



Information Paper

Developing Business Environment and Internal Control Factors for Operational Risk Measurement and Management

Emily Watchorn and André Levy – April 2008



Copyright

The material in this publication is copyright.

You may download, display, print or reproduce material in this publication in unaltered form for your personal, non-commercial use or within your organisation, with proper attribution given to the Australian Prudential Regulation Authority (APRA). Other than for any use permitted under the *Copyright Act 1968*, all other rights are reserved.

Requests for other uses of the information in this publication should be directed to APRA Public Affairs Unit, GPO Box 9836, Sydney NSW 2001 or public.affairs@apra.gov.au

© Australian Prudential Regulation Authority (2008)

Disclaimer

While APRA endeavours to ensure the quality of this Publication, APRA does not accept any responsibility for the accuracy, completeness or currency of the material included in this Publication, and will not be liable for any loss or damage arising out of any use of, or reliance on, this Publication.

Inquiries

For more information on the contents of this publication contact:

Emily Watchorn or André Levy
Supervisory Support Division

Australian Prudential Regulation Authority
GPO Box 9836
Sydney NSW 2001
Tel: 61 62 9210 3000
Email: emily.watchorn@apra.gov.au,
andre.levy@apra.gov.au

Acknowledgements

Author: Emily Watchorn and André Levy

The authors would like to acknowledge Harvey Crapp, Sarah He, Michael Murphy and Justin Zeltzer for their contribution to this paper.

Contents

Introduction	4
What are business environment factors (BEFs)?	5
What are internal control factors (ICFs)?	6
Measuring BEICFs	8
Key Risk Indicators	8
Measuring BEFs: Objective and Subjective	8
Measuring ICFs: Observing Control Effectiveness	8
Scaling and Scoring	8
Transforming the Metrics	9
Leading or Lagging	9
HFLI or LFHI	10
Aggregating BEICFs	12
Combining BEFs with ICFs	12
Constructing Composite Indicators	12
Group Level Analysis	12
Operational risk capital calculations	13
Measuring Required Capital	13
Allocation Mechanisms	13
Interim Adjustments	13
Monitor and managing operational risk	14
Driving Behaviour: Thresholds, Triggers and Escalation Criteria	14
External Benchmarking	14
Conclusions	15
References	15

Introduction

Banks using the Advanced Measurement Approach (AMA) for operational risk (OR) measurement are required to include four data elements in their framework: internal loss data, external loss data, scenario analysis, and business environment and internal control factors (BEICFs)¹. In contrast to the historically based internal and external loss data inputs, BEICFs and scenario analysis add a forward-looking perspective to the AMA model. Scenario analysis typically considers the extreme, low-frequency/high-impact (LFHI) operational events, whilst BEICF measures are usually associated with the day-to-day, high-frequency/low-impact (HFLI) events. Despite this labelling, it is important to realise that a spate of small losses can often be a warning signal, indicating potential for more serious trouble ahead. Hence using BEICFs to manage the smaller losses can potentially mitigate the exposure to a future extreme event.

The use of BEICFs as an OR management tool has been spurred by Basel II implementation², although similar techniques are historically evident in concepts such as the *balanced scorecard* (BSC) and the use of *key performance indicators* (KPIs). Most banks³ have now created *operational risk scorecards*, and the development of *key risk indicators* (KRIs), whilst proving to be challenging, is well underway.

Business environment factors are those characteristics of a bank's internal and external operating environment that bear an exposure to operational risk⁴. These environmental risk exposures are referred to as the *inherent* risks of the bank. *Internal control* factors reflect elements of the bank's internal control system that are implemented in order to mitigate the inherent risks of the bank, leaving what is known as a *residual* risk profile, under which the bank operates on a daily basis.

In order to utilise these BEICFs, banks require techniques to measure them. In other words, banks face the challenge of quantifying the OR exposures arising from each business environment factor, and the effectiveness of internal controls in mitigating these risks. The measures can be determined objectively, using quantitative data, or subjectively, using a variety of scaling and scoring tools to capture expert opinions. Tools commonly used to measure BEICFs include scorecards, heat maps, and key risk indicators, each of which can measure either the inherent or the residual risk profile.

The BEICF measures can be used to calculate, allocate and adjust the OR capital held by a bank. For these purposes, the metrics will often need to be aggregated into a summary measure. Aggregation can also be desirable when presenting BEICF data to management, who do not want to be overloaded with a plethora of quantitative metrics. Effective aggregation of indicators allows for a relevant risk information summary of the bank's (or business unit's) OR profile to be presented to management. However, inappropriate aggregation techniques can disguise an underlying problem if a warning signal is 'smoothed-out' when combined within the aggregate. Challenges also arise in drawing the line between visibility of all the relevant underlying issues and an overload of technical information.

