

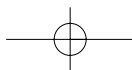
Key Risk Indicators – Their Role in Operational Risk Management and Measurement

**Jonathan Davies, Mike Finlay,
Tara McLenaghan, Duncan Wilson**

RiskBusiness International Limited

In comparison with other operational risk management and measurement tools such as loss data (internal, public and consortium), risk-and-control assessments, capital allocation and performance measurement, key risk indicators (KRIs) remain one of the outstanding action items on most firms' to-do lists, along with scenario analysis. KRIs are not new, but, up until recently, attempts to implement such programmes have often been characterised as less than effective. We believe that there are emerging best practices for KRI programmes that overcome some of the traditional challenges in KRI implementations. Further, we believe that investment in KRI programmes will reap many benefits, including the ability to clearly convey risk appetite, optimise risk and return, and improve the likelihood of achieving primary business goals through more effective operational risk management.

In this chapter, we will seek to demystify KRIs, understand the basic fundamentals in identifying, specifying, selecting and implementing quality indicators, and consider how to monitor and report on them, in conjunction with other useful operational risk management information, to create powerful management reporting. We will also examine the potential for more advanced applications of KRIs, touching on the measurement of risk for correlation purposes, and the potential for composite indicators as well as KRI benchmarking. Finally, we will overview an industry KRI



AMA APPROACHES TO OPERATION RISK

initiative which can help many firms get their own KRI programmes started.

THE FUNDAMENTALS OF A KRI PROGRAMME

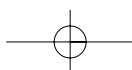
As with so many aspects of operational risk management, one of the biggest challenges in creating a KRI programme is communication – both in understanding how market practice is evolving and in explaining objectives and policy internally. In this section, we will describe what KRIs are, how they can be used, as well as the importance and value of establishing a common language and structure to support KRI programme implementation. We will then outline the main steps and considerations in selecting KRIs, as the foundation for any KRI programme.

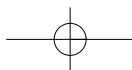
What is an indicator?

KRIs are measurable metrics or indicators that track exposure or loss, or, as one person put it, “trouble”. Anything that can perform this function may be considered a risk indicator. The indicator becomes key when it tracks an especially important exposure, or it does so especially well, or ideally both. In operational risk, we are interested in KRIs that monitor operational risk. Operational risk can be defined as the risk of loss resulting from inadequate or failed processes, systems, human performance or external events.

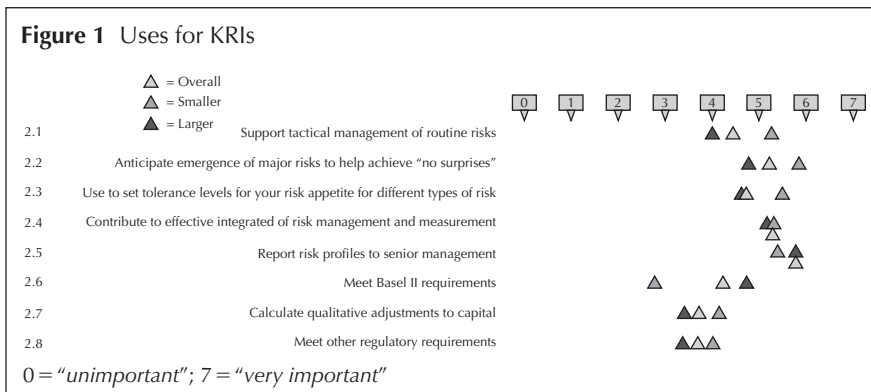
The number of customer complaints is an example of a *risk* indicator. As customer complaints increase, the probability that there are some underlying and potentially systemic mistakes and errors of judgement being made is likely to rise. In other words, there is a rationale for thinking that, at least in some ranges, changes in the value of this indicator are likely to be associated with changes in operational risk exposure or operational loss experience.

The number of customer complaints is also an example of a *common* indicator – an indicator that would seem to be relevant at most points of risk in an organisation. Similarly, staff turnover and the number of audit points may also be considered common indicators. Most indicators are not common, but, rather, specific to individual businesses or processes. For example, the frequency of unmatched trades would be a predictor of losses arising from the settlement process within a retail brokerage but is irrelevant to other businesses.





KEY RISK INDICATORS – THEIR ROLE IN OPERATIONAL RISK MANAGEMENT AND MEASUREMENT



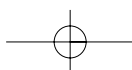
The frequency of unmatched trades is also an example of a *performance* indicator – in this case, of performance in the trade-matching activity. In fact, one person’s KRI is another’s performance indicator (KPI) and a third person’s control-effectiveness indicator, Key Control Effectiveness Indicator (KCI). The preferred terminology depends on the user’s perspective and the activity in which they are engaged, but, not unexpectedly, there is often some overlap.

Uses for KRIs

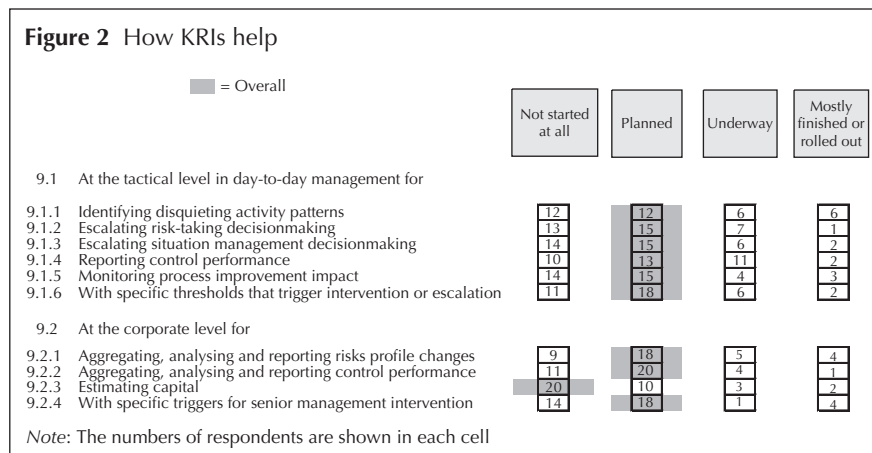
Financial institutions are interested in KRI programmes for many reasons. The Risk Management Association (RMA) conducted a survey of 38 financial institutions in May 2005 on the subject of KRI programmes.¹ As shown in Figure 1 they found that, while most are still in planning stages, they intended to pursue virtually all of the specified objectives for such programmes (see Risk Management Association, 2005).

The highest priority programme objective among respondents to this survey was to use KRIs to report risk profiles to senior management. The next-highest objectives were to create a no-surprise environment and to integrate risk management and measurement effectively. If KRIs are focused on the areas of most significant risk, then they should provide managers with reasonably clear direction as to what levers to pull to reduce exposure, as well as quick feedback on their effectiveness.

Communicating risk appetite (through the setting of KRI thresholds and triggers for action) and the day-to-day management of



AMA APPROACHES TO OPERATION RISK



routine risks in various financial services processes were also viewed to be important objectives.

