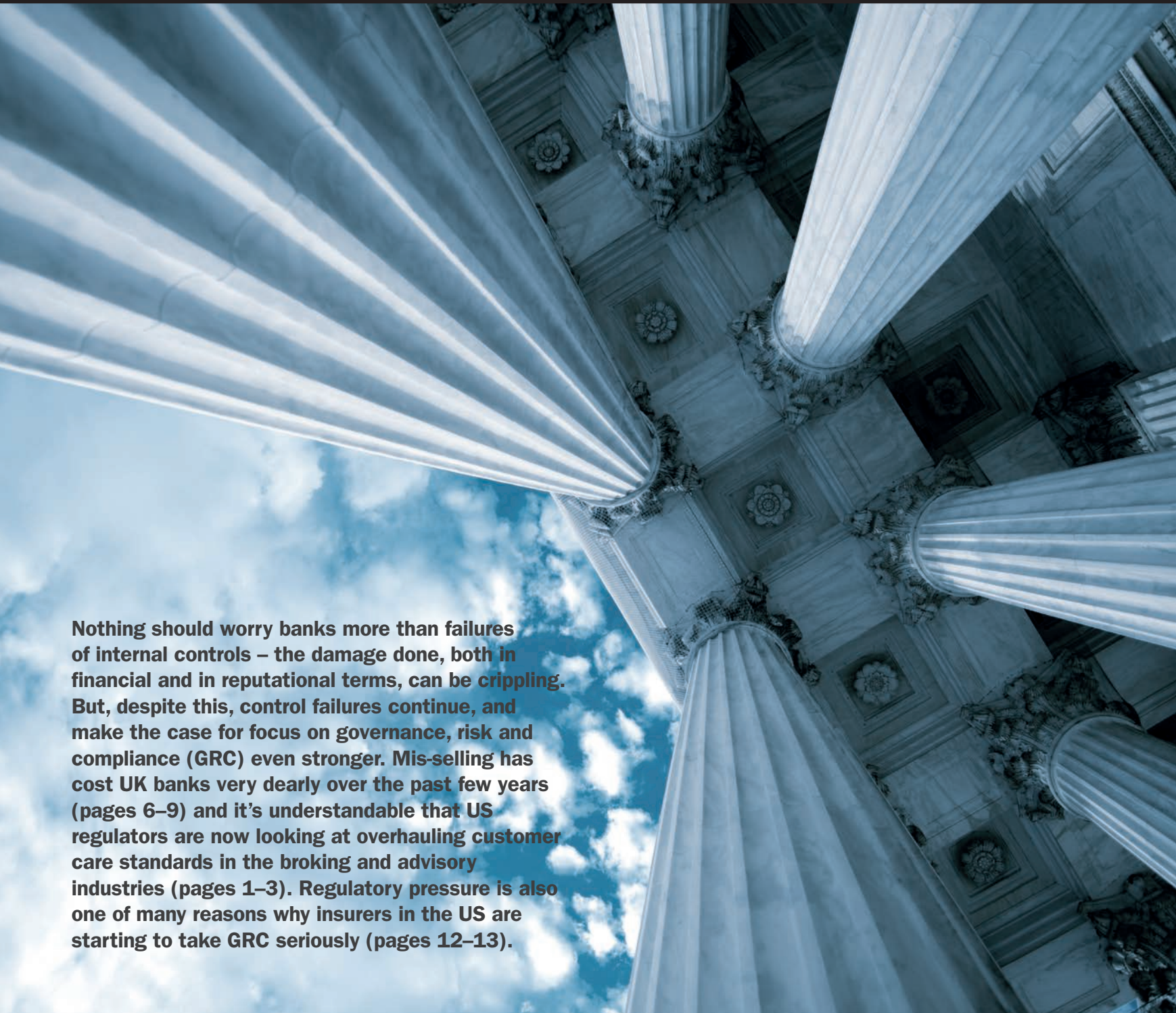


# Operational Risk & Regulation

**GRC**  
Special report



Nothing should worry banks more than failures of internal controls – the damage done, both in financial and in reputational terms, can be crippling. But, despite this, control failures continue, and make the case for focus on governance, risk and compliance (GRC) even stronger. Mis-selling has cost UK banks very dearly over the past few years (pages 6–9) and it's understandable that US regulators are now looking at overhauling customer care standards in the broking and advisory industries (pages 1–3). Regulatory pressure is also one of many reasons why insurers in the US are starting to take GRC seriously (pages 12–13).

Sponsored by



**ORACLE®**  
FINANCIAL SERVICES



# Standard deviations

Investment advice in the US came under scrutiny when Dodd-Frank was signed into law in 2010. An SEC review carried out in January 2011 about aligning standards of care has left the industry waiting to find out exactly what it will be expected to comply with. **Jessica Meek** investigates

When the US Dodd-Frank Act was signed into law in July 2010, one of its key aims was to make the US financial system fairer and clearer for the consumer. Since then, certain sections of the law have been hogging the limelight – Title VII and over-the-counter derivatives reform and the Volcker rule being the most obvious ones. But there are other less-remarked sections of the act that have still been a source of continued debate for Congress and the industry, and which will have wide-reaching effects once implemented – in particular Sections 913 and 914, which cover the obligations of broker-dealers and investment advisers to their clients.

As mandated by these two sections, the US Securities and Exchange Commission (SEC) carried out two studies: the first a study on investment advisers and broker-dealers, as mandated by Section 913 and the second a study on enhancing investment adviser examinations, as mandated by Section 914. Both studies were released in January 2011. One of the main objectives of the study on investment advisers and broker-dealers was to try and understand whether they should both be adhering to the same standards of client care – a uniform fiduciary stand-

ard ([www.risk.net/1564973](http://www.risk.net/1564973)). Debate has raged on the issue since Dodd-Frank addressed it and though no concrete decisions have been made, it is widely expected that at some point in the not-too-distant future, Congress will announce that a uniform fiduciary standard will become law.

To take a step back and understand the context of what this means, it is helpful to look at the current regulation of investment advice in the US. There are presently two types of financial adviser: the first operates as a broker-dealer and the second as a registered investment adviser (RIA). The broker-dealer acts as an agent simply recommending deals that he or she thinks the client should invest in as and when the deals arise. If and when the client makes an investment, the broker-dealer makes a commission on that transaction. An RIA, on the other hand, manages a client's assets and is paid a fee for managing the assets, regardless of how many investments may be made over the course of the year.

Importantly, the two different types of financial adviser are held to different rules and regulations. RIAs have to comply with the US Investment Company Adviser Act of 1940. Broker-dealers do

not. The act lays out a fiduciary standard to which all RIAs must adhere, essentially saying that an RIA must operate only in the best interests of their client and make clear to the client any potential conflict of interest that may for any reason mean that the advice given is not in the best interest of the client.

But the 1940 act exempts broker-dealers from the fiduciary standard it lays out. It states that “any broker or dealer whose performance of such services is solely incidental to the conduct of his business as a broker or dealer and who receives no special compensation therefore” is exempt from the definition of being a registered investment adviser and thus exempt from the fiduciary standard within the act.

What this means is that the standards for RIAs are much higher than those for broker-dealers. The fiduciary standard for an RIA fundamentally says that the adviser is responsible for the recommendations they make to their clients. So the RIA has to have a clear understanding of who their client is and what their client wants. They also need to ensure that all investments made are done so in the best interest of their client, rather than because the RIA might think the investment is a good deal with a high rate of return.

