



# 10 KEY PREDICTIONS FOR 2011

#### Also in this issue

- DO WE HAVE ANYTHING NEW SINCE 2008 TO OFFER PROTECTION FROM A NEW CRISIS?
- BANK INTERNAL AUDIT...THIRD LINE OF DEFENCE OR FIRST LINE OF ATTACK?
- BEYOND THE CALCULATION KERNEL: SOLVENCY II'S PROPORTIONATE ROGUES!
- REASSESSING AND UPDATING CREDIT ANALYSIS AND MODELS
- OPERATIONAL RISK – HERE ARE THE NEW RULES, SAME AS THE OLD RULES
- HELICOPTERS DROPPING MONEY OR THE NEED FOR A NEW WORLD ORDER

# OPERATIONAL RISK – HERE ARE THE NEW RULES, SAME AS THE OLD RULES

*In December 2010 the Bank for International Settlements (BIS) turned its attention back to operational risk. As you know operational risk was clearly at the heart of the financial crisis so changes had to be made. OK so operational risk is really nothing whatsoever to do with the crisis – but nonetheless the BIS have chosen now when there is so much other change going on, to make changes. Two papers have been produced, one setting out principles for sound practice and the other providing guidance for banks using the Advanced Measurement Approach (AMA). In this article key elements are set out, although for more information you will still need to make reference to the original papers, the links for which appear on the Risk Reward Global Risk Forum, a closed group on LinkedIn.*

## **The Sound Practice for the Management and Supervision of Operational Risk**

This was issued by the BIS in December 2010 for comment by 25 February 2011. Remember that the original sound practices paper was issued in 2003, so the question is whether there is anything really new in this paper.

This consultative document incorporates the evolution of sound practice and details eleven principles of sound operational risk management covering:

- (1) governance,
- (2) risk management environment and
- (3) the role of disclosure.

By publishing an updated paper, the Committee enhances the 2003 sound practices framework with specific and updated principles and guidelines for the management of operational risk that are consistent with sound industry practice. It is claimed that these enhanced guidelines have been developed through the ongoing exchange of ideas between supervisors and industry since 2003 and becomes

the document that is referenced in paragraph 651 of Basel II.

So here are the principles:

### **Fundamental principle of operational risk management**

**Principle 1:** The board of directors should take the lead in establishing the “tone at the top” which promotes a strong risk management culture. The board of directors and senior management<sup>7</sup> should establish a corporate culture that is guided by strong risk management and that supports and provides appropriate standards and incentives for professional and responsible behaviour. In this regard, it is the responsibility of the board of directors<sup>8</sup> to ensure that a strong operational risk management culture exists throughout the whole business.

There are requirements for the board to establish a code of conduct or an ethics policy and clear expectations that bank staff should understand their roles and responsibilities for risk, as well as their authority to act. In common with the current tone of regulation, compensation policies should be

aligned to the bank’s statement of risk appetite and tolerance, long-term strategic direction, financial goals and overall safety and soundness. They should also appropriately balance risk and reward.

There is a welcome focus again on training with an appropriate level of operational risk training being required at all levels throughout the organisation.

**Principle 2:** Banks should develop, implement and maintain a Framework that is fully integrated into the bank’s overall risk management processes. The Framework for operational risk management chosen by an individual bank will depend on a range of factors, including its nature, size, complexity and risk profile.

The policies defining the Framework should clearly:

- (a) identify the governance structures used to manage operational risk, including reporting lines and accountabilities;
- (b) describe the risk assessment tools and how they are used;
- (c) describe the bank’s accepted

## OPERATIONAL RISK – HERE ARE THE NEW RULES, SAME AS THE OLD RULES

- operational risk profile, permissible thresholds or tolerances for inherent and residual risk, and approved risk mitigation strategies and instruments;
- (d) describe the bank's approach to establishing and monitoring thresholds or tolerances for inherent and residual risk exposure;
  - (e) establish risk reporting and Management Information System (MIS)
  - (f) provide for a common taxonomy of operational risk terms to ensure consistency of risk identification, exposure rating and risk management objectives;
  - (g) provide for appropriate independent review and assessment of operational risk; and
  - (h) require the policies to be revised whenever a material change in the operational risk profile of the bank occurs.

Of these it is perhaps that in balance they are indicating that additional quantification is required, with a common language (or taxonomy) being at the heart of the issue.