The RMA survey also asked respondents to indicate how they expected KRIs to help them achieve specific business-related objectives. Again, most financial institutions were still in the planning stages, but expressed their intent for virtually all of the specified objectives. In addition to those *planning* for these objectives (one-third to one-half of respondents), a further one-sixth to two-fifths were already rolling out plans to achieve these same objectives, or they had completed their implementation. The most popular objectives are to aggregate, analyse and report risk profile changes at the corporate level and to report control performance at the business-unit level. Also, most organisations intend or already use KRIs with specific thresholds that trigger intervention or escalation. The only objective that received notably lower focus was that of estimating capital, where the majority of respondents indicated that they have not started to think about this potential application of KRIs.

Value of a common language and structure for KRIs

KRIs are not new, but they are very topical at the moment, being widely viewed as having the potential to make operational risk management a more effective discipline. Financial services regulators in particular have expressed interest in KRIs as a potentially important tool to manage operational risk. However, up to this point, the promise has not been realised for a number of reasons:

KEY RISK INDICATORS – THEIR ROLE IN OPERATIONAL RISK MANAGEMENT AND MEASUREMENT

- ❑ it has been difficult to show that KRIs really track losses well;
- ❑ there is no consistency in the way organisations use KRIs – various units track the same thing but call it something different, and calculate it differently;
- ❑ KRI specifications are often incomplete or inaccurate; and, as a consequence,
- ❑ it has been difficult to aggregate, compare or interpret KRIs in a systematic way.

Clearly, the challenge is to implement KRIs in such a way as to improve consistency, relevance, transparency and completeness. To achieve this, we believe some standardisation is required across the firm and, ideally, across the financial services industry, in terms of both language and approach to KRI implementation. Increased standardisation is increasingly being demanded by regulators and supervisors (who need confidence in metrics used for capital adjustments and other purposes), rating agencies (who need defensible comparative metrics for their models) and stakeholders and auditors (as a way to develop a true understanding of exposure, on the road towards improving corporate governance).

The first step in standardisation should be use of a common language around risks, business activities and products or business lines. A logical place to begin in the development of this language is with the risk types and business lines specified in the “International Convergence of Capital Measurement and Capital Standards – a Revised Framework”, commonly referred to as Basel II, although this is only a starting point. Most organisations find they need greater granularity in risk categories and business lines and they would also benefit from standardisation in the definition of specific business activities, as well as in the definitions and specification of KRIs. Benefits to the firm in developing this kind of common understanding include:

- ❑ permitting indicators to be related to specific risks in a clear and consistent way;
- ❑ permitting alignment of internal and external loss data, risk-and-control assessment results, capital and scenario analysis with KRI data for much more powerful management information and operational risk management reporting capabilities;

AMA APPROACHES TO OPERATION RISK

- reducing confusion when it comes to ensuring robust, complete coverage of all risks, be it for self-assessment, KRIs or collection and classification of loss data; and
- with the use of common KRI definitions, both internal and external benchmarking becomes much easier.

Similarly, a common structure for KRI implementation in terms of the approach used to assess risk, develop indicators, set thresholds and protocols and aggregate and report results across the whole organisation has many benefits. It:

- conveys strong sponsorship at senior levels of the organisation and a commitment to risk management;
- can be used to establish and communicate risk appetite in a deliberate and meaningful way;
- facilitates meaningful aggregation and reporting;
- allows meaningful (internal and external) comparisons;
- ensures efforts to develop KRIs and monitor risk are relevant and focused on areas of highest risk;
- provides greater consistency and assurance in the way risk issues are managed across the organisation;
- ensures robust coverage while reducing duplicative efforts in tracking and monitoring risk; and
- permits systematic adjustments to capital estimates with enhanced credibility.

So, if we can agree that there is great potential business value for a KRI programme, particularly if it is implemented in a systematic way across the organisation, with a common language and structure, then let us proceed to some of the fundamentals in getting such a programme started.

Properties of a good indicator

Key to the effectiveness of any KRI programme is the quality of the KRIs themselves. An assessment of KRI effectiveness largely depends on expert opinion, which is based, in turn, on knowledge of how specific business functions and processes work, where they are vulnerable, and what can affect that vulnerability. Given the inherent subjectivity implicit in most KRI programmes, there is a strong case for establishing a framework for assessing effectiveness.

KEY RISK INDICATORS – THEIR ROLE IN OPERATIONAL RISK MANAGEMENT AND MEASUREMENT

Table 1 Criteria for good KRIs

Effectiveness	Comparability	Ease of use
Indicators should: <ul style="list-style-type: none"> <input type="checkbox"/> apply to at least one specific risk and one business function or activity; <input type="checkbox"/> be measurable at specific points in time; <input type="checkbox"/> reflect objective measurement rather than subjective judgement; <input type="checkbox"/> track at least one aspect of the loss profile or event history, such as frequency, average severity, cumulative loss or near-miss rates; and <input type="checkbox"/> provide useful management information 	Indicators should: <ul style="list-style-type: none"> <input type="checkbox"/> be quantified as an amount, a percentage, or a ratio; <input type="checkbox"/> be a reasonably precise and definite quantity; <input type="checkbox"/> have values that are comparable over time; <input type="checkbox"/> be comparable internally across businesses; <input type="checkbox"/> be reported with primary values and be meaningful without interpretation to some more subjective measure; <input type="checkbox"/> be auditable; and <input type="checkbox"/> be identified as comparable across organisations (if in fact they are) 	Indicators should: <ul style="list-style-type: none"> <input type="checkbox"/> be available reliably on a timely basis; <input type="checkbox"/> be cost-effective to collect; and <input type="checkbox"/> be readily understood and communicated

We believe that the ideal features of KRIs are that they are effective in tracking the risk, they are comparable within and outside the organisation and they are practical and easy to use. Table 1 provides some criteria for assessing indicators against these three objectives.

Along with a framework for assessing KRIs, it is helpful to develop some standards for fully specifying an indicator. It is our experience that a relatively high degree of detail is beneficial in minimising misunderstandings and in ensuring a high degree of quality and efficiency in the implementation of KRIs. This detail should include:

- full definition and description of what is collected;
- how to measure and calculate (in detail); and
- guidance for implementation (sources, collection, uses and so forth).

For example, staff turnover as an indicator could be described as the turnover percentage across all categories of permanent staff

AMA APPROACHES TO OPERATION RISK

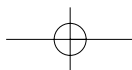
during the preceding month. It is a measure of risk due to inadequate or failed human performance. It would rate relatively high on the KRI assessment criteria listed above. It can be measured against multiple dimensions, including location, country, business unit, product or service group and job function. It should probably be measured for full-time and part-time employees separately. We should also have some rules for the period of time to be assessed and the frequency of measurement, and some specifics of who should be included and excluded in the count (eg, it may be that contractors should be excluded). There should also be rules for scaling the indicator to allow comparisons with differently sized units (not applicable for this indicator) and aggregation of results within a line of business or the organisation as a whole.

Leading, lagging and current indicators and trending indicators

Indicators can be leading, lagging or current in nature. Most managers want leading or preventative indicators – to predict problems far enough in advance to prevent or eliminate them or at least mitigate the damage. Unfortunately, prevention of incidents is a desired but rarely achieved forward-looking aspect of operational risk management.