Shutterstock



Accordingly, RIAs have had to introduce detailed onboarding process with specific know-your-customer (KYC) processes for each new client. Marcelo Fava, a Charlotte, North Carolina-based principal for Americas wealth management at EY, explains further: “A registered investment adviser will have to undertake a pretty detailed KYC process with all new clients. This means understanding where your client is in their life stage, their investment objectives, time horizon for the investment, risk profile, what the goals are that the client has in mind for investing a specific amount of assets and so on. All of that needs to be properly done by a registered investment adviser.”

Known as the suitability process, this requires an RIA to ensure that every investment suggestion it makes to the client matches what is in the client’s investment profile. On top of this, the profile needs to be maintained annually in order to document any life changes the client may go through which might alter their investment profile.

Of course, a broker-dealer does not need to do this with the regulations as they currently stand. A broker-dealer technically acts simply as an agent, telling a client that a deal looks good and is worth investing in. The client’s needs and risk profile in relation to the deal are up to the client to determine. Thus the standard to which broker-dealers have to adhere is much lower than that of the RIA.

This is not to say that broker-dealers have low standards or indeed that they don’t operate with their own, perhaps self-imposed, fiduciary standard, but it does mean they are not obliged to adhere to the same higher fiduciary standard as RIAs ([www.risk.net/2046650](http://www.risk.net/2046650)).

### Blurred lines

As might be expected with such similar business models, over the years the lines between RIAs and broker-dealers have become blurred. An example of this is an increase in discretionary accounts – where a broker-dealer may exercise a certain amount of control over the buying and selling of securities from a client’s account without always informing the client – thus managing the assets in more than just the transactional fashion of a traditional broker-dealer. Some broker-dealers also offer a fee-based account, which obviously strays into RIA territory.

On top of this, Fava points out that many of the large broker-dealers also work as RIAs, meaning they already adhere to the RIA fiduciary standard in some

capacity. “They have advisers who wear two hats depending on what he or she is talking to the clients about,” he explains. “I could be a broker-dealer in one relationship with one client or I could be an investment adviser when I work with some other clients. Most of the folks in the US that work for the large investment management firms or wealth management firms have both licences and requirements.”

But when the uniform fiduciary standard comes – and all commentators are certain that it will – there may be significant operational implications for broker-dealers.

“Instead of a point-in-time monitoring of whether an investment you made for a client was the right one, this will be a continuous monitoring which impacts all the way downstream. You have a constant level of responsibility for your client assets and that

---

**“I could be a broker-dealer in one relationship with one client or I could be an investment adviser when I work with some other clients. Most of the folks in the US that work for the large investment management firms or wealth management firms have both licences and requirements”**

Marcelo Fava, EY

would be a monumental change,” says Robert Dicks, leader of Deloitte Consulting’s human capital financial services practice in New York.

Firstly, the uniform fiduciary standard may force broker-dealers to decide how many clients they can cope with at the new continuous level of service, Dicks explains. “There are all kinds of operational and technology implications here,” he says.

For example, broker-dealers will have to go through every client and ensure all of the key points relating to the uniform fiduciary standard are covered. This requires documenting the risk profile, the risk appetite, the investment goals, the time horizon and so on, explains EY’s Fava. “A key challenge will be to go into more detail. It is worth noting that every client for all these organisations is not really one client. Most of us have multiple financial services relation-

ships with multiple accounts, so you have to do this for the individual, not just for the accounts,” he adds.

This householding, as it is called, poses significant operational challenges, not least manpower and changes in documenting processes. On top of this, institutions moving over to the fiduciary standard will have to identify which accounts relate to which investment profile or risk profile, which means trying to match the accounts with the overall investment profile of the client. “This will be quite an undertaking,” says Fava. “Going through the documentation processes, having the right tools, the right platforms to get all of that documented, to keep it updated, having the risk checks, balances and controls, then to go back and make sure that none of this is getting out of sync with what I’m recommending to the client and where the client is now based on their different life stages. It will be something significant.”

### Counting the cost

These operational challenges will, of course, have cost implications. In July this year the Securities Industry and Financial Markets Association (Sifma), an industry association, wrote to the SEC, highlighting what some of those costs might be. The first area it pointed out was the costs involved in developing an upfront disclosure document. This was chosen as an example because the SEC has suggested that this might be a requirement it imposes across brokers and advisers once the uniform fiduciary standard is implemented, explains Kevin Carroll, Washington-based managing director and associate general counsel of Sifma.

“We decided to see if we could identify the costs for building that type of upfront disclosure document for broker-dealers, who don’t have any documents like that today. We asked our members how to go about building that sort of document and what the cost would be both upfront – meaning there would be more costs initially to develop it and vet it – and secondarily the ongoing costs of updating it and maintaining it.”

Carroll explains that the cost components for this would include outside legal fees, outside compliance costs, staff-related costs, out-of-pocket costs and so on. Seventeen of Sifma’s significant member firms submitted cost estimates for creating such a document and while there was no clear consensus on what the cost would be, a cluster of those 17 presented estimates between \$1.2 million and \$4.6 million for

the initial cost. An average estimate of ongoing costs from the majority of firms was \$630,000 a year. “And that’s just for the upfront disclosure document,” Carroll points out.

The second area that Sifma looked at was building the compliance and supervisory procedures for broker-dealers to deal with the uniform fiduciary standard. Carroll describes it as a “significant undertaking” to build a system that contemplates all the elements the fiduciary standard would require. “For that piece of it, the average upfront cost was about \$5 million and that was to build the system and procedures and then thereafter about \$2 million per year to update and maintain it. We got the sense that we were probably in the ballpark with those estimates.”

He explains that they asked members to tell them how much they had spent complying with the new Financial Industry Regulatory Authority (Finra) suitability rule ([www.risk.net/2179909](http://www.risk.net/2179909)) – the standard that broker-dealers currently adhere to, enhanced in July 2012. Sifma chose this as a comparison because of its similarity to the fiduciary standard that broker-dealers will be expected to adhere to. “It is similar in that it’s the type of rule that you have to build a system around when you’re giving advice to a customer. Our members came up with an average of around \$4.6 million to comply with a rule that is similar to the one we expect this fiduciary standard to be.”

It is not just the tangible operational implications or costs that need to be considered where a uniform fiduciary standard is concerned. There will need to be a shift in the relationship broker-dealers have with their clients: it will need to be a continuous management of the relationship rather than the as-and-when basis on which most broker-dealers currently manage their client relationships.

Duane Thompson, Maryland-based senior policy analyst at f360, a service provider for investment advisers, points out that because many brokers are already jointly registered as investment advisers, the transition to a fiduciary standard may not be as difficult as it is sometimes portrayed. He says that broker-dealers are already making the transition by managing assets for a fee as fiduciary advisors under the Investment Advisers Act. “Nearly nine out of 10 investment adviser representatives are dually registered as brokers,” he points out.

However, he is clear that there will be significant cultural issues to overcome for broker-dealers when



Kevin Carroll, Sifma

the transition occurs. “It will take time to change the embedded sales culture on the sell side to a client-centric focus,” he says.

He highlights the review that was carried out to ascertain how the new and enhanced Finra suitability rule is working. The new rule has some fiduciary aspects to it, for example new suitability factors. “Unfortunately, the most common deficiency Finra noted was a lack of documentation of a broker’s ‘hold’ recommendations. This illustrates to me the difference between an adviser’s way of doing business, in which there are typically fewer transactions on the buy side, and the brokerage industry’s need to push product out the door on the sell side.”

### Agents of enforcement

There is also the question of effectively enforcing a uniform fiduciary standard once it is implemented. Broker-dealers are generally examined by the SEC or Finra once every second year, while RIAs are only examined around once every 10 to 13 years.

