Winning the risk governance battle

Questions they'd prefer you didn't ask

Anita D. Millar

July 2009

Risk, Regulation & Strategy Ltd.

JWG IT

The Think-Tank for EU Driven IT Change in Financial Services

About this research: The research in this document has been conducted by ADM Risk, Regulation & Strategy with contributions and comments gratefully received from JWG-IT. It is based on the author's:

- experience of evaluating firm risk frameworks
- analysis of industry practice (as evidenced in the annual reports of various financial services firms)
- distillation of guidance and practices adopted/discussed by the regulatory community (e.g., ARROW II and CEBS' work on the Supervisory Review process under Pillar 2)
- review of a number of recent publications relating to the topic and cited in the article. Of particular note are the Turner Review, CEBS' consultation paper (CP24) entitled 'High-level principles for risk management', the Shareholder Report on UBS' Write-Downs, and JWG-IT's Analysis Report "*What if ... you could have heard the bubble bursting?"*

About the author: Anita D. Millar is proprietor of ADM Risk, Regulation & Strategy (www.AdmAdvisory.com) and has 18 years' experience of working in the risk and regulatory arena in both risk and audit at financial services firms in Canada and the UK and as an independent consultant and sub-contractor to top tier consultancy firms. Prior to setting up ADM and between 2000 and 2002 she developed the Royal Bank of Scotland Group's lobbying platform on Basel II and established RBSG's dialogue with the FSA and international regulatory community. Since then she has contributed to the regulatory and industry dialogues on Pillar 2 and MiFID.

About JWG-IT: JWG-IT is the only Financial Services industry think-tank to facilitate collaborative work to resolve industry issues created by regulatory change better, quicker, cheaper and with less risk. Based on a working model started in 2005, JWG-IT has established strong relationships with EU administrators, leading firms and technology companies. It is neither lobbyist nor consultancy and revenues are restricted to membership fees and content sales. In 2008, the JWG-IT Think-Tank established the Liquidity Risk Action Network (LiRAN) and the Customer Data Management Group (CDMG) which is developing industry guidance for the UK's FSA. For more information, see: www.jwg-it.eu, www.liquidity-risk.info or email info@jwg-it.eu.

Contents

1 The current economic and regulatory environment

In response to the global recession and unstable markets, we have seen politicians and regulators attempt to identify and address the management failures contributing directly to the losses and insolvencies we now associate with significant segments of the financial services sector. For instance, on 15 November 2008, the G20 leaders agreed that regulators 'should develop enhanced guidance to strengthen banks' risk management practices, in line with international best practices, and should encourage financial firms to re-examine their internal controls and implement strengthened policies for sound risk management' by 31 March 2009.[1]

Following this declaration, in the UK we have had the FSA's Turner Review and the current Walker Review of bank corporate governance.[2] In the EU, the Committee of European Banking Supervisors (CEBS) has issued a consultation paper (CP24) entitled 'High-level principles for risk management'[3] and the European Commission has proposed governance upgrades to the Capital Requirements Directive[4]. Although the industry is currently focused on a number of more immediate initiatives, such as those addressing liquidity risk, regulatory efforts like the Walker Review or CP24 may have a significant long-term impact on the way regulators look at how firms are managed and signal the type of pressure that might be brought to bear on senior managers and boards.

Even if the new rules or guidance coming out of the Walker Review, CP24 and similar initiatives are significant, will they immediately help boards and senior management assess and identify shortcomings in their approach to risk management? Probably not – the purpose of rules and guidance is not to explicitly identify the key outcomes that stakeholders expect senior managers and boards of financial services firms to track to assure themselves and their stakeholders that firm risk frameworks are sound and supported by a dynamic approach to risk governance.

What boards and senior managers need are outcome-focused tests for soundness that will help them move from merely concentrating on the form of a firm's risk framework – a static view of risk management – to having the ability to focus on what a risk framework should deliver and how good risk governance supports this delivery. Like houses, risk frameworks can take a variety of shapes and forms, but what is fundamental is that they keep their occupants warm, dry and safe.