BEICFs create an important link between the OR capital measurement system and the day-to-day management practices of the bank. Used effectively, BEICFs can help managers to drive behaviour within the organisation, to keep in line with their risk tolerance and objectives. In order for the BEICF measures to be functional, they need to be given a frame of reference. To achieve this, banks must define relevant thresholds, reporting requirements, and escalation criteria. Implementation of an effective BEICF framework can meaningfully influence management decisions by ensuring that risk, not just performance, is taken into account in the day-to-day management practices of the bank.

¹ APRA (2008, Attachment B, Paragraph 38, p19), and Basel Committee on Banking Supervision (2006, Paragraph 676, p154).

² The Basel II Implementation date in Australia was 1 January 2008

³ 'Banks' in this paper refers to those institutions who have applied to APRA for use of the Advanced Measurement Approach to operational risk.

⁴ Environmental risks include strategic and other risks, that whilst are not included in the Basel definition, can be included for banks' internal management purposes.

What are business environment factors?

Business environment factors (BEFs) describe a bank's inherent risk. An analysis of the business operating environment can help banks better understand the sources and nature of OR in their organisation. Specifically, banks should aim to understand which particular features of the business environment drive their OR exposures. Assessing the business operating environment can aid in the identification of the bank's key risks, and promotes discussion and further understanding of the root causes of those risks.

BEFs can include internal factors, such as the size and volume of the business; the nature and complexity of the products or services offered, and of the processes and technology required to supply them; the skills and turnover levels of the staff; and the level of change and development within the business. External BEFs include factors such as the competitive, economic, regulatory, legal, geographic, political and natural environment.

Banks should consider the manner in which each BEF contributes to their overall inherent OR profile. Each factor can influence the frequency or severity exposure, or some combination of the two. For example, a higher degree of manual processing may be linked to an increased frequency of processing errors, but not necessarily a higher severity exposure, should an error occur. Alternatively, growing business volumes can increase both the likelihood and severity of the loss exposure.

Banks must also consider the direction of the relationship between the factors and the risk exposures. Furthermore, this relationship can be linear or non-linear, and it may change over time. To illustrate, as a business grows and the number of staff increases, so will the OR exposure, since the potential for losses from human error or fraud also increases. Alternatively, a falling number of staff may also increase OR exposure, as business controls typically depend on staff to enact them. The points at which risk is defined as rising or falling may change over time, depending on the growth and complexity of the business, and the assumed optimal number of staff required for its operation.

An assessment of the business environment should not be a new concept for business managers. Managers are likely to have assessed various elements of their business environment as part of a traditional SWOT analysis, strategy planning, project analysis, and other decision-making activities. Banks may leverage from their existing business environment assessment activities by integrating them into their AMA framework. This is consistent with the Basel II Framework in its endeavour to make operational risk management an integral part of the day-to-day management and decision-making of the bank.

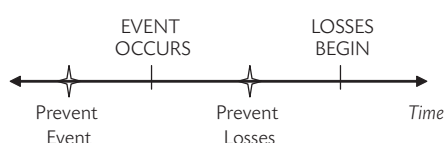
What are internal control factors?

Internal controls are the means by which management can mitigate their inherent risk exposures. Specifically, the internal controls implemented by management will shape the business's OR profile by defining the residual risk profile under which the bank operates on a daily basis. Examples of internal controls include probity checks on new employees, documentation requirements, records management, periodic password changes, and separation of duties structures.

Controls can be classified as *preventative*, *detective* or *remedial*. In order to understand the differences between the control mechanisms, it is important to distinguish between an *event* and a *loss*. An OR event may occur, after which it may or may not give rise to a monetary loss. Incurred losses may materialise on a single occasion, or they may continue to surface over a period of time, whereby a loss start date and loss end date are often captured in the bank's internal loss data records.

Preventative controls are already in place before an operational event occurs. They can operate:

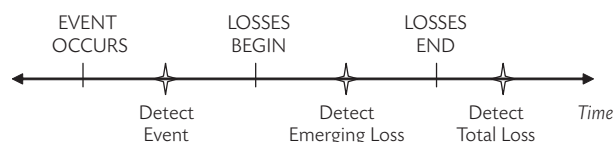
- before an event, to prevent that event from occurring; or
- after an event, by preventing that event from causing a loss, even if the event has not been detected.