In June 2012, Richard Ketchum, chairman and chief executive of Finra, spoke before the US House of Representatives Committee on Financial Services about his concerns on this matter. He pointed out that of 4,800 broker-dealer firms registered with the SEC, 55% were examined annually by the SEC and Finra. However, according to the SEC, only 8% of registered investment advisers were examined in 2011 and approximately 38% of advisers registered with the SEC have never been examined.

He also said that the average SEC-registered investment adviser is looked at by regulators only once every 10 to 13 years, and that the frequency of SEC examinations of investment advisers has decreased 50% since 2004. “No one involved in regulating securities and protecting investors can be satisfied with a system where only 8% of regulated firms are examined each year. It is completely unacceptable and represents a major gap in investor protection,” he told the committee.

Sifma’s Carroll agrees. His concerns don’t lie in broker-dealers’ uniform fiduciary standard compliance not being enforced properly, but RIAs not being examined effectively. “Broker-dealers are examined around once every other year by [the SEC or] Finra and so they would get that regular visit and Finra would be familiar with the new standard and they would examine them for compliance with it. A separate issue is on the investment adviser side because they are examined around once every 11 to 13 years and that is where we have an examination shortfall, which represents a risk to investors.”

This “dramatic lack of oversight”, as Ketchum called it when speaking to the House of Representatives, led to Section 914 of Dodd-Frank requiring the SEC to review and analyse its need for enhanced examination and enforcement resources for investment advisers. The result was gloomy. Released in January 2011, the results state that the SEC “will not have sufficient capacity in the near or long term to conduct effective examinations of registered investment advisers with adequate frequency”.

It seems a serious investment is needed in order to facilitate a stricter examination process for investment advisers. While the focus over the coming months may be on the compliance burden the uniform fiduciary standard may bring to broker-dealers, the question of enforcing compliance seems to be more of an issue on the RIA side. Not only that, but the SEC will also have to keep in mind recent history where investment advisers are concerned, in order to ensure compliance enforcement is as effective as it should be.

“Bernie Madoff was technically a fiduciary when the SEC required him to register under the Advisers Act a few years before his Ponzi scheme fell apart,” f360’s Thompson points out. “In order to enforce it, Congress will have to give the SEC the funding it needs to boost examinations of advisors.” ■

# A cultural guide to GRC

**CoreStream** offers a set of considerations when implementing or refining a practice, be it integrated governance, risk & compliance (GRC) or a single risk or compliance area, with the primary aim of fostering the right culture. There isn't a one-size-fits-all approach to effective GRC, but there are common threads that will have a significant impact on the likelihood of success

The term governance, risk and compliance (GRC) means different things to different people. To some, GRC is a vendor-driven term to categorise products and services. Others suggest the scope of GRC is flawed and should encapsulate 'performance' or that the reference to 'governance' should be removed. Is GRC a culture, a practice or a programme?

In truth, it is probably a combination of all three, depending on the level of organisational maturity. Change programmes help implement or revise GRC practice. This practice, if implemented effectively, will help the firm develop a desirable GRC culture. What matters is that the scope of a firm's GRC activity is based on what is optimal for the organisation and the environment in which it operates. Endlessly debating nomenclature will do little for you. Instead, firms would be well advised to focus on a number of practical considerations as they work towards a GRC-aware culture.

## Educate

Making an organisation risk-conscious is imperative. Without this, GRC can become a mandatory bolt-on, viewed as a cumbersome burden on 'real' jobs. Employees who are risk-aware and understand the importance and value of effective GRC are more likely to embrace the content, rather than simply comply by following due process.

Education is necessary to create this awareness. Employees need to understand the importance of GRC, the benefits of an effective approach and the potentially damning consequences of an ineffective one. They also need to be aware of how they contribute to its success.

This awareness helps dispel the myth that GRC is some mythical hard-to-conceptualise theory. People make risk-based decisions several times each day, for example, when crossing the road or deciding on what time to leave for an important meeting. An effective GRC practice formalises this way of thinking and improves the availability and quality of information that informs future decisions.

## Lead and reward

The desired GRC culture is frequently one that is inclusive and collaborative. Mandating policies and rigorously policing them will seldom encourage the desired culture and will likely create an 'us' (the business) and 'them' (audit or risk management teams) relationship that is actually counterproductive.

Adoption is encouraged by leadership setting the correct tone from the top and furthered by incentivising. Embedding GRC within balanced scorecard objectives, for example, helps ensure the spotlight is focused on

performance. Remuneration packages directly attributable to these metrics goes a stage further towards encouraging individuals to make GRC considerations on a routine basis. To reinforce the message, senior management should consider explicitly linking company successes to GRC performance whenever appropriate (commenting on annual results, for example) so a clear benefit is demonstrated to those who operate the processes on a daily basis.

In order to be sustainable, GRC should rely on repeatable processes and knowledge sharing, not on a limited number of specialist risk or compliance professionals operating in isolation. To this end, the business should be encouraged to take ownership and be involved at the control design stage. Processes dictated by remote compliance departments will seldom be as effective as those designed collaboratively, with due consideration for business-as-usual activity. The role of an effective risk or compliance team is to facilitate, advise and review, not independently own the content or approach.

## Help, don't hinder

Organisations should know what it is they are trying to guard against and prioritise controls accordingly. Unnecessary roadblocks that create a compliance burden but do not deliver on specific objectives should be avoided. Disproportionate controls can result in compliance fatigue and be detrimental to developing the desired culture.

GRC culture should encourage proactive prevention. It is less helpful to review what caused the fire once the building has burned down, and so GRC should minimise the likelihood of issues occurring and the impact of them if they do. Processes to detect, report and address issues are important – you don't want the house to burn down repeatedly – but prevention is more beneficial than simply dealing with the clean-up exercise effectively.

Beyond minimising the likelihood or impact of negative events, GRC objectives should comprise positive benefits. Consider the negotiation of a complex contract; an organisation with a deep understanding of risk is able to flex the risk-reward balance more proactively, building a position of strength relative to competitors. More simply, building a reputation as an ethical, compliant, risk-conscious organisation can in itself provide competitive advantage. Communicating these benefits internally helps employees recognise that GRC is not simply a line of defence – it can potentially improve an organisation's performance. GRC is not just about staying out of the headlines.

## Standardise

In organisations where compliance has typically been a reactive undertaking, it is common for a series of silos to have formed. Something goes wrong, regulators or shareholders insist on action and a process change, technology or a particular department is put in place to address the problem. Aside from not benefiting fully from economies of scope, there are other issues attributable to this reactive behaviour. Multiple review functions digging up the same stretch of road repeatedly, but for different reasons, are not only inefficient but can also cause audit fatigue within an organisation. The more burdensome GRC becomes, the more difficult it is to develop the desired culture.

One option is to centralise. A compelling business case can be put forward as technology and resource cost savings are measurable, as are the efficiency gains through reducing duplication. However, the significant cultural, political and operational challenges in centralising disparate units may outweigh the benefits. Whether an organisation chooses to centralise or not, standardisation will almost always drive significant benefits.

The majority of GRC efficiencies are actually gained from having a common framework, common terminology and common reporting. A standardised approach breeds familiarity from shop floor to board level. The former are more likely to embrace something that is less convoluted and the latter can more easily review performance and make decisions using management information (MI) with common categorisation, structure and format.