Accordingly, current and lagging indicators also have their place. Current indicators provide a snapshot or current view of operational risk exposures. They may identify a situation that may require attention to reduce exposure or minimise loss. Lagging indicators can be considered as more “detective” in nature, and can provide useful information regarding the historical causes of loss or exposure. They may also be useful where losses are initially hidden from view, or where changes in historical trends can reflect changes in circumstances, which may in turn have predictive value. An example of a current indicator could be the number of threatened legal actions or the number of customer complaints. An example of a lagging indicator could be the number of critical system outages.

In our experience, leading indicators are generally environmental indicators, or they are based on causal analysis or expert opinion. Environmental factors are the most common leading measures of operational risk. These are measures of the state of people, process, technology and the market that affect the level of risk in a



KEY RISK INDICATORS – THEIR ROLE IN OPERATIONAL RISK MANAGEMENT AND MEASUREMENT

particular organisation. A leading or preventative KRI can be something as simple as the number of limit breaches on market or credit risk exposures, or cash movements, or the average length of delays in executing a transaction. In themselves, such limit breaches may not be incidents, but, if the number of breaches and their value starts to increase, this may point to the potential for a higher frequency or severity of incidents: unauthorised breaches, or impending failures in other processes.

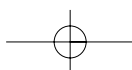
One misconception about leading indicators is the assumption that establishing or projecting future values from historical trends results in a leading indicator of risk. While this may be the case where sophisticated techniques such as charts and dynamic anomaly pattern response are used, in general, trending does not produce leading indicators, which need to provide useful information about future events in and of themselves, generally through the use of thresholds and triggers, which are discussed later in this section.

However, it *is* beneficial to measure KRIs over time, in order to detect trends and provide contextual information. For example, consider the KRI for late-trade processing for Firm X, shown in Figure 3. In May, the percentage of late trades is 9% for London and Singapore and 10% for New York, which in the face of those facts alone might lead us to conclude that New York has a slightly riskier operation. However, further analysis of the trends suggests that, in fact, Singapore may have an emerging problem.

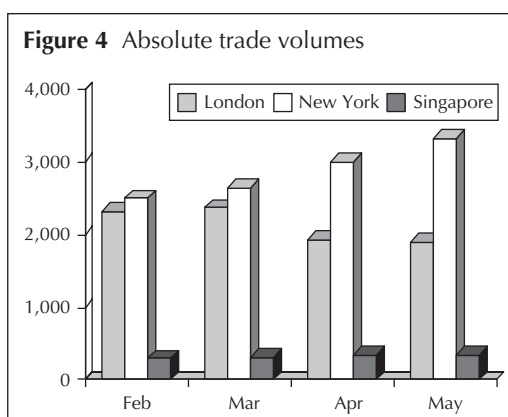
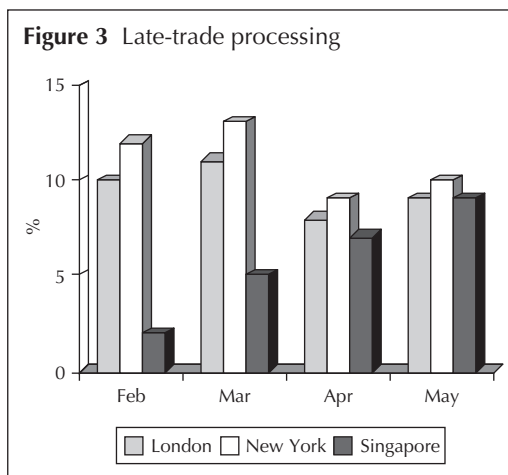
But, again, if we check the absolute trade volumes of these various locations (see Figure 4), we learn that New York's late trades have risen only slightly against a significant increase in volumes, and Singapore's increase in late trades is based on a very low volume of trades. Context is everything! It is usually beneficial to know the underlying trend of an indicator, as well as to look at it in the context of other KRIs and other management information, in order to really understand the story the numbers are suggesting.

KRI selection

Having a good understanding of the desirable characteristics of a KRI, we now come to the stage where they must be selected and bundled into a programme for a business area or unit or the organisation overall. Most practitioners believe that KRIs are of highest use when applied at a fairly granular level within the organisation,



AMA APPROACHES TO OPERATION RISK



used by middle managers to monitor and manage day-to-day risks. They can then be filtered and aggregated for reporting to more senior management. Accordingly, the construction of a KRI programme ideally starts with an individual business unit.

Because KRIs are supposed to track key risks, the first step in KRI selection is to identify areas of highest risk for the business unit in question. It is important to have a consistent and comprehensive approach to this analysis. It can be done by risk mapping or profiling each business unit, or leveraging risk-and-control assessment programmes already in place. The analysis should

KEY RISK INDICATORS – THEIR ROLE IN OPERATIONAL RISK MANAGEMENT AND MEASUREMENT

focus on component processes or business functions within each business, considering how they work, and where a material loss has been or could be experienced.

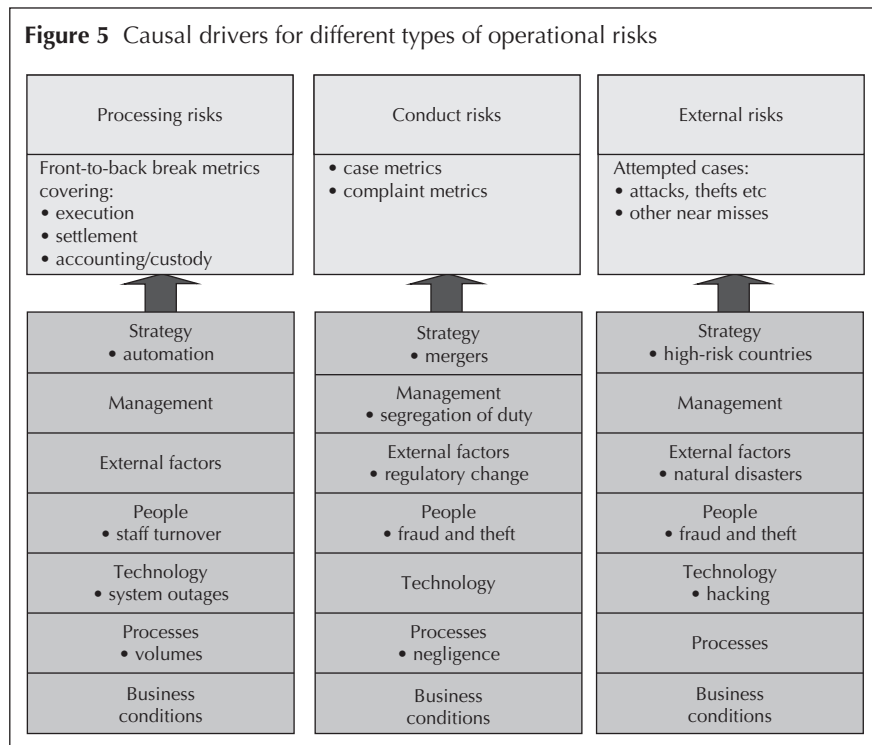
Participants in the assessment should assess *residual* risk, after the impact of current controls is taken into account. It is helpful to ask them to focus on the expected loss in the worst year over an understandable time horizon, for example, 10 years – this captures the effect of a typical economic cycle on risks, is reasonably easy for most participants to conceptualise and embraces the time horizon of most strategic initiatives and the majority of banking obligations. Generally, we suggest that assessments should include the impact of reputation damage as well, as these are real impacts to the organisation, if a little harder to quantify.

