BCS CONSULTING

A Defenceless Three Lines

The first line of defence is drowning in an ocean of risk management frameworks. The only lifeline is an integrated approach to non-financial risk management.

At BCS Consulting we only work with clients across financial services. Our portfolio includes a varied range of multinational and UK banks, smaller banks, insurance firms and payment and card companies. Across our 140+ strong team of permanent consultants, we have deep domain knowledge in Capital Markets, Retail and Corporate Banking, Risk and Finance.

Robin Murray
Managing Director
Robin.Murray@bcsconsulting.com

Robert Crewdson
Managing Consultant
Robert.Crewdson@bcsconsulting.com

Lawrence Anderson
Principal Consultant
Lawrence.Anderson@bcsconsulting.com

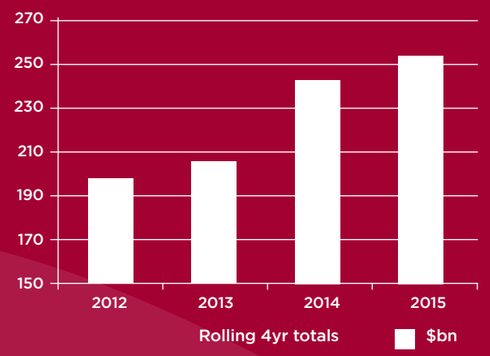
David Thomas
Principal Consultant
David.Thomas@bcsconsulting.com

Published February 2017.

BCS CONSULTING

Financial institutions are experiencing regulatory pressures, costly fines, and escalating losses across a range of non-financial risks and this is driving a (shifting) focus on risk management.

1. **Costs of Conduct Events**



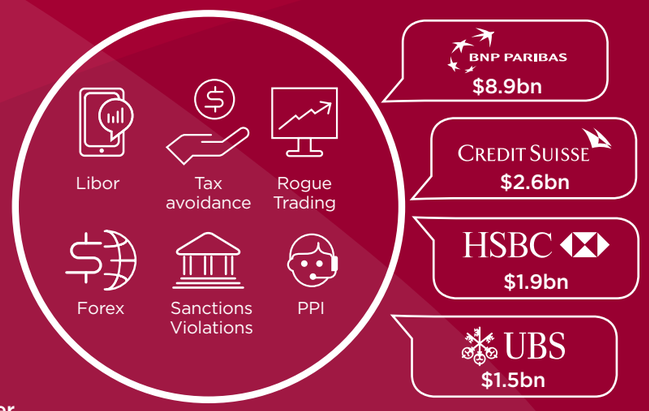
2. **Big increases were seen in 2015 by Lloyds, RBS and Deutsche Bank**

3. **Increased focus on cyber security after a number of high-profile FS and non-FS data breaches. FS firms are twice as likely to have been a victim of cyber crime, with 39% reporting an incident**

4. **£27bn**

in provisions by 5 major UK banks for PPI claims

5. **Increasing cost of regulatory fines across a range of offences**



6. **A UK Government task force has been set up to defend against emerging cyber threats as it is now considered one of the most severe threats facing the UK**

7. **$31bn** **lost to rogue trading (excluding fines and indirect costs) since 1992**

8. **64%**

increase in internet banking fraud in the UK to £134m in 2015

9. **Regulatory change costs banks up to $4bn a year and is driving the agenda for what operational risk teams need to focus on. The latest drivers include the Senior Managers Regime in the UK, and the imminent demise of AMA**

1. & 2. www.conductcosts.ccpresearchfoundation.com/conduct-costs-results
3. www.pwc.com/gx/en/financial-services/publications/assets/pwc-gecs-2014-threats-to-the-financial-services-sector.pdf
4. www.theguardian.com/money/2015/nov/26/fca-unable-to-estimate-future-ppi-cost-to-banks
5. blogs.wsj.com/moneybeat/2014/07/30/the-cost-of-new-banking-regulation-70-2-billion/
6. www.gov.uk/government/news/britains-cyber-security-bolstered-by-world-class-strategy
7. BCS Analysis, "Factbox - UBS trader joins rogues' gallery of financial crime" UK.Reuters.com.
8. www.paconsulting.com/our-thinking/the-new-norm-for-regulatory-change-cost-cutting-and-execution-risk-management/
9. www.next.ft.com/content/e1323e18-0478-11e5-95ad-00144feabdc0

Executive Summary

The first line of defence is drowning in an ever expanding ocean of overlapping risk management frameworks, duplicative processes, unnecessary governance structures and floods of MI.