2 Tests for soundness

So is there a set of basic questions that will test the soundness of a firm's risk management framework? Can these be framed for use by board and senior management and be independent of any given risk silo, provide a summary view of the firm's approach to risk and

---

[1] The full G20 declaration of 15 November can be found at: http://www.g20.org/Documents/g20_summit_declaration.pdf

[2] For more on the Turner review see – http://www.fsa.gov.uk/pubs/other/turner_review.pdf – and for more on the Walker Review of Corporate Governance in the UK banking industry see – http://www.hm-treasury.gov.uk/walker_review_information.htm. The conclusions of the review are expected in October 2009 based on evidence gathered since February 2009 and feedback on the 16 July 2009 Walker consultation document.

[3] CEBS' consultation on CP24, 'High-level-principles for risk management', attempts to consider gaps in current guidance addressing risk management focusing on areas of: (i) risk appetite and risk tolerance, the role of the Chief Risk Officer and risk management functions; and (ii) risk management models and integration of the risk management areas and the new product approval policy and process – http://www.c-ebs.org/getdoc/0861a22e-0eb8-4449-9b3a-f4b1959267c7/CP24_High-level-principles-for-risk-management.aspx

[4] http://ec.europa.eu/internal_market/bank/regcapital/index_en.htm

offer some measure of assurance to the board, senior management and the firm's stakeholders?[5]

We would like to suggest ten tests and discuss (i) their relevance and (ii) the further questions senior managers and board members can ask when evaluating them. Many of these tests will be instantly recognisable to risk practitioners and regulators but they are not often discussed together and/or explicitly in terms of risk governance and/or with the view of supporting senior managers in their assessment of their firm's risk frameworks.

1.	Risk appetite/risk tolerance	Does the firm's risk governance support the communication and implementation of a consistent series of board decisions relating to risk appetite/risk tolerance?
2.	Planning	Does the firm's risk governance structure ensure that the financial services firm's capital, strategic and new product/new business planning is treated as a board level concern and is directly informed by the firm's risk profile and how its risk profile may change given the planning decisions taken?
3.	Risk-taking	Does the firm's risk governance structure put responsibility for taking on new business, and the risk associated with it, with the business?
4.	Reporting lines	Can the firm show that its reporting lines are clear, precise, well-defined and coherent?
5.	Risk process and conflicts of interest	Can the firm show that responsibilities for its risk process are clearly articulated, allocated and enforced, as well as taking into direct consideration the conflicts of interest that might arise if responsibilities for risk control and risk assurance are not sufficiently segregated from each other or from other components of the risk process?
6.	Risk tools and measures	Does the financial services firm's risk governance structure require that the ownership and responsibility for the integrity and use of risk tools and measures be clearly articulated and enforced?
7.	Risk identification	Does the financial services firm's risk governance require that its principal risk categories be fully articulated and make provision for the identification and accommodation of risks falling outside these strict definitions and/or new and/or emerging risks?
8.	Monitoring, reporting and escalation	Does the financial services firm's governance structure specify responsibilities for monitoring and reporting, and ensure that its monitoring and reporting capabilities are sufficiently resourced?
9.	Challenge and culture	Does the financial firm's governance help to cultivate challenge and simultaneously recognise the function that risk, compliance and audit roles fulfil in challenging the business?
10.	Committee transparency and performance	Is the firm's risk governance underpinned by management committees with clearly defined responsibilities for risk and risk-related issues, and are these committees able to demonstrate their effectiveness in responding to risk-related issues in a timely and appropriate manner?

[5] Financial services firms have a wide number of stakeholders including their regulators, shareholders, debt-holders, employees and the communities they work in.

Of course, one question is whether any of the ten is more important than the others. Although we would like to suggest that all ten are essential to the continuing health of a financial services firm, one of the aims of this article is to generate a wider discussion of these outcomes/benchmarks, their definition, their relationship to one another and their relative weighting.