Once high-risk areas are identified, the business needs to consider what existing indicators or metrics could be leveraged or new ones created to help anticipate a loss, monitor an exposure, measure the risk, manage the exposure or loss, or report on the risk and its implications. An inventory of existing KRIs, as well as the identification of the high risks for which there are not currently KRIs in place, is often a good first step in this process. Once gaps are identified, it is important to consider a variety of KRIs against each risk type, as each KRI is reflective of a specific causal element which may come into play if a loss occurs. Figure 5 illustrates this concept.

Ultimately, however, in order to keep the number of KRIs being monitored to a manageable number, it will be necessary to select the few that best reflect the business unit's collective understanding of the key causes of each potential problem. This selection should also be guided by consideration of the quality of the potential indicators against the effectiveness, comparability and ease-of-use criteria discussed above, as well as their contribution to the goal of obtaining a reasonable mix of leading, current and lagging indicators. This is an art rather than a science at the moment, but, in the hands of experienced practitioners in the business, should represent a reasonable start. Of course, fine-tuning the KRIs will naturally occur over time as the business learns and gains experience with these relationships.

Once selected, each indicator needs to be defined and specified as discussed above to ensure clarity of interpretation and implementation. The next step is to establish bands of acceptance that essentially codify risk appetite, and triggers for escalation and/or

AMA APPROACHES TO OPERATION RISK



some other form of action. Indicators are then assessed on an ongoing basis against this frame of reference.

In the case of high-frequency, low-impact exposures, it is often useful for managers to think about different *ranges* of indicator value as calling for different kinds of action:

- low-risk range: no action required;
- medium-risk range: some action required; and
- high-risk range: issue to be escalated to management; other actions required urgently to mitigate damage.

Thresholds can be set to define each range and trigger each kind of response. After a threshold is breached, actions taken by managers to accept or mitigate the risk should be recorded.

Thresholds and escalation triggers are an important risk management tool. KRI thresholds will vary from institution to institution, depending on management's risk appetite, as well as strategy

KEY RISK INDICATORS – THEIR ROLE IN OPERATIONAL RISK MANAGEMENT AND MEASUREMENT

and ability. For some risks the thresholds may be quite low and others higher. They can also change over time, if there is a strategic decision to manage risk down (or sometimes up). Managers will become more experienced at setting the appropriate level of threshold over time. This is where art meets science as there can be no one-size-fits-all approach or algorithm for thresholds. It is subjective and based upon the managers' risk appetite and experience, and that of their peers within the firm.

What is a reasonable number of KRIs? Many financial institutions have a very large number. This may be justified by the heterogeneity of operational risks and complexity of financial services and products. We believe that a large diverse institution would reasonably use between several hundred and a few thousand indicators in middle management. Of course, these cannot all be reported to senior levels of management. Accordingly, it is very important to have an appropriate strategy for reporting and aggregating KRIs to senior management and the board.

AGGREGATION AND REPORTING OF INDICATORS

In the previous section, we explained the basics of KRIs, starting with what is a good indicator, through the need for a common language and, finally, techniques for KRI selection. It is these building blocks that provide the foundation for the aggregation and reporting of KRIs.

Key elements of a robust structure for KRI aggregation and reporting are:

- clear objectives for the reporting and aggregation mechanism;
- common data dimensions and classification;
- content appropriate to the required level of analysis and decision making; and
- timeliness and accuracy to the required level of materiality.

Let us explore these factors further.

Clear objectives for the reporting and aggregation mechanism

The objectives of any management information system need to be defined before data are gathered to populate it, otherwise a meaningless paper chase will be delivered with no added value to operational risk management. The objectives can be defined at the

AMA APPROACHES TO OPERATION RISK

business-line level, although some homogeneity of concepts will be essential across the firm to facilitate benchmarking and multidimensional risk analysis.

There is a clear difference between data and management information. Data can be fairly “raw” and of little or no use to any manager. Information is the result of transforming the data into meaningful and incisive management tools for the better management of operational risk exposures in a timely manner. When so-called indicators are being collected without a clear view about what they are reported for, or to whom or where they are reported, the firm has a problem. The data-collection effort will be in vain and any management information will be lost with no value added to the business or firm-wide operational risk management process.

Few KRI reporting frameworks will succeed if they are implemented merely with the objective of regulatory compliance.

Data collection without risk management decision making will provide the businesses and functions with negative added value: they will implement a reporting framework for a cost without benefit. A better and more reasonable objective would be “to better manage operational risk”. This will provide the managers in the businesses and functions with information for operational risk management decisions regarding risk acceptance and/or mitigation.

Common data dimensions and classification

To facilitate aggregation of KRI data in a meaningful way, the firm must have a classification system with appropriate hierarchies reflecting the organisational structure. Ideally, this system of classification and the concepts embedded in it should be common across the operational risk framework, and in many cases with pre-existing management reporting. As we alluded to earlier, most managers have risk *and* performance objectives, so it makes sense to have some commonality of concepts across risk and performance measurement, although the granularity may differ with risk exposure being at a more aggregated level than process efficiency.

Accordingly, we would expect that most firms will have already defined a number of core data dimensions that are integral to aggregating and reporting KRIs, such as:

- incident* (historical and potential), normally consisting of:

KEY RISK INDICATORS – THEIR ROLE IN OPERATIONAL RISK MANAGEMENT AND MEASUREMENT

- one or more causes;
- one or more events (as in a chain of events);
- financial and non-financial (ie, reputational) impact on profit and loss; and
- risk categories;
- process*, with a clearly defined hierarchical level consisting of:
 - end-to-end processes, typically referred to as a complete business function;
 - sub-process components;
 - process types;
 - function domains (HR, finance, compliance, IT, communications and so on);
 - shared processes; and
 - hand-offs between departments or business functions;
- control*, consisting of:
 - control types (ie, reconciliation, accounting, review, management);
 - control attributes (ie, automated, manual); and
 - preventative and detective controls;
- product*, consisting of:
 - business lines; and
 - product and service groups;
- reporting entity:
 - branch, territory, function, business line, legal entities, joint ventures, outsourcers and so on.

The regulators have defined the scope of operational risk and have provided, for regulatory reporting purposes, an event-type classification. The other data dimensions should be defined by each firm according to its own risk management framework with the appropriate emphasis placed upon each one in relation to the specific attributes of each firm: complexity of business model, global and local operations and management structure, number of product lines and so on.