Each time a regulator raises a question of deficiency and places a new category of operational risk in the spotlight, Financial Services providers respond with another operating model aimed at placating the industry watchdogs. Too little attention is paid to the longer-term implications of a design that should ultimately complement rather than conflict with an overarching framework.

As a result, organisations are often unable to identify and assess their material risks consistently, manage them successfully or report against them accurately. And this can be despite having almost as many second line risk and compliance employees as those dedicated to the business of sales and servicing.

Few would argue that this situation is either efficient or effective, and the management of operational risk needs to be both. Not only do the regulators increasingly demand effective risk management, with the likes of OCC risk management guidance in the US and the individual accountability imposed by the Senior Managers Regime in the UK, but the industry is still reeling from a series of headline-grabbing incidents, whilst also suffering average operational risk losses of €3.01 per €100 of gross income (according to 2015 figures for European institutions, from ORX).

To meet the changing requirements of both regulators and the operating environment, we have seen significant investment in non-financial risk management. Risks are being identified and assessed both within the operational risk management framework (ORMF), and through parallel, and often overlapping frameworks, resulting in a proliferation of methodologies, and associated change initiatives. In most cases the supporting technology infrastructure has not kept pace with changes in the risk function meaning systems are unable to meet the demands of multiple 'enhanced' frameworks or deliver the MI required to support or challenge their efficacy.

This growth in non-financial risk management practices has become a significant burden on financial services organisations. The increasing complexity is both costly and confusing, as the first line of defence is forced to deal with the implications of frameworks enforced by an expanding second line presence. And while the continual implementation of new approaches seemingly satisfies regulators, it also leads to duplicated activity and diminished engagement from the people taking, and managing, the risk. This actually inhibits the firm's understanding of its risks and ultimately its ability to manage exposure effectively.

The reality is that friction between the non-financial risk functions and risk owners is nothing new, but with an increasing focus on non-financial risk management, rising regulatory pressures and the spiralling associated costs, the business should demand more for less.

We advocate taking a step back. Review the frameworks created to support non-financial risk management and strive to consolidate them into a single, holistic, integrated framework encompassing all non-financial risk; a framework that draws together common taxonomies and common processes to deliver standard language and a simplified set of risk management activities. Embed this through a simpler, more pragmatic articulation of roles and responsibilities, using a stripped back Three Lines of Defence Model, and empower your people to better manage your risks.

The irony of implementing a new change programme and risk framework, to resolve the problems of too many change programmes and frameworks, is not lost on us. We believe, however, that only a coordinated, cooperative and collaborative three lines of defence can drive a positive transformation and create a sustainable, beneficial approach to non-financial risk management.

Engulfed by non-financial risk frameworks and assessments

An already complex risk environment has been further complicated by the evolution of additional autonomous, non-financial risk management frameworks. These frameworks typically have different owners, diverse objectives and agendas and require the business to complete duplicative processes leading to confusion, inefficiency and a silo mentality.

We have seen far too many examples in financial services of unclear classifications of operational risk management: what the scope is; where the boundaries lie; and who is responsible for what. In some organisations operational risk covers all 'non-financial' risks, but in others, conduct risk, operational risk, financial crime risk, and regulatory compliance, to name but a few, form distinct functional areas. Each of these areas often operates separately, with a different framework, but perform very similar risk management activities.

> "We've found it difficult to simplify and streamline activities across risk and compliance as each area has invested in, and relies on, their own risk assessments and systems."
>
> Group Operational Risk Executive

This silo mentality presents a challenge to many organisations, and while we are not saying that the only successful non-financial risk management model is one where there is a single function responsible, we do believe that there needs to be an overarching framework with clear roles, transparent responsibilities and an ultimate decision maker.

Unconnected, non-aligned frameworks lead to inconsistent interpretation

Each non-financial risk management framework contains differing definitions of materiality and different ways of classifying the causes and impacts of risks. These principles can often be hard enough to understand individually, but when risk owners are also asked to apply them in parallel, it can result in incongruous application across an organisation.

Moreover, by developing a disparate set of risk management criteria deployed sporadically across business units, corporate functions, and geographies, the ability for each area of an organisation to keep pace with change and align to policies and control requirements of an ever changing regulatory environment becomes very difficult.