## Get the best from technology

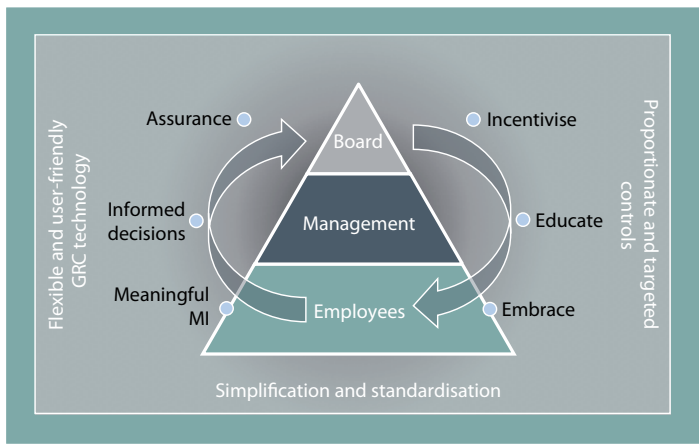
Irrespective of the level of investment or sophistication, technology is not a self-contained GRC solution. It should be regarded as an enabler that improves the efficiency of people and processes; not as a substitute for them.

Technology improves the management of information, highlights potential issues and automates what is repetitive and inefficient. A previously cumbersome process for reporting enterprise-wide operational risk, for example, is far more efficient when data is input to a single register and MI is produced automatically and in a consistent format.

The automation of decision-making should be handled with care. Decisions that lend themselves to automation will typically have few variables and are generally based on a static response to a threshold; when x happens, the consistent response is y. Even when this is the case, the automation is usually only the short-term reaction, and the longer-term response will still need to be determined by management. Absolving people from the responsibility of making decisions is not only impractical, it also serves to distance them from GRC if they believe 'the technology takes care of that'.

The use of GRC technology is also susceptible to the law of diminishing returns. At a basic level, it is notable how many organisations would benefit from simply providing access to central repository for policies, processes and risks. The next step might be to use technology for assigning ownership of controls, or raising and tracking audit issues and associated remedial actions. As the use of technology begins to address more sophisticated areas, management should consider the net benefit of implementing and maintaining a technology-based solution. If 80% of the benefits can be realised with 20% of the effort, it might be wise to stop there. If the

### 1. GRC –The virtuous circle



technology itself is becoming a burden, then the GRC culture will suffer.

Deployed effectively, technology can contribute towards establishing a GRC culture. Technology encourages user adoption and collaboration through being accessible, intuitive and uncomplicated. Experience tells us that the more pleasurable something is to use, the more likely we are to use it. Implemented properly, technology can contribute towards making GRC a habit.

**“Our life is frittered away by detail. Simplify, simplify”**

Henry David Thoreau

## Keep it simple

Keeping things simple is overarching and something to be conscious of at all times. Education can only be effective, collaboration only encouraged and technology only successfully adopted if the content, approach and associated benefits are understandable. You can't expect

to foster a culture outside of GRC professionals if the practice is too complicated to be understood by a wider audience.

While regulation and risks can be inherently complicated, there is no need to add to this complexity by adopting a convoluted response. The most complicated regulation can still often be boiled down to a set of logical controls that are embedded in well-thought-out processes. The most effective GRC practices will address the complexity at the design stage and avoid reflecting it in the controls themselves. Keep the implementation simple and it unlocks the potential to foster the desired culture.

**CoreStream is a UK-based provider of GRC technology solutions, helping our clients manage risk, satisfy compliance obligations and operate more effectively.**

**CoreStream's technology is based on three key principles:**

- Providing an intuitive and pleasurable user experience;
- Being affordable; and
- Rapidly delivering real business benefits.

**To request a free demonstration or a GRC health check, please email [info@corestream.co.uk](mailto:info@corestream.co.uk)**



# Mis-sellers' market

As well as spending billions of pounds in compensation to customers mis-sold both PPI and interest rate hedging products, banks are expected to spend millions on staff, fines and fees for handling complaints. **Miranda Alexander-Webber** looks at the true cost of mis-selling financial products

UK banks have paid out £11.5 billion so far in compensation to customers who were mis-sold payment protection insurance (PPI), and an end to the repayments is not in sight. The latest figures from the Financial Conduct Authority (FCA) show that £528 million was paid back to customers in July 2013, above the average for the year so far at £442 million a month – the total payouts continue to rise (see graph).

And PPI mis-selling is far from being the banks' only concern. Mis-sold interest rate hedging products (IRHPs) are expected to be yet another costly burden to financial institutions. Banks have also had to spend millions in hiring staff to handle complaints, and pay millions more in fines for failing to handle complaints properly. They have also paid fees to the Financial Ombudsman Service (FOS),

which handles complaints that have initially been rejected by the banks. The UK's four biggest banks are expected to pay an estimated £372 million in fees to the FOS for complaints received since 2011 – up to £900 per complaint.

Firms have now received over 6.6 million complaints over PPI since July 1, 2009, figures from the FCA show. The British Bankers' Association (BBA) estimates that banks sold 45 million PPI policies across the market. Provisions against the mis-selling of PPI are now believed to total over £18 billion, of which £15.4 billion has been set aside by the four major UK banks – Lloyds (£7.3 billion), Barclays (£4 billion), RBS (£2.4 billion) and HSBC (£1.7 billion).

Consumers who wish to complain about PPI must first go to their bank, either directly or through a claims management company, although most banks

encourage customers to contact them directly. Thousands of staff have consequently been employed at banks to handle PPI complaints, including 7,300 at Lloyds, 1,320 at HSBC, and 1,800 at RBS.

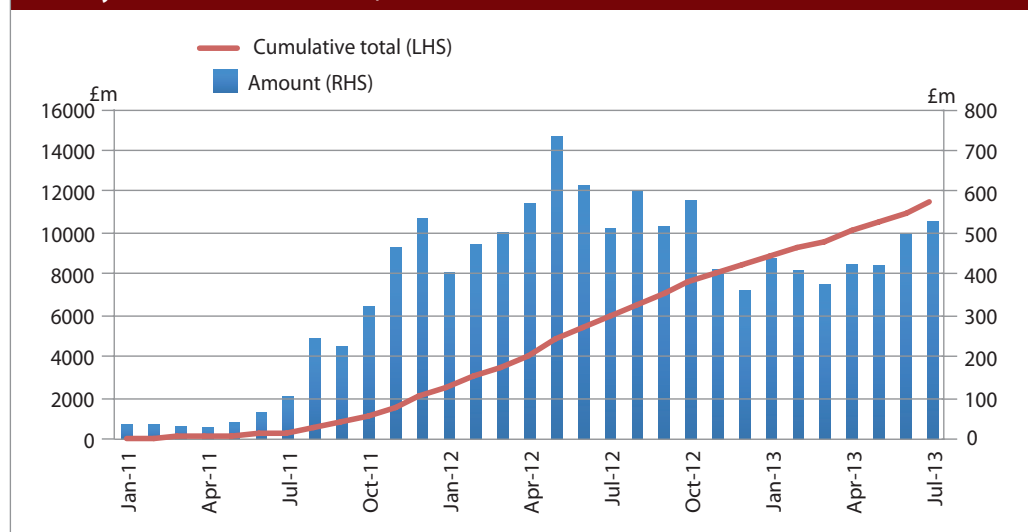
In the case of Barclays, for example, the group had received and processed 1.46 million complaints at June 30, 2013. It upheld an average of 41% of all claims received. This excludes payment of gestures of goodwill and reflecting claims for which no PPI policy exists, Barclays said in its interim results announcement. The average redress per valid claim to date was £2,830.