Detective controls operate automatically to provide a warning signal to the bank. They can:

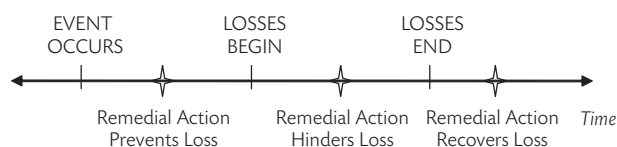
- detect and signal an event, before a loss emerges, thus providing an opportunity for the bank to avoid incurring a loss; or
- detect and signal emerging losses⁵, thus providing an opportunity for the bank to mitigate the severity of the losses from the event; or

- detect a loss after the final loss has emerged, and inform the bank staff who can deal with the situation.



Remedial controls do not operate automatically; they must be consciously implemented, after it is known that an event or loss has occurred. Remedial controls can be implemented:

- after an event has been detected, to remedy the situation before a loss emerges;
- when emerging losses have been detected, to remedy the situation before further losses can occur;
- after the total loss is known, in an attempt to recover some or all of the loss suffered.



Banks can extend this analysis to consider whether a particular control reduces the frequency or severity of its inherent operational risk exposures⁶. For example, a probity check on new employees is a preventative control that mitigates the frequency of internal fraud. Independent reconciliations are a detective control that can reduce both the frequency and severity of internal frauds: their very existence can deter potential fraudsters from committing the act, thus reducing the frequency of internal frauds; and the detection of a fraud can alert management of the event, allowing remedial action to be taken, thus reducing the severity of the fraud.

⁵ The phrase 'emerging losses' is used here to refer to the losses arising between the loss begin date and end date.

⁶ This is particularly relevant for banks considering ICFs in the Scenario Analysis process.

There is not always a clear line between the control types and their effects on frequency and severity. Nonetheless, conducting an analysis such as this will improve the bank's understanding of the nature and effectiveness of its internal control mechanisms, and hence its residual risk profile.

The set of controls that are implemented to mitigate a certain risk exposure will not always include each type of control mentioned above. Managers may decide not to implement a control if the cost of implementation outweighs the benefits. In some cases management may find that they are unable to identify an effective control at all. Due to the ever changing nature of the bank's OR profile, internal controls may become less effective over time, and a need for new types of controls may arise. Analysis of the internal control environment for a BEICF framework can often inspire ideas for the design of new and improved controls, or bring managers to consider whether any existing controls have become outdated or ineffective. Consequently, it is important that banks regularly review their ICFs in order to assess the ongoing effectiveness of their internal control system.

Measuring BEICFs

Key Risk Indicators

Banks can attempt to measure the BEICFs they have identified. The resulting metrics allow the bank to monitor changes in its operating environment, being the inherent risk profile, and in the quality of its controls, or its residual risk profile. Accordingly, these metrics are known as Key Risk Indicators (KRIs).

Measuring BEFs: Objective and Subjective

Some BEFs can be measured objectively, using quantities such as asset size, revenue, or number of staff. Others are not readily quantified and must be assessed subjectively, using expert opinion. Examples include the complexity of products and processes, and the level of change or innovation in the business, or in the wider industry. These answers to these types of questions may vary between respondents, depending on their interpretation of the context, as well as their subjective beliefs. Despite these shortcomings, objective measures alone are not sufficient to cover the sphere of OR exposures faced by the bank. Subjective expert opinion must be used to complete the picture.

Measuring ICFs: Observing Control Effectiveness

Similar to business environment factors, ICFs can be assessed using subjective expert opinion of their qualities, or objective data reflecting their effectiveness. One difficulty faced when trying to measuring the effectiveness of a preventative control is that its success and failure rate is not always observable. To calculate the success and failure rates, managers need to know both the number of times that a control failed and the number of times it succeeded in preventing an OR event, over a chosen time horizon. Control failures resulting in OR events are typically observable, but certain OR events may pass by unnoticed for some time, or even indefinitely.

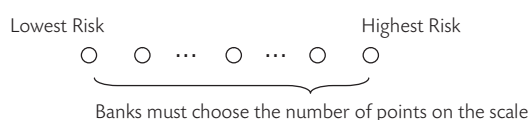
Further, it is not always observable when a control is successful in preventing an OR event (for example, when the presence of a security camera prevented an act of vandalism, or a robust segregation of duties structure deterred a staff member from attempting to execute unauthorised trades). Banks should appreciate the existence of control successes and failures that are unobservable, and that evaluating control effectiveness involves assumptions, estimation and uncertainty.