A Defenceless Three Lines
Managing Non-Financial Risks

An array of tools and artefacts results in duplication of activity

Establishing and administering multiple risk management frameworks means creating and deploying multiple artefacts, processes and tools. These are generally developed with only their specific risk category in mind and very rarely with a vision of alignment to other risk management structures.

Consequently, a business can have multiple risk & control taxonomies & libraries, risk level classification matrices, risk & control assessment methodologies, internal event processes, issues & actions management processes and systems of record. When examined together, however, there is usually considerable overlap between these activities with those performing them experiencing frequent déjà vu.

Making non-financial risk management costly and inefficient

Organisations have found that performing this multitude of risk management activities is not only highly confusing and time consuming, but prohibitively expensive. With many of the tasks appearing the same and much of the information captured duplicative, it is difficult to demonstrate where the value is being added. This is compounded when the duplication causes bottlenecks in processes and requires data to be input and maintained in multiple systems, which on its own becomes an additional, significant overhead. This negative perspective is further enhanced where unnecessary controls are put in place to mitigate very specific risks, when the enrichment of existing controls (designed for other risk types) would be a more cost effective option.

Creating frustration across the business

With such multifarious frameworks in place, we have found that both risk and control owners feel that they are constantly assessing their risks and reviewing their controls, meaning they're less able to focus on their BAU activities of servicing clients and growing the business. In a typical institution, when risk and control assessments are initiated and require major input from key stakeholders, they are quickly followed by compliance reviews, then conduct risk assessments, IT security evaluations, SOX assessments, control testing and attestations and so on. Each activity becomes a battle for the same resources to review the same set of risks and controls and ask the same senior managers to sign-off the assessments.

Like them, we believe there is a better answer...

Is your first line of defence subjected to similar, additional non-financial risk management requirements?

Too much structure, not enough collaboration

The creation of discrete risk management frameworks to address multiple non-financial risks has delivered a series of overlapping, and sometimes conflicting, artefacts and activities.

Separate taxonomies and libraries covering non-financial risk types include multiple duplicated risk events.

One of our clients tried to consolidate 15 disparate taxonomies relating to non-financial risks causing issues with consolidated board reporting and MI.

RCSAs / ORAs should provide a consistent assessment of operational risks, however, frameworks such as those for Information Security risk create additional assessment methodologies that duplicate effort and cannot be compared back to RCSAs.

A risk owner at one of our clients had to perform six separate assessments of the same risk that fed into various non financial risk programmes.

With the perceived importance of conduct risk, due to regulatory focus and historic fines, firms have put in place control frameworks and organisational models without aligning them to the operational risk framework. This has resulted in disjointed assessments of control effectiveness, risk management siloes and duplicative reporting.

We have seen controls rated effective in conduct risk when assessed against conduct risk incidents, whereas they have been correctly rated ineffective in the RCSA as there were numerous operational risk incidents and manual work arounds identified.