If they aren't satisfied with the bank's initial response – or if the bank simply fails to respond – consumers have the option of complaining to the FOS. "After eight weeks if they have not heard anything back from the bank then we can look at the complaint. Or else, if they have heard back from the bank and have had a final decision on their complaint but they're not happy with that, then they can bring their complaint to us as well," says a spokesperson for the FOS.

## Pass the buck

Despite banks employing thousands of staff to handle complaints, as well as setting aside billions in provisions, FOS figures suggest thousands of legitimate complaints are being turned down. An average 65% of PPI complaints received by the FOS in the year to March 2013 were upheld in the favour of the consumer. This compares to 82% in 2011/12 and 66% in 2010/11. The most recent figures show that the proportion of complaints upheld against Barclays Bank and what was formerly Lloyds TSB Bank was above the industry average. 74% of PPI complaints received against Barclays Bank in the first half of 2013, for example, were upheld. 90% of the PPI

**PPI PAYOUTS PER MONTH**  
(Monthly amount vs cumulative total)





Getty Images

complaints received against Lloyds TSB Bank, meanwhile, were also found in the favour of the consumer.

A Lloyds spokesperson says: “We are seeing that the ombudsman now agrees with more of our decisions in PPI cases than they have done previously. This measure is improving, but not at the rate that we would want it to, so we are working hard to put it right.”

86% of PPI complaints were upheld against Lloyds TSB Bank in the second half of 2012. This is lower than the 97% upheld against Lloyds subsidiary Black Horse during the same period.

“FOS data refers to only a small percentage of the total number of cases referred to the ombudsman, and is therefore not representative of all cases. In addition, the reason for the overturn on the vast majority of these cases is because the bank, rather than the ombudsman, has instigated the change in decision following a further review of the case,” the spokesperson for Lloyds adds.

A spokesperson at the BBA also says a backlog at the FOS means uphold figures continue to remain

**“These [PPI] numbers are quite high now and probably will continue to be high for a little while, but will start to fall. You’re basically looking at cases that are up to two years old. There’s now much better understanding of what the rules are around this”**

BBA spokesperson

so high. “These numbers are quite high now and probably will continue to be high for a little while, but will start to fall. You’re basically looking at cases that are up to two years old. There’s now much better understanding of what the rules are around this,” he says.

The complaints received by the FOS are small in comparison to the millions dealt with by banks – the

FOS received 191,803 PPI complaints against the UK’s four biggest banks in the first six months of this year. However, this figure is still significant, as banks are charged a £900 fee by the FOS for each PPI complaint received, regardless of whether it is upheld in the favour of the consumer or not.

A supplementary case fee for PPI complaints of £350 was introduced in April 2012 on top of the £550 standard case fee (which is waived for the first 25 complaints per bank). This was to help tackle the unprecedented number of PPI complaints the FOS now has to deal with. More than eight in every 10 complaints that the ombudsman receives are about PPI. It therefore has had to take on 1,000 extra staff to tackle the mis-selling scandal in the past 12 months – and is currently in the process of recruiting another 1,000 staff.

The £900 fee for each case handled therefore raises the question why banks are rejecting thousands of complaints that are actually found to be in the favour of the consumer by the FOS. *OpRisk* has calculated



that the four major UK banks will be expected to pay £372,013,275 for complaints handled since January 2011. While data is not available for complaints received against individual banks before 2011, the industry as a whole is expected to have incurred costs equal to £92,429,500 between 2009 and 2011 (*see table for more details*).

Despite taking on thousands of extra staff, complaints can take anything up to 18 months to resolve. This is partly due to a lack of engagement by some financial institutions, the FOS says. “Disappointingly, some businesses continue to not engage with us – failing to provide us with the information we need in a timely manner which has caused delays to all parties involved,” an FOS spokesman says. In the past, banks – including Lloyds TSB, Bank of Scotland and the Co-operative Bank – have been fined over their failure to compensate consumers in a timely manner.

PPI complaint handling is currently being reviewed by the FCA at six large financial firms responsible for 80% of PPI complaints. In its recent review of 18 medium-sized firms, which only account for 16% of total PPI complaints, it found room for significant improvement. “We found that some of these firms are mainly delivering fair outcomes to PPI complainants but that others still have some way to go, with significant issues that they need to put right,” the FCA report said.

Common deficiencies in complaint handling often occurred when handlers were assessing the merits of a PPI complaint. “We find that complaints are being rejected inappropriately because some complaint handlers are overlooking the inadequate demand and needs assessment carried out at the time of sale,” the FCA cited as an example.

Firms in the review are taking steps to put remedies in place, the FCA report said. One of the firms has also been referred to its enforcement division for further investigation.

A new wave of complaints over mis-sold IRHPs could be a similar financial burden to banks. 30,000 cases are currently being reviewed in which products might have been mis-sold to businesses that were unable to appreciate the true risks involved. This includes potentially mis-sold interest rate derivatives, including structured collars, swaps, simple collars and caps.

A further 16,000 customers assessed as “non-sophisticated” – and thus unsuitable for some IRHPs – have been invited to join the review, the FCA recently announced.

Given that the total value of the 22 redress offers so far made has already reached £1.5 million, the true cost of mis-selling IRHPs is likely to be in the hundreds of millions. The UK’s four biggest banks have now made provisions which stand at over £3 billion – Barclays (£1.5 billion), RBS (£750 million),

Lloyds (£400 million) and HSBC (£375 million).

“Across the board most customers are going to feel there’s been a considerable delay, considering the review was announced in June 2012, and very few customers have received any form of redress so far,” says Richard Hodge, a lawyer at Carter Ruck’s commercial litigation practice in London. The banks are aiming to send out more than 1,000 offers in October, according to the FCA.

To receive redress, a customer must pass a certain number of steps in the review process. They must be a private customer or a retail customer sold an IRHP on or after December 1, 2001. They need to also be of a certain size.

“The thresholds are approximately a turnover of less than £6.5 million, less than 50 employees and a net balance sheet of no more than £3.6 million,” says Hodge. “The product has to have a notional amount of less than £10 million, although there are ongoing judicial review proceedings to challenge that test.”

The biggest grey area is the final test which looks at whether the banks think the customer had the required level of sophistication to understand the products. “If you took out a product, and you had an MBA and dealt in derivatives before then, obviously you’re quite sophisticated, but that’s a bit of a tricky test,” says Hodge.

Banks and independent reviewers have employed 2,800 people to review potential cases of mis-sold

FINAL YEARLY COST OF PPI COMPLAINTS					
Group	Barclays	HSBC	Lloyds	RBS	Total for period
PPI complaints received by the FOS, H1 2013	37,627	15,603	120,640	17,933	191,803
Total estimated fees in £ to the FOS for handling complaints, H1 2013*	32,838,750	13,587,000	105,364,875	15,624,000	167,414,625
PPI complaints received by the FOS, full-year 2012	57,911	21,120	103,974	15,520	198,525
Total estimated fees in £ to the FOS for handling complaints, full-year 2012**	45,633,075	16,261,675	84,522,825	12,379,575	158,797,150
PPI complaints received by the FOS, full-year 2011	21,509	17,000	42,585	11,494	92,588
Total estimated fees in £ to the FOS for handling complaints , full-year 2011***	10,662,500	8,425,000	21,092,000	5,622,000	45,801,500
Total estimated fees paid, January 1, 2011 to June 30, 2013	89,134,325	38,273,675	210,979,700	33,625,575	372,013,275

\* This has been calculated for the 26th and any subsequent case for each institution, as the first 25 cases received by the FOS are free. Half of the cases have been calculated at a fee of £850 and half at a fee of £900. This is because the increased fee of £900 was introduced in April 2013.  
\*\* This has been calculated for the 26th and any subsequent case for each institution, as the first 25 cases received by the FOS are free. 3/4 of these cases have been calculated at the fee during this period of £850, which was introduced in April 2012. A quarter of the cases have been calculated at a fee of £500, which was the charge before April 2012.  
\*\*\* This has been calculated for the 26th and any subsequent case for each institution, as the first 25 cases received by the FOS are free. These have been calculated at the fee of £500 which was charged during this period.