Scales and Scores

One way of measuring the qualitative BEICFs is to map their characteristics to a scale, then ask business experts to choose the point on the scale that they believe is reflective of that factor. *Scaling* refers to the construction of the response scale, typically performed by the bank's Group Operational Risk function. *Scoring* refers to the behaviour of the respondents in selecting answers on the provided scale. Various types of scales can be constructed, and there are some important considerations for banks when choosing the structure of their scales.

Banks must choose whether their scale will be continuous or discrete, and in the latter case, the number of points on the scale and the distance between them. A continuous scale, say from zero to 100%, may introduce spurious accuracy, whilst a sparse discrete scale may not be precise enough to discern information.

A discrete scale should have at least three points (Cohen, 1983). In fact, Jacoby and Matell (1971) argue that three points are all that is needed. Conversely, when using more than seven points, the reliability of the assessments tend to level off (Nunally, 1978), and only up to nine points can be used effectively by respondents (Bass, Cascio, and O'Connor, 1974).



Further, banks must consider whether the choice of an odd or even number of points is relevant. For some types of scales, a middle point can be used to convey neutrality, and Kline (1998) argues that this option is desirable. Conversely, Dumas (1999) asserts that using an even number of points, and hence forcing the respondent to make a decision either way, will provide a better reflection of the respondents' opinion. Kahn, Nowlis and Dhar (2000) argue that the choice is irrelevant, since if the respondents are truly neutral, they will randomly choose one way or the other on an even-numbered scale, hence given a large enough number of respondents, this randomness would be diversified away. This, however, is generally not the case for operational risk scorecards, which are typically answered by a single business unit manager, or operational risk staff, with respect to a single business unit.

Whatever the choice of scale, assessors' responses may still exhibit bias. Albaum (1997) lists three possible biases:

- Leniency – tendency to rate something too high or too low, i.e. to rate in an extreme way;
- Central tendency – a reluctance to give extreme scores;
- Proximity – give similar responses to items that occur close to one another.

It is important to recognise whether any biases are present, as they may significantly skew risk estimates, and should be mitigated as much as possible. Biases may vary across cultures (Herk, Poortinga and Verhallen, 2004; Johnson et al, 2005), and this may be quite relevant to multi-national institutions.

Likert (1932) suggested the use of a scale ranging from 'agree' and 'strongly agree' to 'disagree' and 'strongly disagree' in answer to a specific statement, for example, 'The process is simple'. A practical solution for banks' OR scorecards is to ensure that each point on the scale is clearly defined so as to mitigate the subjectivity in interpretation of the points. The range of practice for Australian banks has varied, with some banks defining each point on the scale clearly and objectively, whilst others have simply left the meaning to the respondent's interpretation.

Transforming the Metrics

Raw data values alone do not always give a clear message about a risk profile. Banks should aim to find a way of presenting the data which allows managers to easily and effectively discern information about the level of, and changes in, the bank's OR profile. Sometimes this will simply be the absolute value of the quantity (for example, number of processing errors = 43). Alternatively, the data may be expressed as a percentage change (percentage improvement or deterioration in processing errors), by product or process type (cheque processing errors), per units of time (errors this week, or improvement this month), or as ratios in terms of other quantities (processing errors per staff member).

Leading or Lagging

There are two main types of KRIs, called *leading* and *lagging* indicators. Leading indicators are *ex-ante*, providing a signal before an OR event occurs. Lagging indicators are *ex-post*, providing information after an event has occurred. Clearly, leading indicators are more desirable for managers, as they can provide an early warning signal to prompt preventative action before an OR event occurs. However, Davies and Haubenstock (2002, p42) emphasise the importance of balancing the ex-post measures with the more predictive ex-ante measures. Their reason is that predictive KRIs are often determined subjectively, and may be difficult to validate. Alternatively, lagging indicators can usually be identified and validated objectively using data, and are hence more reliable, if not as effective in preventing loss.

A distinction should be made between leading indicators and predicting OR losses. The concept of leading indicators is that a deteriorating OR profile can be recognised before a risk exposure crystallises into a loss. Even if a loss does not eventuate, the KRI should be duly sensitive that it reflects the increased risk exposure. That is, KRIs are not just meant to predict losses, they are meant to indicate risk.