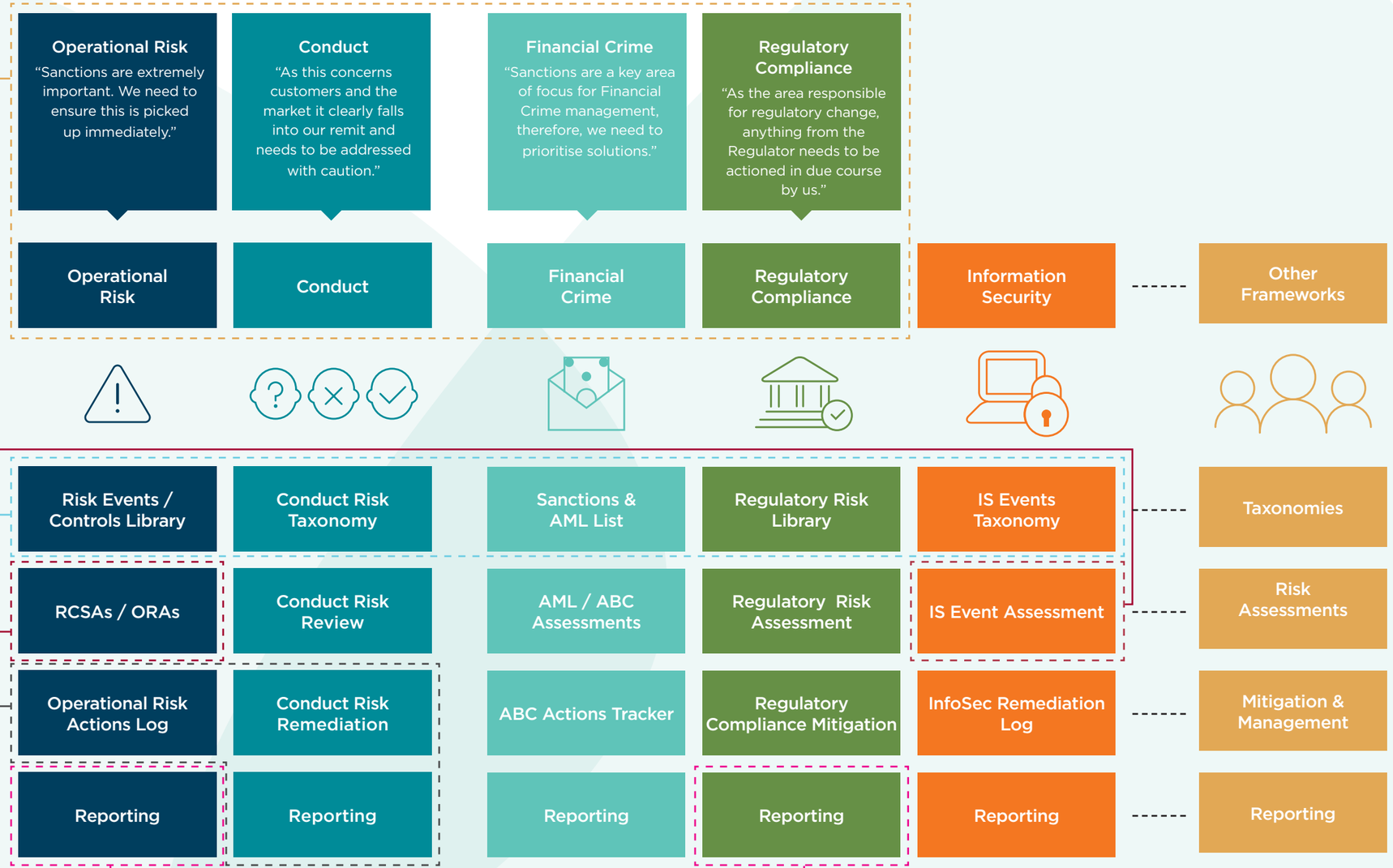
Consider a regulatory focus on an organisation's control framework in relation to sanctions, it's easy to see the overlaps in terms of responsibilities:

Operational Risk
"Sanctions are extremely important. We need to ensure this is picked up immediately."

Conduct
"As this concerns customers and the market it clearly falls into our remit and needs to be addressed with caution."

Financial Crime
"Sanctions are a key area of focus for Financial Crime management, therefore, we need to prioritise solutions."

Regulatory Compliance
"As the area responsible for regulatory change, anything from the Regulator needs to be actioned in due course by us."



With differing data sources and conflicting assessments, based on differing framework methodologies, reports from areas such as Regulatory Compliance are often difficult to reconcile with those from Operational Risk.

Whilst often satisfying individual regulatory and risk-specific reporting requirements many organisations have struggled to provide coherent and accurate views of their overall non-financial risk profile. Most commonly the operational risk view of a specific risk exposure differs from that of the specific risk function.

Reporting on floods of data

Non-financial risk functions are struggling to assimilate and make sense of the volume of data available, which is often duplicative and sometimes conflicting. Unsurprisingly, the resulting reports generally provide a lot of content but little value.

The issues

The proliferation of risk management frameworks has delivered duplication across various framework components and it has only served to complicate what is already a difficult task; to provide meaningful and insightful reporting of operational risk.

Multiple taxonomies influence an organisation's risk language and present problems in finding consistent categorisation and identifying comparable data sets. Consequently, we repeatedly see organisations that are unable to deliver consolidated reporting that brings to life the relationships between risk types. Management require a 'line of sight' through the risk data to understand how information presented at the highest level is influenced by levers in the organisation. Without a cohesive data set, it isn't possible to present a coherent story that articulates the drivers behind changes in risk profile and point to the steps that can be taken to mitigate.