Test 1: Risk appetite/risk tolerance

Does the firm's risk governance support the communication and implementation of a consistent series of board decisions relating to risk appetite/risk tolerance?

Risk appetite is generally understood to be an umbrella term encapsulating risk tolerance and normally makes reference to a firm's overall risk capacity. Classic indicators of risk appetite are a target credit rating or target capital ratios. Risk tolerance, on the other hand, is normally understood to be a more narrow statement and is generally presented as an acceptable level of variation around some objective. For example, in an operational risk context, account servicing losses due to operational failures is a common risk indicator, is viewed as a cost of doing business and is often described as a risk tolerance.

However, no matter how it has defined these terms, the firm needs to deploy them consistently both across and within its risk silos. If it speaks of, say, its credit limits as measures of risk appetite but concentration limits as measures of risk tolerances, what is it saying? Likewise, if a credit limit is identified as a risk appetite but a liquidity ratio that measures liquid cashflows on the balance sheet is described as a risk tolerance, then how can anyone internally or externally appreciate whether these risks and measures are viewed and treated comparably?[6] So, has the board defined these concepts and deployed them consistently? In turn, have the board and senior management demanded discipline in how these concepts get attached to the numerous limits and thresholds set across the bank so that they can obtain some assurance that the firm is operating within the parameters they have set for it?[7]

Effective implementation requires that the senior management/board be assured that business is operating within the parameters being set by the board. So, have risk appetite/risk tolerances been cascaded down from the group to legal entities, each business and for each risk? Are statements of risk appetite linked to risk policies and procedures?

Test 2: Planning

Does the firm's risk governance structure ensure that the financial services firm's capital, strategic and new product/new business planning is treated as a board level concern and is directly informed by the firm's risk profile and how its risk profile may change given the planning decisions taken?[8]

---

[6] In CP24, CEBS also discusses risk appetite/risk tolerance but does not clearly distinguish between them and, in fact, appears to use the terms interchangeably. Nevertheless, CP24 is clear that senior management needs to ensure that trading, credit, liquidity and other risk limits remain within the firm's overall risk appetite, even in a stressed economic environment.

[7] In a liquidity risk context, JWG-IT has highlighted the extensive quantitative and qualitative liquidity data that the FSA is proposing boards and senior management review. See press release of 8 June 2009 – http://www.jwg-it.eu/20090608_CP0914_MA – in relation to the FSA's CP09/14 Strengthening liquidity standards 3: Liquidity transitional measures, June 2009 – http://www.fsa.gov.uk/pubs/cp/cp09_14.pdf – that follows on, in part, from the FSA's CP08/22 *Strengthening liquidity standards*, December 2008 – http://www.fsa.gov.uk/pubs/cp/cp08_22.pdf – which highlights the responsibilities of a firm's senior management and board.

[8] It is worth noting that in CP24, CEBS also underlines the importance of a new product approval policy process. CEBS' comments are largely product-focused and do not include new business; but it does stress that new products,

The inclusion of risk profile information in planning is essential. It helps to ensure that a financial firm's board is acting with a full set of information when setting business objectives.

Under Basel II and the Capital Requirements Directive (CRD), consideration of a financial services firm's risk profile in its capital planning process should now be demonstrated via the firm's mandatory ICAAP (Internal Capital Adequacy Assessment Process) filing. So, when evaluating 'capital planning', a senior manager or board member needs to ask whether the firm has filed a successful ICAAP with its regulator (i.e. one that has not been returned with a demand that it be rewritten and resubmitted).

Linked to the capital planning process should be the wider process for transforming high-level business strategy into detailed shorter-term business plans. So, has the firm generated such a process and in what manner have the risks associated with the plan been reflected and planned for?