IRHPs and over five million documents have so far been reviewed. Nonetheless, the lack of redress so far is causing concern to many customers.

“Typically, an average case now is four and a half months,” says Fraser Whitehead, a practice group leader and head of the group litigation and commercial services department at law firm Slater & Gordon in London. “We haven’t had a word since we put in our client’s position. What are all these hundreds of people the banks have employed doing?”

Rafi Saville, a partner specialising in forensic accounting and royalty auditing and licensing at chartered accountants HW Fisher & Co in London, has also seen a delay, although he believes progress is now starting to be made. “I had people in my office who were saying they’d been calling the bank every Friday of the last six months and there had been no progress whatsoever. I think they’re getting their act together now,” he says.

The banks, however, are not fully to blame for this delay, according to an industry source. “Each customer has 56 working days to get back to their bank so that builds in a significant time lag, but that means there’s been some delay on the customer side,” the source says.

### Know your limitations

A more rapid response from the banks is nonetheless being urged by customers whose six-year statute of limitation from the trade agreement of their IRHP is fast approaching.

“My great worry is that in the time these people have been waiting, and some would say conned into waiting by the FCA, that their time limits have expired,” says Whitehead. He queries whether the regulator should have told customers not to approach a lawyer.

“Maybe someone should have asked the FSA whether that was a wise thing or whether they’re creating a legal liability on themselves for people who took the FSA at value and now discovered they’ve lost their litigation rights,” he says.

Hodge says this time limit may force some to turn to litigation instead of the FCA’s review process. “If they’re coming up to limitation and if they’re serious about taking action, they’re going to have to do one thing or another,” he says.

A spokesperson for the FCA said as long as customers get their claim form in they will be

considered for the review, adding the review had received a lot of publicity.

As well as facing litigation, the delay in redress is also proving costly for banks as they have agreed to adopt the standard approach used by the FOS when calculating interest on redress – meaning customers will be offered 8% simple interest on top of redress payments.

“You’ve accepted you owe someone money and you’ve accepted you’re paying them 8% and you’re hanging on to it, does that sound like good financial management?” says Whitehead. “They’ll end up paying on nearly all of them eventually, and they’re just going to pay more than they would otherwise have had to.”

Banks might also have to pay further costs as some customers are making a claim for consequential losses. The complicated nature of calculating this is delaying redress even further, although Saville warns

---

**“I’ve never come across a business sector so motivated on the principle that we have an almost unfettered right to cream off what we want from other people’s money. ‘What can we get away with?’ is the motto of the banking industry. That needs to change”**

Fraser Whitehead, Slater & Gordon

that if customers make a claim for consequential losses they risk losing the 8% interest rate.

“The banks do seem to be just offering 8%, but then if you try and calculate your consequential loss they start investigating it,” says Saville. He adds that in some cases it is more worthwhile to the customer to simply accept the 8% interest payment.

Banks may nonetheless be willing to pay for legal, professional or accountancy fees as a result of the IRHP mis-selling.

While the full cost of both PPI and IRHP mis-selling has yet to be fully calculated, banks have started to implement changes to culture and controls to prevent further mis-selling scandals. Obvious failures, however, have left a more permanent damage to the reputation of financial institutions for some.

“It’s a disgrace what happened,” says Whitehead. “The banking industry engaged in a massive operation to sell wholly unsuitable products and in the process of its eagerness to convert loss income streams from one area into new income streams from other areas, it completely lost the plot about what was proper conduct.”

### Sell, sell, sell

And the culture of the firms at the time undoubtedly played a role.

“Was the sales person really focused on asking the customer and understanding from the customer what their real appetite for risk and their loss capacity might be?” asks Jane Woolcott, a partner in risk assurance at PwC in London. “That leads into the question of whether the sales forces themselves had been properly trained, how well were they controlled, what was their remuneration element, was that driving poor behaviours?”

A report published by the FCA in January 2012 found incentive schemes were likely to drive people to mis-sell and that these risks were not being properly managed. For example, the FCA saw one firm where sales staff could earn an incentive of up to 100% of their basic salary for sales of loans and PPI. However, no bonus would be paid unless staff sold PPI to at least 50% of all customers. Another firm operated a ‘super bonus’ scheme competition which was run on a ‘first past the post’ basis for reaching a sales target or threshold. The first 21 people to reach this target earned up to £10,000.

The FCA report said, however, that it welcomed the significant recent changes that a number of firms have made to reduce the risks in their incentive schemes. “There are some very costly remedial exercises that have been undertaken. At the heart of that is putting the customer view first, and I think most of these organisations are recognising that and really actually pushing ahead with that,” says Woolcott.

Not all, however, are as optimistic. Recent research by EY suggests that there is still a long way to go ([www.risk.net/2285833](http://www.risk.net/2285833)).

“I’ve never come across a business sector before that’s so motivated on the principle that we have an almost unfettered right to cream off what we want from other people’s money,” says Whitehead. “‘What can we get away with?’ is the motto of the banking industry. That needs to change.” ■

# Managing enterprise GRC and big data

Effectively managing risk is a big challenge for financial institutions, the manifold aspects of which can affect the best way to approach it. Two of these factors are risk/reward and big data and, in this article, **Oracle Financial Services** discusses both approaches and how they can benefit the governance, risk & compliance process

Managing risks that affect the business is a fundamental activity, as these risks influence an organisation's performance, reputation and future success. With this, the enterprise governance, risk & compliance (GRC) framework is steadily becoming an integral and vital element for enabling financial institutions to operate profitably and effectively. In today's environment, organisations have started to perceive the GRC framework as a tool to provide better corporate governance and performance, rather than it simply being a risk register of their assessments as it has been in the past.

## Risk versus reward

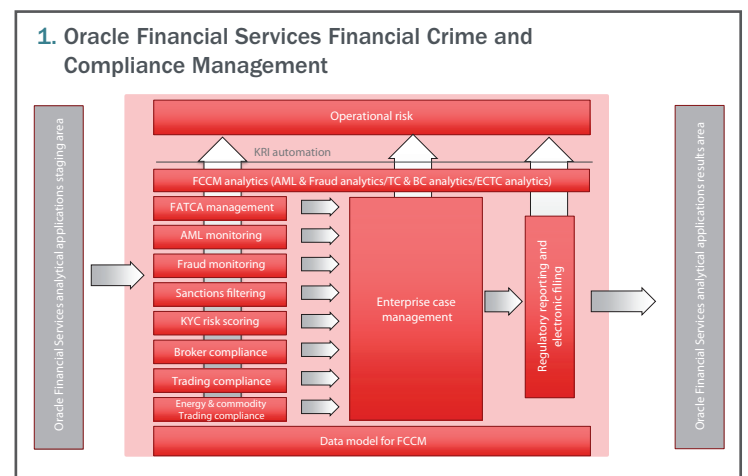
Though risk/reward are two sides of the same coin, they are often looked at and managed in silos. The GRC framework in recent few years has become quite systematic, informative and advanced. It is increasingly becoming the tool of oversight for boards of directors. Hence, organisations are now trying to adopt much more coherent, board-led frameworks for GRC that communicate with all risk departments.