Content appropriate to the required level of analysis and decision making

One of the most important challenges in establishing a KRI programme is to ensure that each level and area of management gets the KRI information that is appropriate for its needs and

AMA APPROACHES TO OPERATION RISK

responsibilities. This is a big part of the art of creating management information out of data, as discussed earlier. Each manager should be receiving KRI information that allows them to proactively identify problems within their area of concern, and take appropriate action, even if that is simply to escalate or delegate to the next level up or down. In essence, KRI reporting needs to be customised within each business unit and at each level of the organisation, similar to other kinds of management reporting. While this may seem like a tall order, it is actually a natural part of the KRI programme roll-out within each area of the firm, and, once completed, will represent a very powerful tool in managing operational risk more effectively.

There are several elements to consider when deciding who should see each KRI. We will consider each of these in turn.

The level of granularity or risk exposure being measured by the KRI
KRIs can be set at any level of risk exposure. Consider the following examples:

- At a regional level the firm may track the number of actual breaches of specific local laws and regulations for a single process, which are not declared to regulators.
- At the global level it might monitor the number of internal audit points overdue for each business unit.

The management information that these KRIs provide are at two different levels but both are relevant for the management of operational risk. In the first example, the number of undeclared actual breaches of laws and regulations gives an indication of exposure to potential fines if and when the regulators find out during one of their inspections. This means something to the regional head who is managing the reputation of the branch across all business lines, as well as to the manager responsible for the breach. However, it should not impact the CEO's decision making, as the CEO has delegated this responsibility to the regional head, so should not concern themselves with such minutiae.

In the second example, the lack of action regarding implementation of internal audit points is a global KRI, and one that would be of interest to both the head of internal audit and the CEO. These two indicators measure different levels of exposure: one at the individual process level in a region and the other across all processes

KEY RISK INDICATORS – THEIR ROLE IN OPERATIONAL RISK MANAGEMENT AND MEASUREMENT

and exposures within the firm. Generally, the higher the level, the greater the interest to senior managers, provided it relates to their area of purview.

The breadth of risks represented by the KRI

When KRIs point at causes that could lead to multiple events across all event types, the CEO will be very interested. In essence, these multi-event indicators, analysed by cause rather than specific potential events, provide early-warning signals regarding unexpected losses and a flag to senior management to start asking some pointed questions.

A good example of a multi-event indicator is the total number of audit points outstanding. Some audit points can easily be related to specific exposures and mapped to the Basel II event types. It is more difficult to do this with others, for example, when they are related to causes such as a lack of appropriate management skills. If a KRI analysis results in the conclusion that there are insufficient management skills in any specific unit or location, this is an issue appropriate for the attention of senior rather than lower levels of management.

The current “temperature” (red, yellow or green) of the KRI – bottom-up indicators

Most indicators collected by businesses stay in the business without any reporting to a higher level within the organisation. Senior management delegates the authority to manage most operational risks to appropriate levels and functions and outsourcing service providers throughout the firm. As we discussed earlier, each business unit or function is then responsible for developing its own KRIs based on a bottom-up assessment of the risk in its area. The process level indicator measuring undeclared local law breaches is a typical bottom-up indicator.

However, if a KRI breaches the thresholds or trigger points previously established, then it is usually escalated to the next level of management, depending on the materiality of the situation. The senior manager must then decide whether to accept the risk and increase the threshold or reduce the risk indicated by the management information. Some managers also set triggers at an earlier point, when the indicator *starts* to trend upwards or accelerate

AMA APPROACHES TO OPERATION RISK

towards the threshold level. This is useful if the manager prefers a window to deal with any emerging situation *before* the threshold is actually breached, and they are obliged to report it to more senior management. In some cases, triggers can be set so as to escalate only when a condition persists, or when a certain level of indicator volatility is exceeded. For example, a single breach of a KRI threshold may result in immediate action that is within the delegated authority of the manager, thus not requiring escalation to the next level of management. However, if the condition persists or becomes repetitive, then the trigger is set off, and the problem is escalated. Thresholds should be dynamic, so that when volume increases the thresholds are “scaled up” to take account of the increased volume, otherwise too many excesses over thresholds will be reported.

Of course, if a KRI is considered to represent a particularly significant risk, or it tracks risk in a business unit of significant size or materiality relative to the entire firm, or it exceeds the threshold by a significant amount, this KRI may need to be escalated beyond the immediate senior manager. Ultimately, there may be some bottom-up KRIs that need to be escalated to business or function heads or the CEO. This gives the most senior levels of management a window on emerging areas of significant risk in the organisation as and when they occur.

The specific risk focus of the KRI – top-down indicators

Top-down KRIs are generally set in conjunction with group functions and may relate to general causes or specific potential process failures or events. Total outstanding audit points or the state of the overall management skills of an entity are typical examples of top-down indicators set by the heads of internal audit and human resources respectively, for the CEO’s review. Other examples set by the heads of group functions are:

- legal*: the total number and value of legal claims against the firm, in total and by business line and peer group;
- finance*: the number of incidences of late financial reporting by legal entities within the group, or number of accounting errors or unexplained differences; and
- IT*: the number of attempted external attacks to the firewall.

KEY RISK INDICATORS – THEIR ROLE IN OPERATIONAL RISK MANAGEMENT AND MEASUREMENT

Clearly these KRIs are somewhat specialised and generally of interest only to the CEO and the most senior management, particularly within functional areas.

In some cases, top-down and bottom-up KRIs can be directly linked together to form a chain in the operational risk exposure management process. For example, we can imagine a situation where many audit points have arisen from various control-effectiveness reviews. These can be considered bottom-up KRIs as they arise directly from detailed risk analysis of specific processes. The respective process owners/departments will be allocated responsibility for taking remedial action before the audit points are reported to the CEO at the global business level.

However, the cause of the problem of many outstanding audit points may not be within the powers of the individual managers to solve. The individual managers may not have the mandate to address some of the root causes due to their breadth or implications; they may have insufficient resources to carry out the day-to-day operations *and* fix endemic control or system issues that require some modest investment; or they may not have the scope of management information to recognise a larger systemic problem. This is a particular concern in trading and sales businesses where the profit and loss is very short-term-focused and the medium-term operational risk exposures of chronically lagging back offices are often ignored or underinvested. So, at the end of the day, the mitigation of the risk by investment or the acceptance of the exposure needs to be the responsibility of the business unit head or the CEO. The CEO can put pressure on the business unit head based upon the KRI of outstanding audit points. They can also assist with a reallocation of resources as required, if the exposure to operational risk is above that desired.

Ideally, through the application of the above principles, each manager will end up with a portfolio of KRIs that reflects the risks of most importance to their mandate. The manager will also have a clear understanding of the action required when thresholds or trigger are breached, including which KRIs need to be escalated to the next level of management or higher.

Timeliness and accuracy to the required level of materiality

The final element of a robust reporting and aggregation programme for KRIs is timeliness and accuracy of information. If it

AMA APPROACHES TO OPERATION RISK

takes longer to collect the indicators than the timescale required by the decision-making process, then the indicator has failed the “timely” test. Indicator reporting and aggregation should balance speed with accuracy. The late reporting of indicators achieves nothing. If the systems or manual nature of the reporting process leads to delays, it is better to sacrifice some of the accuracy for speed. In other words, if the indicators are 80% rather than 100% complete or accurate, in many cases that is sufficient information to enable the manager to take appropriate action.