In our experience, the development of multiple non-financial risk frameworks has resulted in the production of data from a wide variety of sources that cannot easily be consolidated for reporting purposes, and does not drive clear decision-making. Where very similar risk types are assessed by different teams using different methodologies from different frameworks, the output is duplicative and even conflicting. Pulling these disparate data sources into a coherent whole is challenging and is exacerbated by the various technology platforms which are implemented independently by businesses and functions.

Identifying the data required, and sourcing it in a useable format is a real constraining factor. Where the data can be sourced, we rarely see single or even a properly connected series of technology solutions across risk functions. Off-system data management tools have been created out of necessity, which doesn't support the objective of running an efficient function.

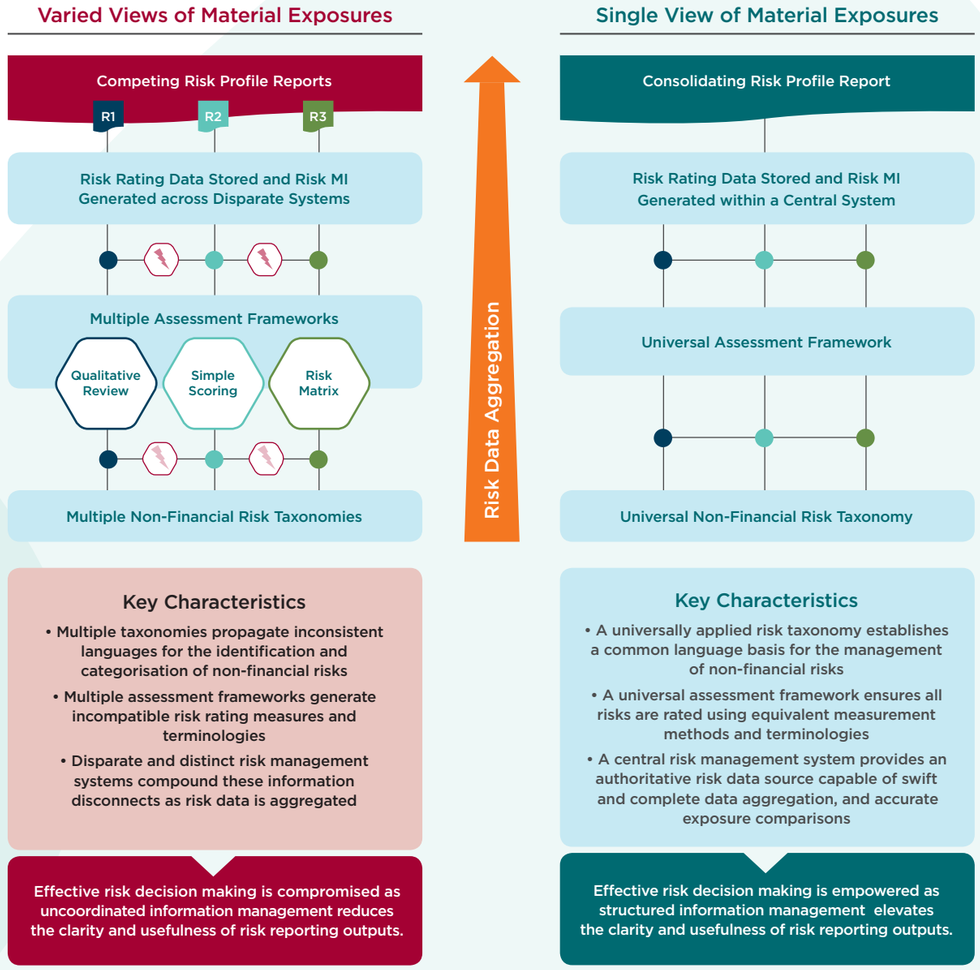
The impacts

The breadth and diversity of available data has made it difficult to aggregate across any dimension, either type of risk, or organisational boundaries. This challenge has become increasingly complex as organisations have implemented competing risk frameworks with independent assessments of the same, or similar, risk types. And the issue is further compounded when we consider the number of diverse systems used to store and analyse this risk data; aggregating diverse data, developed from diverse frameworks, and stored in diverse systems.

When aggregation is not informative, there will be a disconnect between the various views of the firm's risk profile. This is a problem in itself but is compounded when a regulator receives multiple, conflicting reports on the same risk type.

In our experience, finding a way to calibrate the firm's reporting to ensure comparability and effective challenge is vitally important. Without it, management are not able to demonstrate the effectiveness of the framework and there will be a perceived lack of clarity when under regulatory scrutiny.