The GRC framework has also seen itself converging with financial crime and compliance systems of late. There are enough touch points between financial crime and compliance management systems and GRC systems to ensure a reduction in financial crime and operational risk losses, which is particularly significant following the recent bank scandals.

Compliance management within the GRC framework has also gained momentum. It has its natural interaction with operational risk, but of more value are the compliance workflows, which aid actual compliance execution, tracking and monitoring and, hence, interjecting compliance assessments with actual facts. There has been a shift in the compliance paradigm from being simply rule books to becoming comprehensive risk-based compliance management.

Though organisations are quite focused on risk and performance independently, and continue to improve these practices extremely effectively, the convergence of these aspects in order to add value to one another has been missing. Setting up the risk and performance objectives and then combining them with the right risk appetite levels could facilitate very useful business portfolio decisions against risk/reward, of which figure 2 provides an illustrative example.<sup>1</sup>

1. Booz & Co., A comprehensive risk appetite framework for banks, <http://www.booz.com/global/home/what-we-think/reports-white-papers/article-display/comprehensive-risk-appetite-framework-banks-2>



## What is required to get there?

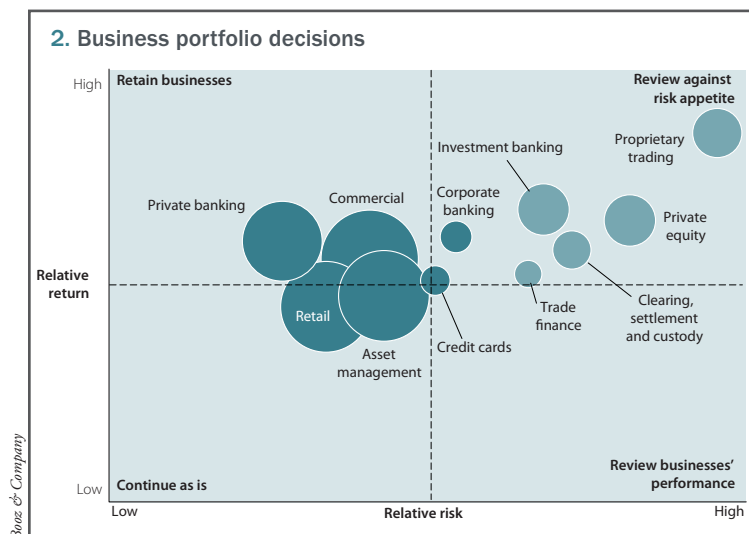
The most important aspect is the creation of a risk-aware and risk-responsive culture, one where risk is embraced in a very receptive, optimistic and proactive manner. Risk is as much about the right culture as it is about people, processes and systems. An aware and risk-responsive culture is one where risk is integrated with strategy setting and its execution. It is important to see the upside and downside impacts of an such an opportunity. Unfortunately, the benefits are so ingrained in us, we quite often overlook the downside impact in an effort to gain instant benefits. However, without sufficient oversight controls, risk appetite and a risk management framework integrated into your business, you will quickly find yourself in situations that will have long-term implications on the business, and especially on its reputation. So, with every new opportunity an organisation needs to identify and assess the possible events associated with the opportunity. It must evaluate how good or bad can it get, and whether it is OK to end up somewhere in between. A comprehensive risk analysis is required before stepping into every opportunity.

## Addressing big data

While trying to balance the risk/reward equation, financial institutions and GRC professionals must tackle the modern-day opportunity of big data. The challenges to be faced and potential lessons to be learned can be huge for an organisation.



## 2. Business portfolio decisions



For example, how can GRC professionals collect, manage and analyse an enormous and disparate volume of data to create and manage their own actionable intelligence covering hidden signs and patterns of criminal activity, the early or retrospective violation of regulations/laws/corporate policies and procedures, emerging risks and weakening controls, etc.? Not exactly the stuff of James Bond, but certainly more applicable to most GRC professionals' day-to-day challenges.

### How can big data benefit the GRC process?

As revealed by recent Forrester research, high-performing companies – effectively, those that are growing 15% or more year-on-year compared to their peers – are taking a selective approach to investing in big data.

There is an ever-increasing volume of regulatory demands and fines for getting it wrong, limited resource availability and out-of-date or inadequate GRC systems all contributing to a higher cost of compliance and/or higher risk profile than desired – a big-data investment in GRC clearly falls into this category.

However, to make the most of big data, organisations must evolve both their business and IT procedures, processes, people and infrastructures to handle these new high-volume, high-velocity, high-variety sources of data and be able integrate them with the pre-existing company data to be analysed.

GRC big data clearly allows an organisation access to and management over a huge amount of often very sensitive information that can help create a more risk-intelligent organisation. This also presents numerous data governance challenges, including those of regulatory compliance and information security.

In addition to client and regulatory demands over better information security and data protection, the sheer amount of information that organisations deal with and the need to swiftly access, classify, protect and manage that information can quickly become a key issue from a legal, as well as technical or operational, standpoint. However, by making information governance processes a bigger part of everyday operations, organisations can ensure data remains readily available and protected.

### The right GRC and big-data partnership is key

To make a big-data GRC initiative work and get the desired value, partnerships with companies that have a long history of success in delivering successful GRC solutions, as well as being at the very forefront of technology innovation, become key.

The solutions that stand out and should be explored are those that can seamlessly merge the traditional world of well-known data, analytics and visualisation with the new world of seemingly innumerable data sources, utilising big-data technologies to generate new GRC insights right across the enterprise. Ultimately, big data is here to stay, and organisations that embrace its potential and outline a viable strategy, as well as understand and build a solid analytical foundation, will be the ones that are best-positioned to make the most of it.

### A blueprint and roadmap service for big data

Big-data adoption is first and foremost a business decision. As such, it is essential that your partner can align your strategies, goals and objectives with an architecture vision and roadmap to accelerate adoption of big data for your environment, as well as establish practical, effective governance that will maintain a well-managed environment going forward.

While your initiatives will clearly vary, there are some generic steps the team and organisation will be required to complete at the outset of the process:

- Clearly define your drivers, strategies, goals, objectives and requirements as they relate to big data.
- Conduct a big-data readiness and information architecture maturity assessment.
- Develop future-state big-data architecture, including views across all relevant architecture domains, businesses, applications, information and technology.
- Provide initial guidance on big-data candidate selection for migrations or implementation.
- Develop a strategic roadmap and implementation plan that reflects a prioritisation of initiatives based on business impact and technology dependency, and an incremental integration approach for evolving your current state to the target future state in a manner that represents the least amount of risk and impact of change on the business.
- Provide recommendations for practical, effective data governance, data quality management and information life-cycle management to maintain a well-managed environment.
- Conduct an executive workshop with recommendations and next steps.

There is little debate that managing risk and data are the two biggest obstacles encountered by financial institutions. Big data is here to stay and risk management certainly is not going anywhere, and ultimately financial services industry organisations that embrace its potential and outline a viable strategy, as well as understand and build a solid analytical foundation, will be best positioned to make the most of it.

For more information on Oracle Financial Services' GRC solution, contact Matthew Long, Financial Crime and Compliance, at [matthew.long@oracle.com](mailto:matthew.long@oracle.com)

# A governing principle?

GRC platforms are gaining popularity for insurers in the US, particularly in light of Orsa. But with a changing business environment alongside an increased regulatory focus, insurance companies need to be sure about what they're investing in. **Jessica Meek** investigates

Operational risk heads at US insurers are increasingly turning their attention to governance, risk and compliance (GRC) systems. At the insurers that already have them in place, the phones are ringing regularly as their peers seek advice. Kay Rahardjo, chief operational risk officer at US insurer The Hartford, has frequent conversations with her counterparts at other companies about The Hartford's GRC platform, and comments: "That really seems to be a fertile area."

