance report (to support certification) was reduced.
3. Time taken to collate evidence files (to support certification) was reduced.

Improved compliance understanding/risk mitigation

The bank can now monitor their NYDFS Cyber 500 compliance status in real-time, can project manage corrective actions and changes (if/when required), and can easily go back to previous 'points in time' so that both historical data and emerging trends can be identified. In addition, auditors or regulators can clearly see that bank management are aware of their key obligations and associated status, are compelled to assess these obligations periodically, and can take appropriate corrective actions as necessary to manage any related risk.

Outcomes

This project has resulted in increased oversight, governance and confidence in the overall understanding of the firm's NYDFS Cyber 500 compliance performance. It has also increased confidence to onboard other regulations or programmes, which would further enhance the RoI in terms of FTE operational efficiencies and risk mitigation.

BENEFITS OF THE 1.5 LINE OVERSIGHT VS THE TRADITIONAL 1ST LINE APPROACH

The key problem that is the focus of this paper is how to provide high-quality oversight to senior executives at financial firms so that they can assure regulators and other stakeholders that they have taken reasonable steps to control their businesses.

Taking practices from other industries like manufacturing, firms are using their 1.5 line of defence to create an oversight process that builds and maintains a knowledge graph of their business, instantiates a monitoring process across all processes and controls and finally stores evidence as proof of oversight.

The reasons given by firms who have implemented this approach are many but most cite the problems they have had relying on teams they do not have long-term control over, 2nd and 3rd Lines or external consultants. These teams provide advice or expertise but do not really have the long-term strategically aligned view of the business that is needed. The 1.5 line is staffed by risk/control experts who are aligned with the business and focused on delivering the most efficient and effective outcomes for the firm.

Secondly, a problem with the traditional 1st line approach is that the staff running the business are constantly dragged off to perform assurance and oversight roles to support stakeholders including senior management, regulators, auditors and 2nd line teams. This process is extremely inefficient and is often quoted as the reason for missing key business goals.

As we have seen from the case study given earlier, there are many benefits apart from the key ones set out earlier. They include

- By defining the items needed for oversight upfront, the downstream processes of policy drafting, system definition and control creation are working to a specification rather than making guesses and

assumptions. This means a better result but also less rework.
- A clear data lineage from the business, through the policy to the regulation, means that neither too much or too little data is collected by the business, and it is possible to do detailed analysis on the important data items.
- When the 3rd line or a regulator comes in for a review, it is easy to produce a complete report and all of the proof points will be there organised according to the regulation/policy that they are reviewing.
- Senior executives can be provided with status updates in the format of the policies they have signed off or the regulations they have been made responsible for, rather than in an internal business format.
- All stakeholders have a language they can use to communicate in and a gold standard they can work with.
- Change, either externally or internally driven, can be managed as an iteration rather than starting from a blank sheet.
- New machine learning techniques can be used on clean data to understand where bottlenecks and inefficiencies lie and risk may appear.
- Strategic change, through M&A (mergers and acquisitions) or other methods, is facilitated by the fact of having a sound understanding of the business and its operational status.

CONCLUSION

Current regulatory focus on senior management responsibility and firm resilience has led to the focus of the financial industry executives and board members on attaining high-quality oversight. The process of oversight is relatively simple in theory but financial institutions have historically made it extremely complex and unwieldy. In order to root out the inefficiencies and make the process more effective, a straightforward rethinking of the process is needed. This does not mean pulling up the roots and starting again, but defining and mapping the oversight requirements and processes as part of defining the core business requirements. In short 'design in good oversight'.

A relevant thought experiment is to consider one's business without management accounts. It is a large exercise to collate and generate them each month, but it would be close to impossible to run a business without them. Now consider joining a business without a management accounts process and it is clear that the first project would be to put in such an accounting process so at least there is oversight of the financial status of the business. Given the regulatory burden and oversight requirements of modern financial firms, it is not surprising that many institutions are now creating processes to provide oversight of the areas that accounting alone cannot reach.

This approach will support good oversight becoming a standard item, and the days of running around looking for old spreadsheets, presentations and e-mails should become a thing of the past.