Finally, does the firm have a formal new business/new product process and, if so, is it a mandatory process? Can it be bypassed? Can the risk function reject the plan, and is risk information captured and considered under the process? For example, when a new business venture is being targeted at a new market, how is the firm collecting client information so that it is accurate and up to date and allows the firm to gain an aggregate view of its customers by product type? If, say, the firm is relying on third parties for client information it needs to be able to independently verify the accuracy of this information, otherwise its venture could fail commercially or be judged inappropriate for its client base.

Test 3: Risk-taking

Does the firm's risk governance structure put responsibility for taking on new business, and the risk associated with it, with the business?

Putting risk-taking with the business helps to ensure the independence of the risk function and to promote challenge, but it needs to be controlled. UBS, in its widely read *Shareholder Report on UBS's Write-Downs*,[9] clearly states that compensation was a contributory factor leading to the losses announced in 2007 and the first quarter of 2008. Problems arose at UBS, in part, because its compensation and bonus structure (i) did not differentiate between returns based on skill in creating additional returns versus returns made from exploiting UBS's comparatively low cost of funding in carry trades; (ii) did not recognise, to any significant degree, risk issues or adjust for risk/other quantitative factors such as internal audit ratings, operational risk indicators or compliance issues; and (iii) had insufficient incentives to protect the UBS franchise where bonuses were measured against gross revenue after personnel costs, with no formal account taken of the quality or sustainability of those earnings.

In the UK, the FSA draft code on remuneration[10] is instructive but voluntary, so it may well be ignored by firms fighting for 'talent'. However, remuneration in the financial services is a widespread concern[11] and as guidance and codes are put in place, boards of directors will

---

markets and businesses should be analysed carefully and firms should ensure that they have the tools and expertise to understand and monitor the risks associated with them.

[9] For UBS's shareholder report, see http://www.ubs.com/1/e/media_overview/media_global/search1/search10?newsId=140329

[10] For more on the FSA's proposed code on remuneration and the consultation paper underpinning the code, see: http://www.fsa.gov.uk/pages/Library/Other_publications/Miscellaneous/2009/cop_remun.shtml and http://www.fsa.gov.uk/pubs/cp/cp09_10.pdf

[11] On 2 April, the G20 leaders agreed to endorse and implement the FSF's (Financial Stability Forum, now succeeded by the Financial Stability Board (FSB)) principles on pay and compensation and to support sustainable compensation schemes and corporate social responsibility of all firms. See

be pressured to look for ways to control risk-taking as they are made to focus on (i) the potential impact of uncontrolled risk-taking on the long-term viability of their firms and (ii) reputation costs to their firms of not adhering to these codes. As stated by the Financial Stability Forum (now the Financial Stability Board), most governing bodies of financial firms 'have viewed compensation systems as being largely unrelated to risk management and risk governance. This must change.'[12]

So, is the business's performance assessed against some risk-adjusted hurdle? Does the firm's bonus structure promote a short-term view with a focus on revenues rather than risk-adjusted profits? Although bonuses can be no less than zero, are bonuses still paid when the firm's financial performance or the individual's performance have been poor? Does the firm's remuneration structure differentiate between business and operational staff? Does risk management have appropriate access to the board and the firm's compensation committee?[13]

Test 4: Reporting lines

Can the firm show that its reporting lines are clear, precise, well-defined and coherent?

Well-defined reporting lines ensure that (i) issues get escalated and (ii) key management information and direction are communicated. However, the larger and more complex the firm, the more likely matrix management has been adopted whereby business and operational staff have multiple reporting lines with potentially competing geographic and functional objectives. Such structures create ambiguity over employee supervision and reporting obligations, particularly where the matrix structure (which demands that that staff manage trade-offs between competing objectives) is overlaid with linear compensation and management of these competing objectives. In a risk context, this can result in line risk/compliance or audit managers being unable to locate the appropriate pathway to escalate issues or, in fact, acting against the interests of their careers in any attempt to escalate issues. This could result in 'issues' falling between the cracks and not being owned by any of the competing management streams. In a trading floor context, global matrix management could lead to neither the functional supervisor nor the local supervisor owning responsibility for control over a trader's book and the misconduct it might reflect.[14]

So, are all the firm's reporting lines clearly documented and communicated? Has the firm attempted to streamline multiple reporting lines, introducing them only when they are absolutely necessary and re-examining whether triple or even quadruple lines are necessary?