### Governance<sup>9</sup> The Board of Directors

**Principle 3:** The board of directors should establish, approve and periodically review the Framework. The board of directors should oversee senior management to ensure that the policies, processes and systems are implemented effectively at all decision levels.

There is an expectation that there should be dynamic oversight by the board of directors, which suggests a level of reporting to the board which frequently does not currently exist. Recognise that this is in the sound practices paper and therefore applies to all banks regardless of size, so for many smaller firms this will be quite a challenge.

There is also focus on division of duties with the control environment being required to provide appropriate independence/separation of duties between operational risk control functions, business lines and support functions.

**Principle 4:** The board of directors

should approve and review a risk appetite and tolerance statement<sup>10</sup> for operational risk that articulates the nature, types, and levels of operational risk that the bank is willing to assume.

The objective here is for the risk appetite to be consistent between operational risk types to enable consistent reporting. In our view this requires a single metric to be translated into different metrics depending on the nature of the risk. Many firms are still challenged by risk appetite and have failed to grasp its significance in developing a risk management framework, so this additional clarification in the paper is welcomed.

### Senior Management

**Principle 5:** Senior management should develop for approval by the board of directors a clear, effective and robust governance structure with well defined, transparent and consistent lines of responsibility. Senior management is responsible for consistently implementing and maintaining throughout the organisation policies, processes and systems for managing operational risk in all of the bank's material products, services and activities, consistent with the risk appetite and tolerance.

The paper is clearly trying to raise the profile of operational risk management to make it consistent with all of the other areas of risk management. There is additional focus on the governance structure, making it clear that combined enterprise risk management is required. The rules proposed state that governance structure should be commensurate with the nature, size, complexity and risk profile of its activities. When designing the operational risk governance structure, a bank should take the following into consideration:

(a) Committee structure – Sound industry practice for larger and more complex organisations with a central group function and separate business units is to utilise a board-created enterprise level risk committee for overseeing all risks, to which a management level operational risk committee reports. Depending on the nature, size and complexity of the bank, the enterprise level risk committee may receive input from operational risk committees by country,

business or functional area. Smaller and less complex organisations may utilise a flatter organisational structure that oversees operational risk directly within the board's risk management committee;

(b) Committee composition – Sound industry practice is for operational risk committees (or the risk committee in smaller banks) to include a combination of members with expertise in business activities, financial or risk management expertise and independent non-executive board members; and

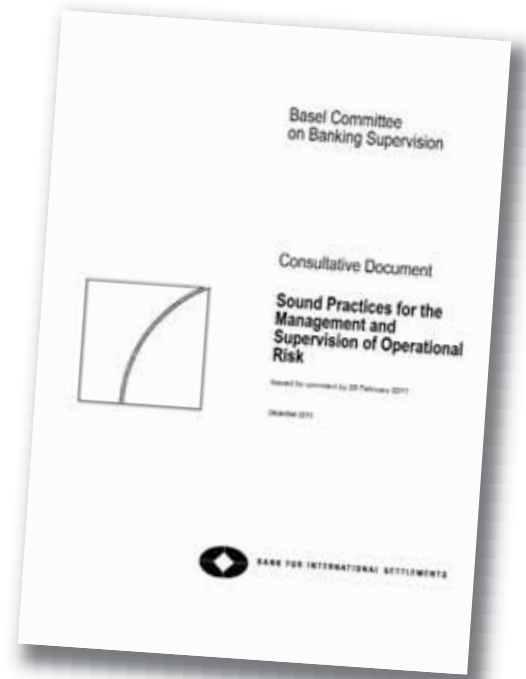
(c) Committee operation – Committee meetings should be held at appropriate frequencies with adequate time and resources to permit productive discussion and decision-making. Records of committee operations should be adequate to permit review and evaluation of committee effectiveness.

So it will no longer be appropriate for boards to consider the operational risk data as the last thing before lunch, perhaps noting the contents. Proper discussion will need to take place and to be minuted.

### Risk Management Environment Identification and Assessment

**Principle 6:** Senior management should ensure the identification and assessment of the operational risk inherent in all material products, activities, processes and systems to ensure the inherent risks and incentives are well understood.