In summary, a strong KRI aggregation and reporting programme will have as its clear objective the effective management of operational risk, and will be founded on data dimensions and a classification system that are common to the entire operational risk framework, as well as many elements of the firm’s general management reporting structure. It will also ensure that each manager views those KRIs that are appropriate to their mandate and scope of decision making, and that the KRI data are timely and accurate within reason.

No discussion of KRI aggregation and reporting would be complete without addressing one more issue, namely the concept of the “top ten” indicators to be reported to the CEO and the board of directors.

The mythical “top ten” KRIs for senior management

Some firms wish to report at the very highest level, the “top ten” KRIs – and the group operational risk team are required to find them. This quest is like searching for the Holy Grail. They will never find what they are looking for but a whole mystical and quasi-religious framework and following will be created in the process. This search will feed itself, resulting in the KRI framework being criticised for lack of added value, the possible withdrawal of investment and a perception that KRI monitoring is an abject failure.

While we understand that senior management desires predictability and conciseness in reporting, every risk manager will know this dream is not achievable through the selection of 10 operational risk KRIs. Businesses constantly change their risk exposure to operational risks as they, and the market and world within which they operate and manage, change. KRIs that were relevant last year may well not be relevant this year. The portfolio of information that

KEY RISK INDICATORS – THEIR ROLE IN OPERATIONAL RISK MANAGEMENT AND MEASUREMENT

is required to communicate these risks will change over time, and will certainly be very different from one business to another.

Of course, there is a role for top-down indicators. Ideally, there will be some support from group functions to set an appropriate number of these in keeping with the perceived risks. It is best practice to have at least two KRIs for each group function: human resources, information technology, legal, finance, compliance, group risk, and audit. There may also be one or two KRIs selected for each main “multi-event” cause. This totals about 12–20 indicators.

In addition to these top-down indicators, as we discussed before, consistent or material breaches of thresholds should be reported to senior management. Those indicators set by managers that are within the thresholds should stay where they are: in the business line or function to be reported and used locally.

Some final comments on reporting

Many KRIs currently collected by businesses and functions are for managing expected rather than unexpected losses. Therefore, their contribution to capital measurement may be limited, but the value added to the businesses for managing exposures to the range of losses between expected and unexpected is immense.

Setting relevant and reliable indicators is a challenge. They should be linked to the causes of operational risk incidents so that operational risk managers can monitor the drivers of operational risk exposures on an ongoing monthly or quarterly basis. It will not be known whether the indicators are “key” until they are refined in the light of experience. Such experience will require at least two years’ worth of complete indicator data and internal incidents. Most firms will not have accumulated such a time series of homogeneous indicators using group-wide concepts and definitions before they have to pass regulatory validation prior to Basel II deadlines. Therefore, this is a challenge both before and after the Basel II validation process. The first gathering of consistent indicators across the firm has commenced in 2006, but the time series necessary to decide on the “key” ones could take another year until 2007.

Nevertheless, firms who do invest in this area will eventually have a dynamic, predictive library of indicators they can interchange depending on the particular business, process, geography

AMA APPROACHES TO OPERATION RISK

or market environment. This target is some way off for most firms today, but we believe the investment will reap many benefits.

ADVANCED APPLICATIONS FOR KRIs

While the benefits of a robust, dynamic and comprehensive set of KRIs across the organisation coupled with strong aggregation and reporting are worthy objectives on their own, they also open the door to some more “advanced applications” and opportunities. These include the potential for measuring the success of our risk management activities, building risk indexes and benchmarking KRI performance. We will briefly consider each of these in turn.

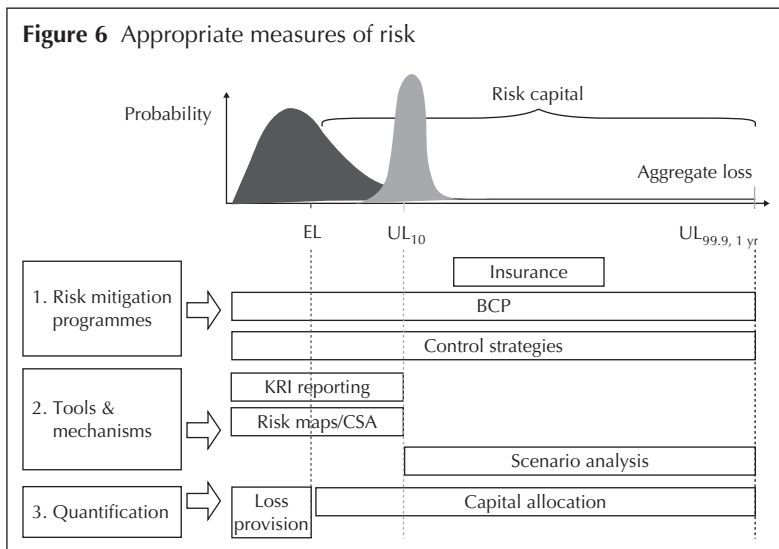
Relationships of KRIs with losses and risk and control assessment (RCA) output

In arguing the benefit of KRIs, many risk managers are seeking a strong cause and effect relationship. After identifying certain KRIs and managing them down, does the organisation see a reduction in risk? The answer depends on a number of factors, but in our experience the statistical correlations will be weak even for the more effective measures. This doesn't mean that the indicator is ineffective. It may still achieve its objective – when identified and managed, the management of the indicator produces a reduction in one or more characteristics of the loss profile: frequency, severity or both. The lack of correlation is due in part to the multifactor relationship between losses and their drivers, and also to the variable timing differences between managing the cause and the impact on the recognition of a loss. But these relationships will be improved if the *measure of risk* used is consistent with the KRIs themselves.

What do we mean by that? Well, there are many measures of risk, in fact, an infinite number. This is illustrated by the loss distribution curve in Figure 6. At different confidence intervals, you are assessing the different likelihoods that a firm will suffer one or more events of a certain aggregate impact.

One common measure of risk illustrated in this distribution is the mean or expected loss (depicted at the point “EL”). However, this is not really risk, as the mean is predictable with reasonable accuracy. Another common measure of risk is the 99.9 percentile on

KEY RISK INDICATORS – THEIR ROLE IN OPERATIONAL RISK MANAGEMENT AND MEASUREMENT



this curve, which is often used to determine capital requirements for the firm. This measure is located on the far right of the curve ($UL_{99.9, 1 yr}$), and shows the aggregate loss at a confidence interval of 99.9% using a one-year holding period. This is equivalent to measuring losses for the single worst year in 1,000 years, for a given loss type. That is almost impossible for management to conceptualise, and in reality very few KRIs are likely to influence such extreme measures of risk.

Which leads us to the question of whether there is a more appropriate measure of risk for *risk management* purposes. Ideally, we would like a measure that addresses that range of exposures between expected and unexpected losses, providing a conceptual or specific target for our risk management activities, and a source of feedback on our success. Well, the answer is a resounding yes!