The reasons for this momentum in US insurers moving towards GRC platforms vary depending on who you speak to, but the Own Risk and Solvency Assessment (Orsa) mandated by the US National Association of Insurance Commissioners is one important factor, as is the general regulatory climate in which US insurers now operate.

Rahardjo links the push towards GRC platforms directly to the increased regulatory pressure US insurers are facing ([www.risk.net/2288948](http://www.risk.net/2288948)). She added that an increased focus generally on operational risk means having a GRC system is making more and more sense for US insurers. "How else do you pull it together if you don't have a systematic way of doing it? GRC allows you to

have a systematic approach to managing your operational risk."

Rahardjo is not alone in seeing GRC as a response to increasing regulatory exigency. Tom Sullivan, former Connecticut insurance commissioner and principal in PwC's financial services regulatory practice, thinks the momentum towards GRC is understandable, especially in light of Orsa ([www.risk.net/2264255](http://www.risk.net/2264255)): "I think when you look at it through that lens, you can appreciate why people are looking at enterprise risk management (ERM) frameworks through a compliance GRC lens, because they know that there is a mandate out there – Orsa – and they are going to have to comply. The optionality is no longer a 'nice to have', it's a mandate."

Others doubt that Orsa is the main reason. The changing business environment in which US insurers find themselves may provide more insight into why insurers are shooting for new GRC platforms, according to Matthew McCorry, New York-based national leader of KPMG's insurance risk practice. Specifically, he says, the push towards GRC for US insurers is being driven by the economics of the business first and foremost. "If you look at our interest rate environment over the last several years,

it's pinching the profit and loss of all these companies, particularly in the property and casualty and the life insurance sectors," he points out.

On top of this, insurers are dealing with increased competition, which has developed over a short period of time, according to McCorry. This is because of the increase in competition not only in the US and Europe, but also in emerging and growth markets, such as China, Brazil and India. He warns that for insurance companies, both organic and inorganic growth are difficult to find at the moment, so insurers need to have the ability to understand their risk fully and establish whether it is as profitable to the extent that they felt it was over previous years. All of this means that US insurers may find that their existing GRC systems are not up to scratch.

"This is pushing older GRC platforms into becoming what is needed now – more efficient, more results-oriented processes for understanding appetites and tolerances so that people understand what the business is doing in a much quicker fashion," McCorry explains.

This also raises the question of efficiency, which is another factor pushing the move towards GRC platforms for US insurers. Historically, GRC platforms

were less technologically advanced than the modern-day platform requires in order to be an effective tool for US insurers to meet their requirements. “A lot of the historical GRC systems didn’t necessarily have the best technology involved; it wasn’t the best way to structure the requirements and needs for both business and compliance purposes. In addition, the people involved had a different skill set than what they are looking for today,” McCorry points out.

With the increased focus on compliance and operational risk for insurers, it is clear that GRC platforms can assist with this, but as McCorry points out, get your business right and the other elements will follow. “If you look at the best-in-class companies, they are making sure the business issues are what we’re trying to tackle first with the GRC platform that they are putting in place. If you deal with those the right way, the compliance challenges – including regulatory reform – are much easier to implement.”

Alongside this, insurers’ enterprise risk management (ERM) programmes are becoming more of a focus for regulators – and also for rating agencies. While this too may now be influencing the move towards GRC platforms for US insurers, it has been on the agenda for longer than Orsa. Rating agencies have been looking at US insurers’ ERM for some time. In 2005, Standard & Poor’s (S&P) began incorporating ERM into its ratings assessment methodology for life insurers. Moody’s and Fitch did the same and, following the shift by the rating agencies, there has been an increased use of ERM by insurers and a clearer understanding of its importance, according to reports issued by S&P since it began including ERM in its ratings of US insurers.

Rahardjo agrees that the rating agencies’ focus on ERM is stronger now than ever before. “We’re really feeling a lot of interest in ERM and interest from our regulators as well as from all of the rating agencies. We deal with four main rating agencies and they are all so much more interested in risk than they ever were before, so we are definitely feeling the interest.”

PwC’s Sullivan thinks this is also having an impact on US insurers’ move towards GRC platforms. He points out that S&P now issues an ERM rating for most of the major insurers, so being able to present ERM information in an organised fashion – via a GRC platform – can only improve your rating. “An ERM rating generally speaks to how well managed you are and how well capitalised you are. When

it comes to the rating agencies – much like the regulators – they are going to want to see that and so the only way you are going to be able to demonstrate it is if you have that level of structure around it.”

### Not a cure-all

However, some commentators are warning that GRC may not be the panacea that some in the industry expect. Jerry Shafran, Pittsburgh-based chief executive of technology provider Compliance Assurance Corporation (CAC), reports an unclear picture: “There is certainly momentum [towards GRCs], but there is confusion. And I hate to say it but the confusion is vendor driven. The concept of what real GRC or a real platform is, is something that we have found there is a lot of differing opinions on. GRC has been portrayed as a panacea for the changing environment that insurers find themselves under. And when you look under the cover and you peel back the onion of what is being promoted, you find that in many cases the GRC solutions out there are in one of two classes: they are either not really fit for purpose and can be expensive and difficult to implement, or they are a suite of non-integrated products that have been branded as GRC.”

---

**“You can appreciate why people are looking at enterprise risk management frameworks through a compliance GRC lens, because they know that there is a mandate out there – Orsa”**

Tom Sullivan, PwC



Mike MacDonagh, a London-based risk and compliance specialist at provider Wolters Kluwer Financial Services, agrees. He points out that most GRC vendors started out life as something else, such as IT risk management, business process management or audit management, which means that there are going to be weaknesses in those platforms and confusion for the buyer. “GRC is a bit like customer relationship management was a few years ago – everyone wants to be a GRC vendor and their claims don’t always stand up. Because most GRC vendors started life as something else, you can at least often gain an insight into their strengths and weaknesses from considering that. But this approach, and the fact that the analysts also differ in their opinions about what constitutes GRC, make it very hard for firms to make informed decisions.”

On top of this, GRC platforms are covering areas that have traditionally been addressed through different governance structures, processes and platforms, such as market risk, liquidity risk, insurance risk and operational risk, KPMG’s McCorry explains. This adds to the confusion. Combine this with the other factors US insurers are dealing with and the difficulties are significant.

“I think insurers are frustrated slightly, not only because of the complexity involved with integrating an enterprise GRC platform, but also an ever-changing landscape of more operational needs of management to run the business and changing regulatory requirements,” McCorry says.

The frustration also lies in the notion of GRC being portrayed as the panacea for US insurers’ regulatory needs. As PwC’s Sullivan points out, Orsa certainly doesn’t mandate insurers to implement a GRC platform. They are expected to explain how they run their business, what that means from a capital and solvency perspective in terms of how they fund their business and how well capitalised an insurer is for potential risks that might threaten the business. “It doesn’t say get a GRC platform, it says tell us your story of how you manage your business, how you contemplate risks, how you identify risks, how you measure risks, how you conduct stress testing, how you look at your broader capital and solvency position and how well prepared you are to weather those storms. That’s what Orsa asks you, so I can see why there is some of that frustration in the market because Orsa doesn’t say ‘go and buy a GRC [system]’.” ■