HFLI or LFHI

BEICFs are relevant for both HFLI events and LFHI events. KRIs for the HFLI event risks can often be objectively determined using statistical data, since the loss data available for analysis is plentiful. In addition, since the losses are familiar and affect the day-to-day performance, management is likely to already be collecting relevant data for their KPIs, hence a historical stream of indicator data is usually available. For example, management is likely to already be collecting indicators such as staff turnover or sales volume, which can potentially be used to indicate OR exposures.

It is important not to rely on data analysis alone, as there is a danger of extracting spurious causal relationships. For example, the statistical data analysis could show a significant correlation between internal fraud and losses arising from accidents in the workplace. However, a tandem increase in both of these event types' frequencies may be simply due to business growth. This distinction can become evident when the bank experiences a change in its operating environment or control structure. If the bank were to subsequently implement a control structure that notably reduced its internal fraud losses, the data may begin to reflect the falling internal fraud losses, without any change in the health and safety losses. That is, once the context changes, the relationship can be lost, and hence the effectiveness of any existing indicators may disappear. Banks should be aware that correlation does not always imply causality, and this is an important consideration when constructing and reviewing the effectiveness of risk indicators.

In contrast, the data is sparse for LFHI operational loss events, so the relevant KRIs are often determined subjectively, using expert opinion. Ideally, experts could identify predictive indicators that could allow banks to prevent the occurrence of severe events. Unfortunately, extreme operational events are often highly unpredictable by their nature, and it may not always be possible to identify a leading KRI to alert management of their imminence.

In some cases, HFLI data can be used to evaluate LFHI events if the underlying causes are the same. Consequently, a number of relevant low impact losses may provide an early warning signal before the occurrence of an extreme event. For example, small seismic tremors can indicate that a major earthquake is on its way, and frequent unauthorised trading losses can indicate potential for extreme rogue trading. In these cases, the HFLI losses themselves can be used as predictive KRIs for extreme events. Their effectiveness will depend on whether they are captured and assessed in a timely fashion.

A useful starting point for assessing the predictability of an event is an understanding of what causes that event to occur. If banks know what causes a certain loss type to occur, they can construct a KRI to monitor that root cause, rather than trying to track the losses or events directly. In this way, the KRI can become leading rather than lagging. There are four different risk/root cause cases to consider, with each situation affecting the ability to identify a leading KRI:

- i) The root cause of a risk is known and measurable. In this case, a leading KRI may be identified if the root cause can be measured in a timely fashion. For example, when driving a car, one can easily monitor the volume of fuel in the tank. If the volume reads low, action can be taken to prevent the car from reaching empty.
- ii) The root cause of the risk is known, but it is not measurable or detectable. In this case, the KRIs may be more lagging, since the root cause cannot be detected before an event emerges. For example, it is not feasible for a bank to monitor seismic activity for a predictive indication of earthquake or tsunami events.
- iii) The root cause of the risk is unknown. Some events may seem truly random, and there is no conceivable way of detecting a cause. For example, *Chronic Fatigue Syndrome* has not successfully been associated with any known causes; hence one is not able to monitor their exposure to developing it (The Medical Journal of Australia, 2002).

- iv) It is unknown that an exposure to a risk exists.
There exist exposures to extreme events that have not been encountered historically, or that banks are yet to identify. For example, prior to the September 11 events in the United States, most people would not have recognised that they were exposed to such a risk.

Unless the root causes of such extreme events can be known and understood, it is unlikely that truly leading indicators can be developed and validated. In the meantime, indicators can be focussed on those elements of the risk that are known and measurable, whilst efforts continue into understanding the sources and nature of extreme OR events.

Aggregating the BEICF metrics

Combining BEFs with ICFs

In order to evaluate their residual risk profile, banks must measure the extent to which their internal controls reduce their inherent risk exposures. This process involves mapping the controls to the BEFs and assessing the residual risk exposure. Some risks may be eliminated completely by controls, while others may be more difficult to mitigate. Mapping risks and controls, and estimating residuals, can be a highly subjective process, involving a high degree of assumptions, estimation and uncertainty. One observation from APRA's experience with the Australian AMA banks is that it is difficult to estimate the true inherent risk, i.e. independently of the mitigating effect of controls. To the extent that the controls are already accounted for in the inherent risk estimates, the mitigating effects are double-counted, and the residual risk is understated. Banks should appreciate the extent to which these estimation errors could undermine their OR capital calculation.