The guidance sets out the variety



## OPERATIONAL RISK – HERE ARE THE NEW RULES, SAME AS THE OLD RULES

of tools available from internal and external loss data to scenario modelling. The focus on the scenario modelling with recognition that the science is not precise is important and welcomed. A robust scenario modelling framework is required. The remaining requirement of indicators, risk control self assessment, mapping, modelling, measurement and identification are all much as before.

**Risk Management**

**Principle 7:** Senior management should ensure that there is an approval process for all new products, activities, processes and systems that fully assesses operational risk.

Here there is a focus on inherent risk within new products, an area that perhaps has not been thoroughly addressed to date. Identifying mitigating controls, considering residual risk and seeking out unexpected outcomes are all part of the requirements here.

**Monitoring and Reporting**

**Principle 8:** Senior management should implement a process to regularly monitor operational risk profiles and material exposures to losses. Appropriate reporting mechanisms should be in place at the board, senior management, and business line levels that support proactive management of operational risk.

The reporting requirements are in both normal and stressed environments. Too many firms have undertaken stress testing for credit, market and liquidity risk – but only scenario modelling for operational risk. This is therefore clearly a change for many firms to understand how their systems and controls would operate were, for example, business volumes to double.

**Control and Mitigation**

**Principle 9:** Banks should have a strong control environment that utilises: policies, processes and systems; appropriate internal controls; and appropriate risk mitigation and/or transfer strategies.

Examples of policy elements and controls are included in the paper, including a suggestion of a two week holiday policy. The

implementation of risk tolerances to manage risk are recommended, indicating that a cascade of risk appetite (or tolerance) to the level of the control is required.

There is a concern at systems robustness under periods of stress and also fragmented systems caused by merger and acquisition activity. Clearly this will represent a challenge to many firms who are dealing with the changing circumstances of the financial market by aligning or combining their operations. The outsourcing proposals within the paper again highlight that the outsourced operation is part of the bank's control structure, although there is little new here.

**Business Resiliency and Continuity**

**Principle 10:** Banks should have business resiliency and continuity plans in place to ensure an ability to operate on an ongoing basis and limit losses in the event of severe business disruption.

This is really just a restatement of the existing rules.

**Role of Disclosure**

**Principle 11:** A bank's public disclosures should allow market participants to assess its approach to operational risk management.

Excited by any of this? I suspect not since it really is little more than a restatement of the rules we have been familiar with since 2003. There are a few minor changes, but nothing of real importance and I doubt that many firms will respond to the BIS on the paper.

So a general welcome to the proposed new sound practices, but the BIS as previously mentioned also produced:

**Supervisory Guidelines for the Advanced Measurement Approaches**

Again issued in December 2010 for comment by 25 February 2011, there are some interesting matters hidden away in what is to some extent an interesting if incomplete 59 page paper.

**Gross Loss Amount**

The statement says a bank may either use gross loss amount or gross loss

amount after recoveries except insurance, as input for its AMA models. The bank should demonstrate to its relevant supervisors that its choice is appropriate and should not use "net loss" (gross loss net of insurance) as an input for AMA models. Well that is what para 24 states. I expect this to be revised – it is better for the gross amount alone to be used and the mitigation to be recorded since the mitigation may not exist next time. Remember that the whole point about the loss database is to estimate next year's losses, not just to do the accounting – so mitigation should surely be separate.

In defining what gross loss actually is, the following is proposed:

Gross loss should include costs incurred as a consequence of the event that should include internal and external expenses with a direct link to the operational risk event and costs of repair or replacement, to restore the position that was prevailing before the operational risk event (eg legal expenses directly related to the event and fees paid to advisors, attorneys or suppliers).

My concern is what do they mean by internal costs? If a member of staff is moved from one function to deal with the matter, does their salary become a loss? I have always taken the view that the loss needed to be incurred (ie in addition to normal costs) rather than being added into the database. The wording here requires some clarification to make sure that it is not misunderstood.

They have also bought in a proposal that if a loss is incurred but quickly recovered as might be the case with erroneous payments, then this could be treated as a near miss. Again I believe this misses the point – just because there was a prompt recovery this time does not mean it will occur next time. I would have preferred that this requirement was not allowed.

**Event Date**

The statement has again tried to confuse itself, requiring a variety of dates to be recorded but then stating that the occurrence date should be used for the capital calculation. That must be the case since the scaling will be based upon the original date, not the date that the event was identified.