---

http://www.g20.org/Documents/g20_communique_020409.pdf for the *London Summit – Leader's Statement 2 April 2009.* Also, see http://www.financialstabilityBoard.org/publications/r_0904b.pdf?noframes=1 for the *FSF Principles for Sound Compensation Practices 2 April 2009.*

[12] From the *FSF Principles for Sound Compensation Practices 2 April 2009.*

[13] As per SIFMA's (Securities Industry and Financial Markets Association) *Guidelines for Compensation*, 10 June 2009 – http://www.sifma.org/legislative/savings/pdf/SIFMA-Comp-Guidelines-06-09.pdf

[14] On 16 June 2007 the FSA disclosed that it was fining the London Branch of the Toronto Dominion Bank under the FSA's Principle 3 because it failed to take reasonable care to organise and control its affairs with adequate risk management systems. The case makes interesting reading, not because of the magnitude of the losses involved, but because it is fairly straightforward and the FSA's detailed discussion of the case makes reference to the firm's matrix management and ineffective supervisory control over the Trader's book – http://www.fsa.gov.uk/pubs/final/Toronto_Dominion_Bank.pdf

Test 5: Risk process and conflicts of interest

Can the firm show that responsibilities for its risk process[15] are clearly articulated, allocated and enforced, as well as taking into direct consideration the conflicts of interest that might arise if responsibilities for risk control[16] and risk assurance[17] are not sufficiently segregated from each other or from other components of the risk process?

Conflicts of interest can arise within any of the risk or compliance silos and at any point in the risk process.[18] In a credit context, it would be inadvisable for a single business credit unit to have responsibilities for relationship management, credit documentation and releasing cash funds to clients. Similarly, in a liquidity risk context, as suggested under Recommendation 3 of CEBS' 2008 technical advice on liquidity, 'special attention should be paid to the powers and responsibilities of the unit in charge of providing funds'. Operational and monitoring functions should be segregated.[19] In a compliance and operational context, a number of potential conflicts of interest can also arise over: the gathering of client information; the collation, management of and access to client data; and the end use of the data to determine MiFID client classifications and results of suitability and appropriateness tests.[20]

So has the firm defined all its risk processes? Has it differentiated its risk control from its wider processes? Has it differentiated risk assurance from its wider processes? Has it actively addressed where conflicts of interest can arise and sought to address these conflicts? Where these conflicts are not possible to resolve with a segregation of duties, has the firm instituted any other mitigating controls such as third party review or some other form of oversight?

Test 6: Risk tools and measures

Does the financial services firm's risk governance structure require that the ownership and responsibility for the integrity and use of risk tools and measures[21] be clearly articulated and enforced?

Risk and compliance units across financial services firms deploy a number of risk tools and measures. Some are simple, while others are complex; however, if they are not governed,

---

[15] A financial services firm's risk process, in general, spans the identification of risk and its assessment, plus its management, controls, policies and procedures, reporting and actions taken by a firm given the information produced by the risk process.

[16]Within a financial services firm, risk control is typically understood to be a subset of a bank's risk process generally concerned with the establishment of control policies and procedures and verifying that these policies and procedures are complied with.

[17]Within a financial services firm, risk assurance is typically understood to be concerned with verifying that the risk controls put in place are effective and efficient. It is generally a function fulfilled by an internal audit.

[18] Within a risk process, conflicts of interest could undermine the reliability of the process and/or can create the appearance of an impropriety. Although often associated with improper acts for personal gain, conflicts of interest exist even if no improper acts result from them.