Constructing Composite Indicators

There are potentially hundreds or thousands of KRIs that can be constructed, and some are more useful and informative than others. To include large numbers of KRIs in management reporting would result in an overload of information, and a burdensome task for management to understand. On the other hand, aggregating all the information into some summary measure could potentially disguise underlying important issues, and make it difficult for management to see where they need to take action. Further, indicators are defined on different scales and using different units of measurement, making it difficult for banks to know how to aggregate them.

Taylor (2006) proposes a solution to this problem with his methodology for constructing *composite indicators*. He describes the problem as trying to 'combine apples with oranges'. The composite indicator method can convert a number of indicators all into 'apples' so that they can be combined in a meaningful fashion. The manner in which the indicators are combined depends on whether they describe risks whose effects would compound one another, or whether the risks are relatively independent. Further, if any of the KRIs are considered more important than others, they can be assigned a higher weighting within the composite indicator to reflect this. Overall, the method ensures that if any one of the component indicators is showing signs of trouble, then the composite indicator will reveal it, not disguise it, allowing management to investigate further.

Group Level Analysis

Banks will need to review their BEICFs from a group-wide perspective in order to calculate, allocate or adjust OR capital. However, the metrics are often not comparable between business units. Some indicators are applicable across the entire bank, such as staff turnover, and others may be specific to certain business units, such as the number of trading limit breaches. Where indicators are universally applicable, they may nevertheless be incomparable, as a result of the unique nature of each business unit. For example, a higher level of staff turnover may be commonplace among the customer call centre staff, but such a high level of turnover would be worrisome in, say, risk management units. If these figures are simply averaged into some group staff turnover indicator, then the aggregated group KRI may not accurately track the true risk level, since it is defined at too high a level.

An article published by OpRisk and Compliance (April 2005), quoted Andrew Cherriman, of Merrill Lynch in London, who agreed that management reporting cannot be formed simply by "*taking risk metrics from the 'grassroots' level and having some automated method of amalgamating [them] up*". He likened it to taking an average temperature of cars on the M25 motorway, and then trying to assess the health of individual cars based on the average.

Operational risk capital calculations

Measuring Required Capital

One way that BEICFs can be used in the OR capital calculation is via consideration in the scenario analysis process. Often the internal and external loss data considered for scenario assessments may be found to lack relevance. In essence, this is because the loss events do not reflect the current business environment or the current internal control effectiveness of the bank. Consideration of BEICFs can assist the scenario assessors in making estimates that are more relevant to the current residual risk profile of the bank. Some banks express their BEICFs outright in terms of frequency and impact exposures. This approach is essentially similar to scenario analysis, the difference being more so one of terminology than approach. In both cases, banks are expected to provide documented rationale for whether a change in relevant BEICFs prompts them to update the frequency estimate or the impact estimate.

Allocation Mechanisms

Some banks have used BEICFs as the means by which they allocate group OR capital to the business units. The intention is that business units hold capital commensurate with their residual risk profile, as measured by their BEICFs. Typically, the allocation is calculated using a scorecard technique, which facilitates a comparison of the relative riskiness of each business unit. The Group OR Function should play a role in ensuring consistency of the scorecard interpretation across business units. One method is to use the change in the scores, rather than the absolute scores. This avoids potential inconsistency in interpretation and responses across business units, and instead assumes that the scorecard interpretation remains consistent within each individual business unit over time.

Interim Adjustments

BEICFs can be used to update a capital figure to reflect changes in a bank's risk profile which may occur between the formal capital calculations, typically performed annually. BEICFs are the most suitable of the four data inputs to perform the role of keeping the OR capital aligned with the bank's residual risk profile. Internal and external loss data are an historical reflection, and scenarios are typically focussed only on extreme events. Hence BEICFs are an ideal means by which the OR capital can be kept more closely aligned with the dynamic risk profile of the bank.

Monitoring and managing operational risk

Driving Behaviour: Thresholds, Triggers and Escalation Criteria

KRIs are not particularly useful unless they can be measured in an appropriate context. Management can achieve this by defining thresholds for the KRI levels. The indicator values are typically mapped to the red-amber-green scale, with the thresholds defined by managers to reflect their unique risk tolerance and performance objectives.

Procedures can then be implemented whereby a breach of threshold triggers the escalation of the issue to higher management. For example, a KRI movement from green to amber may necessitate that senior management be informed of the issue, so that they can more closely monitor the actions of lower management in resolving the situation. A further deterioration to the red zone may dictate that senior management are to intervene and take control of the situation, in the hope that they can restore the situation to an acceptable level.