## OPERATIONAL RISK – HERE ARE THE NEW RULES, SAME AS THE OLD RULES

**Successful Implementation**

The following key issues have been identified that are crucial to the successful implementation of an AMA:

**(a) Internal Loss Data (ILD)**

The Committee expects that the inputs to the AMA model are based on data that represent or reflect the bank's business risk profile and risk management practices. It expects ILD to be used in the ORMS to assist in the estimation of loss frequencies, to inform the severity distribution(s) to the extent possible and to serve as an input into scenario analysis.

**(b) External Data (ED)**

The Committee expects ED to be used in the estimation of loss severity as such data contain valuable information to inform the tail of the loss distribution(s). ED is also an essential input into scenario analysis.

**(c) Scenario Analysis**

A robust scenario analysis framework is an important part of the Operational Risk Management Framework (ORMF) in order to produce reliable scenario outputs which form part of the input into the AMA model. The Committee acknowledges that the scenario process is subjective and that the output from a scenario process necessarily contains significant uncertainties. This uncertainty, together with the uncertainty from the other elements, should be reflected in the output of the model producing a range for the capital estimate. The Committee recognises that quantifying the uncertainty arising from scenario biases poses significant challenge and is an area requiring further research.

**(d) Business Environment and Internal Control Factors (BEICFS)**

Incorporating BEICFs directly into the capital model poses challenges given the subjectivity and structure of BEICF tools. The Committee has observed that BEICFs are

widely used as an indirect input into the quantification framework and as an ex post adjustment to model output.

**Validation**

There is a welcome focus on validation. The validation activity is designed to provide a reasoned and well-informed opinion of whether AMA models work as predicted, and whether their results (capital requirement estimates and other information produced by the ORMS) are suitable for their various internal and supervisory purposes. Validation activities should:

- (a) Have a broad scope, evaluating all relevant items of the ORMS, such as:
  - Distributional assumptions;
  - Correlation assumptions;
  - Documentation;
  - The four elements of the AMA (including observed/actual data, constructed data, figures generated by scenario analysis and business environment and internal control factors);
  - Qualitative aspects (including the internal controls, use test, reporting, role of senior management and organisational aspects);
  - Technological environment relating to the computational processes; and
  - Procedures for the approval and use of new and modified estimation models or methodologies (such procedures should seek explicit opinion from the validation function in the approval process);
- (b) Review qualitative aspects (including the internal controls, use test, reporting, role of senior management and organisational aspects);
- (c) Evaluate the bank's processes for escalating issues identified during validation reviews to ensure that:
  - Escalating processes are sufficiently comprehensive;

- All significant ORMS concerns are appropriately considered and acted upon by senior management; and

- All significant ORMS concerns are escalated to appropriate governance committees;

- (d) Evaluate the conceptual soundness – including benchmarking and outcome analysis – of the ORMS and of the modelling output;

- (e) Reflect policies and procedures to ensure that model validation efforts are consistent with board and senior management expectations.

- (f) Ensure that policies and procedures are sufficiently comprehensive to address critical elements of the validation process. These include independent review; clearly defined responsibilities for model development and validation; model documentation; validation procedures and frequency; and audit oversight; and

- (g) Confirm that the relationship between the model's inputs and outputs are stable and that the techniques underlying the model are transparent and intuitive.

**This is extending the validation requirements. Too often I find that firms are so pleased to have managed to develop appropriate data that they do not really have the time to properly validate the outputs from their systems. This focus on the importance of verification that the modelling and data are appropriate and complete is welcomed.**

So two papers at the same time on operational risk – both have interesting bits within them, neither are really surprising but both will require firms to review their operational risk management programmes and conduct a gap analysis against this minor changes.

*DWC@riskrewardlimited.com*

For further information please contact:

**Dennis Cox – CEO**

telephone: +44 (0)20 7638 5558  
email: [DWC@riskrewardlimited.com](mailto:DWC@riskrewardlimited.com)

**Lisette Mermoud – New York**

telephone: 1-914-619-5410  
email: [LM@riskrewardlimited.com](mailto:LM@riskrewardlimited.com)

**Joanna Kraska – Public Relations**

telephone: +44 (0)20 7638 5558  
email: [JK@riskrewardlimited.com](mailto:JK@riskrewardlimited.com)