[19] For CEBS' September 2008 technical advice on liquidity, see http://www.c-ebs.org/getdoc/bcadd664-d06b-42bb-b6d5-67c8ff48d11d/20081809CEBS_2008_147_(Advice-on-liquidity_2nd-par.aspx

[20] Under the EU's Markets in Financial Instruments Directive (MiFID) there are two main categories of client, 'retail' and 'professional', and a separate and distinct third category for a limited range of business, 'eligible counterparty'.

[21] In a market risk context VAR is a measure that some might also refer to as a risk tool. In a credit risk context expected positive exposure (EPE) is a measure seen as a tool. We speak of 'tools and measures' rather than one or the other so as not to exclude measures or tools that some might view as falling more naturally into one category than the other.

then the insights they offer could be obscured and/or used for tasks for which they are unsuited and/or misapplied and/or compromised.[22]

For example, consider the problem of account-churning where there are allegations of excessive trading on client accounts. A typical indicator is a turnover ratio that measures how often, on average, the securities in a customer's portfolio are traded in a year. The ratio is meant to be deployed as an alert that there could be inappropriate trading and that further investigation is warranted, and not as absolute proof that inappropriate trading has occurred. If the tool and its conclusions are misunderstood, there is a potential for misdirected or inadequate action. Likewise, if the tool is not safeguarded, there is the potential that ratios could be compromised and potential incidences of account-churning could go unreported.

In a liquidity risk context, design authority for tools and measures deployed to arrive at a firm's Individual Liquidity Adequacy Assessment (ILAA) will help to determine the success of the firm's ILAA submission to the FSA. If the liquidity tools and measures are questioned by the FSA, the outcome of the Supervisory Liquidity Review Process (SLRP) will probably be unfavourable for the firm, leading to any number of requirements such as an increased liquidity buffer and/or a request to redo its ILAA.

So, does the firm assign ownership for risk tools and measures, and does the firm track where and how risk tools/measures are being leveraged? Is there a process for introducing and agreeing design changes?

Test 7: Risk identification

Does the financial services firm's risk governance require that its principal risk categories be fully articulated and make provision for the identification and accommodation of risks falling outside these strict definitions and/or new and/or emerging risks?

In its Shareholder Report on UBS's Write-Downs, UBS provides just one example of how not fully identifying current risks can lead to a firm not managing its risk profile and losses; more specifically, the report found that UBS's risk factor loss (RFL) measures did not identify factors relevant to sub-prime exposures, such as delinquency rates or real estate price development. The Basel Committee has recently looked at the interaction between market and credit risk and suggested that the commonly held view – that simply summing up separately measured risk components is conservative – just does not hold up (as, say, in the case of a bank making foreign currency loans to domestic borrowers).[23] Likewise, recent work on liquidity risk by CEBS seeks to identify how liquidity risk interacts with credit risk, market risk, concentration risk, operational risk and reputation risk.[24] Financial services firms that assess risks strictly according to the definitions of their principal risk, and do not examine their risks for potential interactions and/or compounding effects, may find that their businesses are significantly outside the risk appetite set by the board.

---

[22] In CP 24, CEBS further highlights the importance of recognising the practical and conceptual limitations of models, although no comment is made regarding model governance and how it helps to ensure that the limitations of models are taken into account.

[23] For more on the possible compounding effects of credit and market risk, see the BCBS' *Working Paper No. 16 Findings on the interaction of market and credit risk, May 2009* – http://www.bis.org/publ/bcbs_wp16.pdf?noframes=1

[24] *Second Part of CEBS' Technical Advice to the European Commission on Liquidity Risk Management – Analysis of specific issues listed by the Commission and challenges not currently addressed in the EEA*, 18 September 2008. See – http://www.c-ebs.org/getdoc/bcadd664-d06b-42bb-b6d5-67c8ff48d11d/20081809CEBS_2008_147_(Advice-on-liquidity_2nd-par.aspx

In terms of considering the impact of new and emerging risks, the impact of the economic downturn, as evidenced by government bail-outs, demonstrates that a significant number of financial services firms did not fully consider the impact of a downturn scenario on their balance sheets.