One possible standard is a measure of the worst year of losses predicted over a 10-year horizon, or UL_{10} . This empirical measure is roughly equivalent to a probabilistic risk measure using a confidence interval of between 90% and 95%. This standard would better define the risk that can be reasonably and practically assessed in risk assessment processes and that is the focus of KRIs and much of

AMA APPROACHES TO OPERATION RISK

the risk information currently in use. It may also assist in defining the boundary between management techniques such as risk-and-control assessments and scenario analysis.

Most of the KRIs and management information used to manage the risk-and-control environment identify the more routine “unexpected” risks – those that occur once every 5–10 years – through the typical operational, investment, market, credit or economic cycle. This is appropriate because these are the risks that management can realistically imagine resulting in an event, and that they can actively influence. True, management may also mitigate the less regular operational risks through controls such as business continuity planning, but even these are typically “tested in anger” more frequently than once in 20, 50 or 100 years, making them easier to conceptualise, manage and mitigate than risks that occur even less frequently.

Therefore, we believe that a UL_{10} basis provides a more appropriate measure of risk on which to focus our risk-and-control assessments and KRI frameworks, and one that should correlate more closely to good predictive indicators.

Collections of indicators and composite or index indicators

We discussed earlier the common desire for a magical “top ten” set of indicators that can inform the firm or business area on the profile of its operational risks. While we believe this is an unrealistic goal, a more realistic possibility may be a set of KRI “indexes” that comprise different measures, which in essence try to represent a score for each specific risk exposure. It is also possible that the classes of these composites or index indicators could be very similar across business lines and possibly across the industry.

Possible indexes might include:

- process quality index;
- technology stability index;
- client satisfaction index;
- employee satisfaction index;
- litigation exposure index;
- ethical quality index; and
- asset protection index.

KEY RISK INDICATORS – THEIR ROLE IN OPERATIONAL RISK MANAGEMENT AND MEASUREMENT

For example, to compile an index on process quality, the first step is to identify the underlying KRIs that address the risk drivers impacting process quality, such as the level of automation, the process error rate, the aggregate cost of rework, the number of related client complaints and the costs of restitution. These KRIs are then combined into a weighted value that can be tracked over time, and, in aggregate, give a better picture of the risk.

In theory, the “formulas” for these internal indexes could also be agreed externally among peer firms; however, practically speaking, this may be difficult, as establishing such composites is no trivial task. It requires the use of a standardised classification framework across all forms of operational risk information, coupled to factor and multivariate statistical analysis across a relevant data series. Even then, the resultant composite indexes will need to be tested and possibly refined over time in the light of actual experience.

However, one exciting area for operational risk index development currently under exploration is the establishment of indexes for external factors. Examples could include:

- white-collar crime;
- blue-collar crime;
- payment systems stability;
- weather events; and
- terrorism ratings.

Many of these exist today as governmental outputs on socioeconomic conditions. They represent information on the external environment in which an institution operates, and the deterioration in such an indicator would surely be a worthy input into a measure of the risk environment of a firm for a location in which it operates. In fact, these indexes themselves could be aggregated into country ratings for any given country to provide information on foreign country risk. They could even be extended to cover political risks as well.

Internal/external benchmarking

There should be an optimum level of operational risk exposure for a given institution – in theory, being too low could be as costly as being too high. An overcontrolled organisation that continues to

AMA APPROACHES TO OPERATION RISK

make risk investments where the incremental return on increasing controls is actually negative is as risky as the organisation that makes little effort to control such risks.

How do we start to answer the question of whether the level of risk we are implicitly or explicitly accepting is too high or too low? By comparing who is in the newspapers? By comparing loss distributions? By comparing KRIs? Ideally, we could try to mark-to-market operational risk investments, and, perhaps one day, we will be a position to do this. A more practical alternative is to benchmark the risk environment in some fashion either internally against similar business lines, or externally in comparing the performance of business lines across a peer group.

The best operational risk metrics for benchmarking performance are, without doubt, KRIs. KRIs are periodic monitoring mechanisms to identify risk drivers in an objective manner. They make a good basis for comparison because they represent exposure, and business areas relate to them easily. KRIs are likely to be similar in the similar business processes that exist to support similar products. If a common basis is established to measure a KRI across processes within a firm or across institutions, and a process is established to compare performance, then benchmarking is a viable feedback mechanism to compare the riskiness of similar processes across a peer group.

Benchmarking KRIs can provide many benefits to participating firms, including:

- an opportunity to learn from peers and exchange information, ideas and concepts with them;
- an opportunity to assist in developing industry best practice, thereby making it easier to gain internal support and acceptance for risk management principles;
- an increased awareness of risk exposures within the firm, simply through the association with initiatives supported by peers and competitors;
- the ongoing development of standard language and frameworks for the identification, measurement, management, monitoring and mitigation of operational risks; and
- the opportunity to directly compare risk exposures with peers, using exactly the same language and structures, thereby gaining a better understanding of the firm's relative riskiness, and validating or

KEY RISK INDICATORS – THEIR ROLE IN OPERATIONAL RISK MANAGEMENT AND MEASUREMENT

contradicting any preconceived notions of the conceptual level of risk being run by the firm.

While there is no argument that competition remains a driving force in successful business management, there are equally strong arguments that operational exposures facing one firm also face others, with adjustments for differing cultures and risk appetites. Accordingly, there must be mutual benefit in being able to benchmark your risk profile by comparing specifically focused, standardised risk indicators, especially if these can be compared to the firm's own internal loss history, its current risk-and-control assessment scores, specific scenarios being analysed and the amount of economic and/or regulatory capital being set aside. The benefit becomes even stronger when public loss data published into the public domain and loss consortium data employ the same frameworks and structures, thereby facilitating comparative benchmarking.

Today, the industry has begun to recognise these benefits, and, in fact, there is now a specific industry initiative under way that not only permits KRI benchmarking, but, in essence, represents a library of data and information to support the establishment of KRI programmes for participating firms.

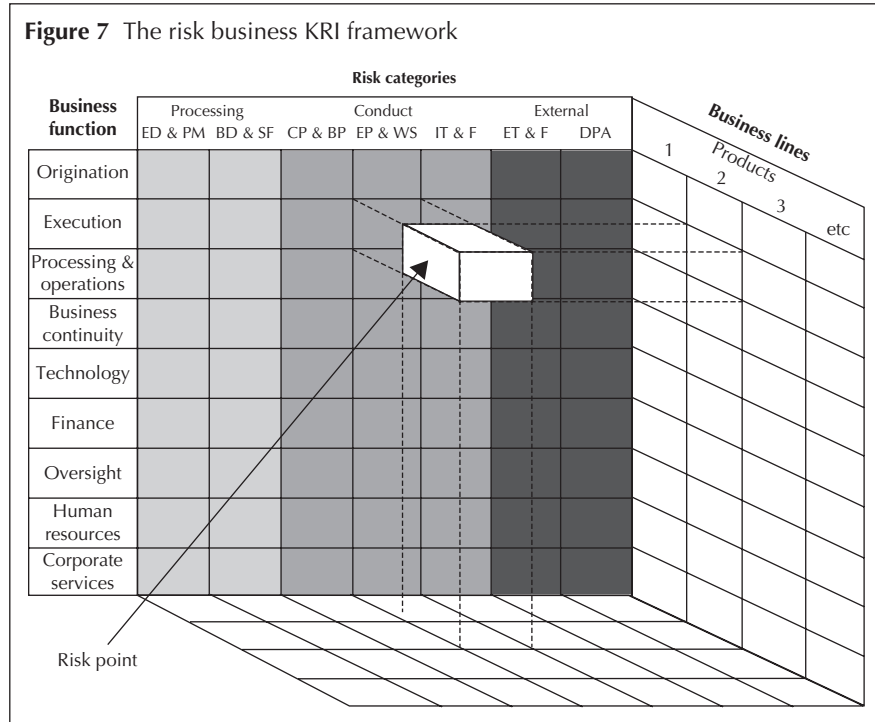
www.KRIeX.org – THE INDUSTRY KRI REPOSITORY