A conflict of interest can arise when such escalation criteria are enforced. A real life example can be taken from Britain's National Health Service (NHS) as described in an article from the Global Risk Regulator, November 2004 issue:

'The UK government decided to monitor the number of patients waiting in line for treatment in NHS hospitals as an indicator of the quality and effectiveness of the service... [It] became clear that hospital management were manipulating patient lists to meet targets, and that queue length was anyway an ambivalent measure of the quality of treatment received.'

Banks must ensure that their OR management policies are embedded and effective in order to prevent such manipulations or avoidance of the rules in place.

Other situations have revealed KRIs to be a highly successful tool for achieving management objectives. Henry (2006) describes the use of 'CompStat⁷', a management model used by the New York Police Department to help them meet their crime reduction targets more effectively. The CompStat program recognises that middle managers are in a better position than headquarters executives to make everyday operational decisions. The model focuses on collecting and analysing relevant data that can be used as an early warning system to alert managers and executives to rapidly changing conditions.

CompStat was implemented in 1994 under the mayoralty of Rudy Giuliani. By 2000, the crime rate in New York City had fallen by 57%, and the murder rate had dropped by 65% (Giuliani, 2005). CompStat has since been adopted by other police departments in the U.S. and internationally (Ibid.).

Henry (2006, p117) comments that the success of the CompStat program did not end with just meeting crime reduction targets:

'The relative ease with which CompStat has permitted the agency to fulfil its primary mission has concomitantly resulted in the capacity to identify and address a host of other new, emerging or longstanding management issues.'

External Benchmarking

KRI thresholds and escalation triggers can be used to drive management behaviour and keep operations within certain risk limits. The exercise of setting suitable thresholds and monitoring indicator trends promotes discussion and awareness of risk management issues, and helps to direct management attention towards risk, and not just performance.

⁷ 'CompStat' is an abbreviation of 'Computer Comparison Statistics'.

Banks can benchmark their key risks and internal control levels against their peers. The US-based Risk Management Association (RMA) sponsored a KRI study in 2003, which has since developed into a KRI 'library'⁸. The library acts as a benchmarking service for banks to anonymously compare their KRIs with those of their peers. In order for a meaningful comparison to be made, there needs to be consistency in definitions and granularity under which the KRIs are measured. Accordingly, the KRI library takes the seven risk and eight business line definitions from the Basel II Framework, and breaks them down into a more granular set of definitions, namely, business units, risk types and function types.

Whilst the KRI Library is often promoted as facilitating development and innovation in the KRI space, Rowe (2004) argues that the all-important links between KRIs and loss probabilities are likely to differ across institutions based on their particular process characteristics. In other words, some KRIs may be meaningful in certain contexts, but not in others.

External benchmarking results should be considered in light of the unique risk tolerance of a bank. That is, rather than simply benchmarking against an average of external KRI values, banks should consider a more appropriately defined benchmark, perhaps higher or lower than the average, based on their risk appetite and position within the industry.

⁸The project homepage is at www.kriex.org.

Conclusion

BEICFs provide the link between the measurement and management components of the advanced measurement approach to OR. Whilst quantifying them may present challenges, having a set of risk metrics provides a useful management tool for decision-making, driving behaviour, and promoting accountability between management layers. The identification and measurement of BEICFs promotes discussion and awareness of OR issues, and creates an environment where decisions can be influenced by risk, not just performance.

The Basel II deadline perhaps had banks developing their KRI programs under pressure, and there remains scope for improvement both within the banks, across the industry, and internationally. With this in mind, it is important for banks to realise the danger of over-reliance on the KRI program they have implemented. Specifically, management should be aware of the gaps that remain in the indicators' coverage of the operational risk space. To use a car analogy, just because your fuel, oil and water meters all read 'full', does not guarantee you will not be hit by a truck.

Operational risk is a relatively young discipline, and BEICFs are a means by which banks can improve their understanding of the nature of their operational risks. A BEICF framework promotes discussion and analysis of the root causes of different risk types, and which are the key risks that drive the bank's OR profile. Increased discussion and awareness of these issues facilitates grounds for improvement of the bank's internal controls and OR management strategy. BEICF programs are expected to become a tool that is willingly embraced and fully embedded within the banks' management culture, and not just the offshoot of a regulatory compliance exercise.