So, how can a financial services firm assess whether it is fully identifying risks associated with its current business and potential new risks on the horizon? Board and senior management can ask: (i) Has the firm defined its principal risks? (ii) Does the firm have a process for managing risks that fall between these principal risk categories and/or is there a process to challenge the firm's categorisation of principal risks in light of new risks? (iii) Does the firm have a stress-testing programme that seeks to examine the relationships between the risks it faces, to identify its vulnerability to risks that cannot be easily categorised, and to complement its other risk management tools such as value-at-risk (VAR)?[25] (iv) Is there a process for managing new risks or newly identified risks whereby they are brought to the attention of senior management and/or the board and ownership for these risks is assigned and resources for their management allocated?

Test 8: Monitoring, reporting and escalation

Does the financial services firm's governance structure specify responsibilities for monitoring and reporting, and ensure that its monitoring and reporting capabilities are sufficiently resourced?

Without monitoring, effective reporting and a clear pathway and procedure for escalating information, the board and senior management can neither assess whether the business is operating within the parameters set for it, nor make informed planning decisions based on its current risk profile, nor take mitigating action against new risks. For example, without formal monitoring, reporting and escalation, in a credit context, a business line that is empowered to grant credit might easily exceed its delegated authorities. In a liquidity context, as per the FSA's CP09/13, *Strengthening liquidity standards 2: Liquidity reporting*, the FSA is asking senior management if they have an appropriate place for capturing, managing and escalating liquidity risk.[26]

So, (i) can the firm identify its key risk reports, discuss why they are viewed as key and name which of the risk metrics and limits are central to these reports? (ii) Is reporting sufficiently frequent? (iii) Are the reports meaningful? For example, are the reports overly complex? Do they assist senior management or merely document events and actions taken before report publication? (iv) On what basis are issues highlighted in management reports escalated? For example, do they include triggers or forward-looking indicators (e.g. a spike in the credit-line utilisations) that warrant the escalation of the issue to a more senior management committee? (v) Can issues be escalated outside the formal reporting process and/or are confidential pathways available to junior business and operational staff that might require the attention of senior management? (vi) Do the bank's management information systems support meaningful reporting across the Group? For example, if risk scorecards and/or dashboards are used in management reporting, are they populated manually and with timely information?

---

[25] The BCBS' *Principles for sound stress testing practices and supervision*, May 2008 – http://www.bis.org/publ/bcbs155.pdf?noframes=1 – provides detailed guidance on the use of stress testing and integration regarding risk governance.

[26] See Annex I of CP09/13 http://www.fsa.gov.uk/pubs/cp/cp09_13.pdf

Test 9: Challenge and culture

Does the financial firm's governance help to cultivate challenge and simultaneously recognise the function that risk, compliance and audit roles fulfil in challenging the business?

The word 'challenge' is a strong one and, for some, has negative connotations. Challenge need not be aggressive, but it does need to be professional, fact-driven and investigatory. Moreover, it needs to be accepted as essential to the health of a financial services firm. Although insufficient challenge can result in losses in earnings, capital and/or reputation, asking questions in many financial services firms, particularly of senior management who are in the business or are insufficiently independent of the business, can mean the end of a career even for those whose job it is to ask questions, whether they be in risk, compliance or audit. Although, arguably, all members of staff are legally covered by whistle-blowing legislation, this does not protect their future, nor shelter them from the intimidation that can follow if the questions they asked cannot be answered without discomfort by the firm and/or individuals within it.