In 2003, the Risk Management Association, in conjunction with RiskBusiness International Limited, launched an initiative aimed at furthering the use of KRIs across the financial services industry. This followed the publication of several white papers by international rating agencies regarding the inclusion of operational risk effectiveness capabilities into a firm's credit rating, as well as the publication of draft Basel II guidelines that suggested that standardised indicators could be used to adjust a firm's calculated capital reserve requirement under the advanced measurement approach.

This initiative had three specific objectives:

- to establish a common "language" or framework through which areas of greater risk exposure could be identified and measured. This structure is depicted in Figure 7;
- for each such high risk point, to identify, define and establish a standard specification for suitable risk metrics to measure, monitor and manage such exposures; and

AMA APPROACHES TO OPERATION RISK

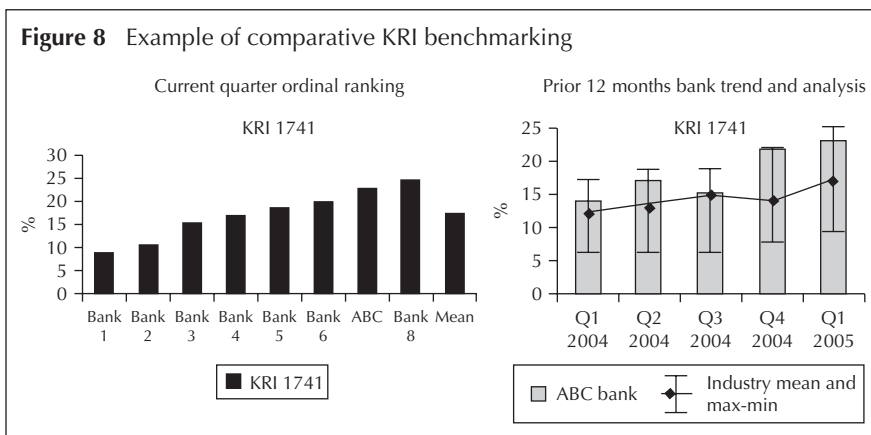


- to facilitate the formal comparison of such exposures between peer groups, using the standardised specifications in an anonymous manner.

Today, this industry initiative has transformed into best practice around KRIs. With more than 100 global firms participating, common areas of concern around operational risk have been identified, and linked to specific risk categories, product or service areas and business functions (ie, specific areas of business activity where such risks arise for each product or service area considered).

For each of the agreed areas of higher risk, subject matter experts from these leading firms have provided their input in identifying, developing and reviewing detailed specifications for suitable indicators that provide timely, value-added information on the exposure. More than 2,000 of these indicators are now provided through a subscription-based online repository of KRIs maintained by the RMA at <http://www.KRIeX.org>

KEY RISK INDICATORS – THEIR ROLE IN OPERATIONAL RISK MANAGEMENT AND MEASUREMENT



Benchmarking

As an extension of the original RMA/RiskBusiness initiative, a global set of working groups continue to investigate both changing trends in exposure and changes in the identified risk profiles. These same working groups are involved in extending and maintaining this library of KRIs. At the same time, subscribers who have identified which indicators they wish to compare with their peers are now engaged in collecting indicator information in accordance with agreed specifications, with the purpose of comparing values against their peer group. An example of the kind of reporting to be generated in support of this benchmarking is shown in Figure 8.

In this example, a fictional bank, ABC, is shown as being above the mean for the current analysis period, and historically not only usually above the mean, but tending towards the top end of the exposure distribution. If ABC considered itself relatively risk-adverse, it would expect to be consistently below the mean for any risk measure. So, in this case, ABC management would want to initiate corrective action to reduce relative risk. However, it is possible that, when this indicator was selected internally for management purposes, a threshold range was established that has still not been triggered – it is only through comparison with peers that we can identify that we are out of synch (or have a competitive advantage) relative to the market.

This initiative has proved two things: first, firms *are* prepared to work together to ensure appropriate internal risk management;

AMA APPROACHES TO OPERATION RISK

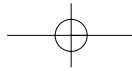
second, we all face very similar operational risk issues. We believe that access to the collective experience and knowledge of the entire industry, as represented by more than 2,000 standardised indicators in the KRI Library, as well as through the various regional and business line working groups, is a powerful tool for enhancing any firm's operational risk management.

CONCLUSION

Today, many firms have, often from necessity, left the establishment of an integrated KRI programme to last in their order of priorities. Many industry participants question the role of indicators, both from a top-down and a bottom-up perspective. Others argue that industry participants would be reluctant to contribute KRI data for benchmarking, due to discoverability issues as well as the potential for gaming.

However, KRIs (or risk indicators in general) have one very specific quality that no other operational risk management or measurement tool offers: quasi real-time exposure information.

- ❑ Loss data, whether internal, provided by a public source or obtained from a data consortium, is fundamentally lagging in nature, representing a past state of affairs, which in most cases is repaired long before the data analysis hits the risk manager's desk.
- ❑ Risk-and-control assessments are periodic subjective evaluations of the state of affairs, often supported by audit programmes, issue tracking and change management programmes. While important in understanding and anticipating exposures, these periodic evaluations cannot measure ongoing change.
- ❑ Scenario analysis allows you to consider what could happen to you, but in isolation tends to be considered as far-fetched, or a measure of the almost impossible – it certainly cannot provide an accurate barometer of real-time conditions.
- ❑ Setting aside economic or regulatory capital as a safeguard is the ultimate fail-safe – any firm that gets to the point where it needs to employ these measures is in such deep trouble that it is probably too late to contain much if not most of the collateral damage from what has already happened. Insurance is also an uncertain safeguard, with some potential relief triggered after the event has occurred.



KEY RISK INDICATORS – THEIR ROLE IN OPERATIONAL RISK MANAGEMENT AND MEASUREMENT

However, similar to the way in which the fuel gauge, oil pressure gauge, engine temperature gauge and speedometer in a motor vehicle all provide you with vital information as to your safety and likelihood of survival, a KRI programme is the only way to provide management with the real-time targeted feedback they need to make mid-course adjustments as required. And that is essential to the achievement of business goals and the safety of the organisation.

1 The Risk Management Association's Web site can be found at <http://www.RMAhq.org>

REFERENCE

Risk Management Association, 2005, "Report on a Survey of KRI Programmes" (Web-based survey conducted with 38 respondents comprising banks with a North American, European or global focus), Summer.