A Defenceless Three Lines
Managing Non-Financial Risks



> Does the second line of defence work together to ensure that all non-financial risks are understood and managed in a consistent, coordinated manner?

Waves breaching the three lines of defence

Financial services firms have failed to implement effective organisational models to manage risk effectively. While there has been substantial investment in human resource in support of non-financial risk management, it has so far yielded poor returns due to overlapping and poorly articulated accountabilities and responsibilities across all lines of defence.

Maximising the efficiency and effectiveness of people are key to the success of any framework. They need to be empowered to focus effort on the activities that enable them to manage material operational risks. Every individual in an organisation has a role to play, so whatever the approach being defined, they must be provided, not just with the tools and information required to fulfil their role, but clarity as well.

We often see organisations fail to deliver logical and transparent organisational models and they become barriers to the effective use and embedding of their risk management frameworks. With multiple, competing frameworks muddying the waters, and disparate, duplicative risk management activities underpinning them, the workload of the firms' finite human resources has increased considerably. And despite sizeable investment in additional heads and skillsets, organisations are stretched, leading to potential gaps in coverage and variation in quality.

These opaque models also limit a firm's ability to really define accountability – a clear theme through recent regulation which is driving everyone to understand their role in the management of risk: that all employees are responsible for the risk management environment. Transparency and accountability at the highest level are becoming increasingly important. Just consider the fundamental aims of the Senior Managers Regime in the UK as a prime example.

Our observations

- Unclear accountability at the top of an organisation for the management of risk within a firm
- Confusion throughout the rest of these businesses regarding roles and responsibilities
- Wasted time in carrying out a multitude of overlapping and duplicative risk management activities causing employee dissatisfaction

The models implemented to date do not meet the aims of effectiveness and efficiency, and have the potential to generate problematic risk cultures which lack collective responsibility and individual accountability.

A simple, pragmatic solution is required and we believe this is possible through an appropriately designed and carefully embedded Three Lines of Defence Model. But this needs to be approached differently; it will not help to fall into the common trap of referring to roles in relation to the lines of defence. A person's position in the lines of defence depends only on what they are doing, not where they sit within the organisation. It should be noted that people can, and do, wear multiple hats – the model must be flexible enough to handle that. The risk management activities defined under the model need to be streamlined, reducing complexity and wasted effort. They should be linked to the strategic objectives of the firm and incorporated into scorecards to support the embedding process.

We have seen organisations take this simple model and customise it to suit their structure and requirements, but this rarely achieves more than adding complexity, and creating limited-to-negative value. Essentially the model should clearly articulate the need for all employees to be involved in the management of risk, and that activities exposing the business to material risk will require some degree of independent oversight.

A Defenceless Three Lines
Managing Non-Financial Risks

Does your first line of defence appreciate the importance and effectiveness of your operational risk management framework?

Steadying the ship

To drive efficiency in the management of non-financial risks, and ultimately improve risk management practises, financial institutions need to consciously take a more pragmatic and coordinated approach to risk management.

We believe the following actions should be considered:

1 – Develop an Integrated Framework

We have introduced the challenges presented by the industry wide trend of risk management framework proliferation and propose an act of significant consolidation. This starts, in our opinion, with a fit-for-purpose corporate-level Enterprise Risk Management (ERM) function. This is essential in order to define and manage common policies, standards and processes, and must be far more pervasive than the ERM functions that we currently see in financial services. Not only will this function be crucial to ensuring effective decision-making, it will play a fundamental role in developing and implementing the core proposition, which is an integrated framework for non-financial risk management.

In the first instance, this requires a complete and coherent definition of non-financial risk to be agreed, and will necessitate a collaborative approach that breaks down the siloes that have been constructed around the various risk types. Clearly the need for specialist expertise will remain, but by acknowledging the commonalities and working together to develop one overarching framework, we believe that efficiencies can be gained, clarity improved and, most importantly, risks managed more effectively.

Framework integration calls for greater alignment and cooperation between, and within, the three lines of defence. The second line must ensure that the risk experts across each of the non-financial risk types are working together to increase coverage, reduce gaps and drive a consistent approach to risk management through policies and standards. At the same time they should build more effective working relationships with the first line of defence, moving beyond a simple 'checker' role to one which endorses best practice and provides real guidance, alongside the important activities of challenging outcomes and focusing assessments. Of course, independence must be maintained.