So, (i) does the firm listen to the concerns of all its stakeholders? For instance, does the CEO support the airing of alternative points of view at the board or executive committee level and/or has the chief risk officer (or equivalent) been given the right to fully and formally communicate his or her concerns? (ii) Has the financial services firm (and/or its stakeholders) adopted any metrics that might allow it to assess the health of the challenge culture within the firm? For example, does it review the distribution of audit report ratings and question if the distribution is skewed or just leave that to the audit committee? Has it looked at the profile of its managers, considered how similar profiles can invite herding and/or whether the profiles of groups that are left, after it has made cutbacks in a downturn, are so homogenous that they may actually exacerbate the challenges facing the firm, rather than providing the original solutions that are needed? Has the firm ever taken action as the consequence of information gathered by Human Resources during employee exit interviews? How many compromise agreements has the firm agreed to, and are the board, its senior management committees and/or the audit committees tracking the frequency of these agreements? (iii) Has the board or senior management actively looked for alternative methods of introducing challenge into the firm?[27]

Test 10: Committee transparency and performance

Is the firm's risk governance underpinned by management committees with clearly defined responsibilities for risk and risk-related issues, and are these committees able to demonstrate their effectiveness in responding to risk-related issues in a timely and appropriate manner?

A complicated and/or opaque committee structure and process make it difficult to determine where risk issues should be escalated or where final responsibility for the issues lies. It can result in inaction and/or a lack of senior management ownership for risk issues. When discussing risk governance, many firms tend to focus on describing senior management committees and their existence in a manner that makes them appear disengaged from the day-to-day workings of the financial services firm. This approach will become increasingly unsustainable as pressure is exerted on, say, the asset and liability management committees to be transparent about the frequency of their meetings and to show that they are proactive and able to tackle the technicalities of liquidity risk management issues as they occur.

[27] In CP 24, CEBS does not address the issue of challenge directly; however, in the context of discussing the role of the Chief Risk Officer, CEBS recommends that the CRO (or equivalent) should have the seniority and independence necessary for him or her 'to challenge and potentially veto the decision-making process of the institution'.

So, (i) are the senior management and risk committees clearly identified and empowered? For example, do they share a formal and standardised term of reference, documenting their responsibilities for risk and risk-related issues, identifying their membership, and documenting what constitutes a quorum? Are these committees clearly mandated to take action on a subset of issues? Does the firm clearly differentiate between committees with mandates to take action and forums where ideas are exchanged? (ii) Are key documents and minutes accessible and the responsibility of a secretariat(s) or central repository? (iii) Can senior management and risk committees show that they do not just rubber-stamp decisions taken by the business and provide clear and solid examples of taking action on risk issues and/or instigating an investigation on risk-related issues without the prompting of an external body?

3 Conclusion

These ten tests are designed to help firms locate structural flaws or weaknesses in their risk frameworks. If these flaws are not addressed with action and resources, a firm's board and senior management will be at risk of not meeting their obligations to their stakeholders. This could lead to both financial and reputation losses for the firm and its directors.

While these tests are not exhaustive and invite challenge, they demonstrate that risk frameworks cannot be discussed without tackling the governance that underpins them. By focusing on basic questions, risk governance can help firms leverage insights from across the organisation in a constructive and managed way.

As indicated at the start, there is a plethora of regulatory initiatives focusing on shortfalls in corporate and risk governance. Will the work of Walker, CEBS, the EU Commission and the UK's FSA and other bodies help to promote a fuller and more balanced view of governance? On balance, probably 'yes'. Will these debates raise the bar for boards? Most certainly 'yes'. However, it should fall to each and every firm to define what risk governance is appropriate for their individual business models. Picking the right tests to pass and proving that the system works will appear on the board's governance agenda for some time to come.

The Think-Tank for EU Driven IT Change in Financial Services

Risk, Regulation & Strategy Ltd.

Registered in England and Wales. Registration No. 05862494
2nd Floor, 145-157 St John Street, London EC1V 4PY
Tel: +44 20 7870 8004 Fax: +44 20 7900 6855
www.jwg-it.eu admin@jwg-it.eu