References

- Albaum, G., 1997, 'The Likert scale revisited,' *Journal of the Market Research Society* 39 (1997) 331-348
- Australian Prudential Regulation Authority (APRA), 2008, 'Prudential Standard APS 115 Capital Adequacy: Advanced Measurement Approaches to Operational Risk', January 2008
- Basel Committee on Banking Supervision, 2006 'International Convergence of Capital Measurement and Capital Standards', *Bank for International Settlements*, June 2006
- Bass, B.M., Cascio, W.F. and O'Connor, E.J., 1974, 'Magnitude estimations of expressions of frequency and amount,' *Journal of Applied Psychology*, 59(3), 313- 320
- Davies, J. and Haubenstock, M., 2002, 'Building Effective Indicators to Monitor Operational Risk', *The RMA Journal*, May 2002
- Dumas, J., 1999, 'Usability Testing Methods: Subjective Measures, Part II - Measuring Attitudes and Opinions,' *American Institute for Research*
- Garland, R., 1991, 'The mid-point on a rating scale: is it desirable? ', *Marketing Bulletin*, 2, pp 66-70
- Greenleaf, E. A., 1992, 'Improving Rating Scale Measures by Detecting and Correcting Bias Components in Some Response Styles,' *Journal of Marketing Research*, Vol. 29, No. 2, May 1992, pp. 176-188
- Giuliani, R., 2005, 'CapStat will Increase Accountability and Performance', *Archives of the Mayor's Weekly Column*, The City of New York, 20th April 2005
- Global Risk Regulator, 2004, 'Key Risk Indicators Move up a Gear', November 2004 p19
- Guy, R. F. and Norvell, M., 1977, 'The neutral point on a Likert scale,' *The Journal of Psychology*, 95, pp 199-204
- Haubenstock, M., Immaneni, A. and Mastro, C., 2004, 'A Structured Approach to Building Predictive Key Risk Indicators', *Operational Risk: A Special Edition of The RMA Journal*, May 2004
- Henry, Dr V. E., 2006, 'Managing Crime and Quality of Life using CompStat: Specific Issues in Implementation and Practice', *United Nations Asia and Far East Institute for the Prevention of Crime and Treatment of Offenders (UNAFEI)*, Resource Material Series No. 68, March 2006 pp 117-132
- Herk, H. van, Y. H. Poortinga, and T. M. M. Verhallen, 2004, 'Response Styles in Rating Scales: Evidence of Method Bias in Data From Six EU Countries,' *Journal of Cross-Cultural Psychology*, May 1, 2004; 35(3): 346 - 360
- Jacoby, J. and Matell, M. S., 1971, 'Three-Point Likert Scales Are Good Enough,' *Journal of Marketing Research*, Vol. 8, No. 4 (Nov., 1971), pp. 495-500
- Johnson, T., P. Kulesa, Y. Cho and S. Shavitt, 2005, 'The Relation between Culture and Response Styles: Evidence from 19 Countries', *Journal of Cross-Cultural Psychology*, (36) 2 264-277 2005
- Kahn, B., Nowlis, S., and Dhar, R., 2000, 'Indifference versus Ambivalence: The Effect of a Neutral Point on Consumer Attitude and Preference Measurement,' *Wharton Working Paper Series*, September 2000
- Kline, P., 1998, 'The New Psychometrics: Science, psychology and measurement,' London: Routledge
- Komorita, S. S., 1963, 'Attitude, Content, Intensity and the Neutral Point on a Likert Scale,' *Journal of Social Psychology*, 61, 327-334
- Likert, R., 1932, 'A Technique for the Measurement of Attitudes,' *Archives of Psychology*, 140
- Medical Journal of Australia, The, 2002, 'Chronic Fatigue Syndrome', *Clinical Practice Guidelines – 2002*, *The Medical Journal of Australia* 6 May 2002 176 (8 Suppl): S17-S55
- Neuman, W.L., 2000, 'Social Research Methods: Qualitative and Quantitative Approaches,' USA: *Allyn & Bacon*

Reference

Nunally, J. C. (1978), 'Psychometric Theory,' New York, *McGraw-Hill*

OpRisk and Compliance, 2005, 'KRIs under scrutiny at OpRisk Europe conference', April 2005, Vol. 6 No. 4, Incisive Media Ltd., London

Robson, C., 1993, 'Real World Research: A Resource for Social Scientists and Practitioner-Researchers,' Oxford: *Blackwell Publishers*

Rowe, D., 2004, 'A difference in kind', *Risk*, June 2004 edition

Taylor, C., 2006, 'Composite Indicators: Reporting KRIs to Senior Management', *The RMA Journal*, April 2006



Telephone
1300 13 10 60

Email
contactapra@apra.gov.au

Website
www.apra.gov.au

Mail
GPO Box 9836
in all capital cities
(except Hobart and Darwin)