The operational risk function (or a broader non-financial risk function) is an obvious place for ownership of this integrated framework; it can align policies and drive standardisation across tools, processes and systems. The function's role should evolve to become one of maintaining integrity in the framework, policing it and coordinating activities across the various non-financial risk categories. It is likely that the function can reduce headcount and complexity as it decreases the breadth of its activities, allocating them to the appropriate experts who are better placed to advise and challenge on matters related to their risk types.

This is not a one-size-fits-all solution; it is important to assess the appropriateness of varying degrees of integration. The basic principles of alignment and standardisation across framework components remain the same, and will deliver efficiency benefits by at least reducing duplication and increasing clarity. The degree to which non-financial risk types are managed under a single framework, however, should be carefully considered with the underlying aim to deliver consistency weighted against idiosyncratic organisational challenges. Better aligned risk coverage will improve the visibility of material risks, enabling the deployment of resources in the right areas and the creation of stronger, more extensive control frameworks.

Create a unified governance structure across all risk types (and businesses) to drive a single, integrated framework underpinned by coordinated policies & standards. This will ensure consistent and coherent decision-making and messaging.

Standardise metrics, reports and analytics to highlight important trends and force appropriate corrective and preventative actions. Ensure the data can be effectively aggregated and facilitates comparison across the various dimensions of risk and business. The reports should strive to tell the story of risk relationships and inform senior management of levers within the organisation to control exposure.

Establish simple processes that can be repeated across the organisation, and that make use of a standard suite of risk, control and performance indicators.

Develop a holistic, standardised risk language with cohesive risk taxonomies and libraries that can be leveraged across risk types and organisational boundaries.

Define assessment methodologies, processes & tools that can be applied across risk types and across the organisation eliminating duplication and gaps of coverage.

Produce 'minimum standard' control libraries based on specific requirements, policies & standards and aligned to cost-benefit investment decisions.

Define clear roles & responsibilities within an appropriate organisational model (lines of defence), which assign the correct individuals to suitable risk management activities. Educate, communicate and embed within the culture.

2 – Enhanced Regulatory Interaction

A key driver in the development of risk frameworks has always been regulatory pressure. The financial services industry has often been too ready to jump on the latest regulatory hot topic and divert attention towards addressing emerging concerns by making wholesale changes that provide demonstrable evidence of action. Instead, a more considered approach that looks at alignment and enhancement of existing frameworks and methodologies will likely result in satisfactory responses to the regulators at lower cost through reduced organisational change.

As a general theme, financial services organisations must build better working relationships with regulators and become more proactive in raising issues and agreeing solutions on hot topics. Not doing so will perpetuate the issues that have historically arisen from reactive responses to industry themes that could be better resolved through close consultation and greater transparency.

3 – Industry collaboration

The ultimate goal of framework integration should see external organisational barriers knocked down. By working together to pool experience, financial institutions could develop an industry standard for management of non-financial risks that takes into account the perspectives of the whole industry. This would also enable the development of a measurable standard by which internal and external challenge can benchmark an organisation.

Industry-wide risk and control taxonomies have been mooted in the past and the adoption of COSO, SOX and ISO standards provide a glimpse of the benefits of consistency, but as yet no such alliances have been formed to help in this area. If non-financial risk management is to progress and be perceived less as an art and more as a science, formalisation of industry-wide frameworks will be a requisite step.

Conclusion

It will be apparent to anyone who is presently working in operational risk management, that the current trends are not sustainable. Developing new frameworks, processes and tools in response to the changing regulatory and business environment, is simply counter-productive. We have seen this drive confusion in both the first and second lines of defence as roles and relationships become unclear, effort is duplicated and outcomes inconsistent. The result is ultimately a lack of clarity in terms of risk exposure and control performance; precisely the opposite of what a risk management framework should be striving to deliver.

3 solutions...

The operational risk function has an opportunity to step forward and:

1. Lead the integration of non-financial risk management frameworks

2. Drive closer collaboration with regulators

3. Engage across the industry to define standards

With the first line of defence drowning and no obvious discernible improvement in the management of non-financial risks, it's time for the operational risk function to throw them a lifeline.

> Does your operational risk function have the mandate and support to drive the changes required?

A Defenceless Three Lines
Managing Non-Financial Risks