

Institute of Operational Risk  
Operational Risk Sound Practice Guidance

**Key Risk Indicators**

November 2010

## **The Institute of Operational Risk Sound Practice Guidance**

The Institute of Operational Risk (IOR) recognises that there is no one size fits all approach to the management of operational risk. However by drawing on the experience of practising risk professionals it is possible to identify examples of good practice described in this paper. Equally it is hoped that these guidance papers will facilitate a shared understanding of key operational risk concepts amongst risk management professionals, regulators and academics, thus contributing towards the further development of the discipline of operational risk.

This is one of a series of Sound Practice Guidance papers being produced by the IOR with the following objectives:

- Providing information on the practicalities and know-how necessary in order to implement the techniques that support a robust operational risk management framework;
- Empowering operational risk professionals to demonstrate the value of operational risk management to senior management in a practical rather than theoretical manner;
- Capturing the real experience of practising risk professionals, including the challenges involved in developing operational risk management frameworks.

This paper is available from the Institute's website at [www.ior-institute.org](http://www.ior-institute.org). If you have comments or suggestions on this paper please contact us on [standards@ior-institute.org](mailto:standards@ior-institute.org).

### **The Institute of Operational Risk**

The Institute of Operational Risk was created in January 2004 as a professional body whose aim is to establish and maintain standards of professional competency in the discipline of Operational Risk Management. It is an independent, not for profit, professional body designed to support its members.

The stated mission of the Institute is to promote the development and discipline of Operational Risk and to foster and maintain investigations and research into the best means and methods of developing and applying the discipline and to encourage, increase, disseminate and promote knowledge, education and training and the exchange of information and ideas.

|        |   |    |
|--------|---|----|
| 1.     | Introduction.....   | 1  |
| 2.     | Definitions.....  | 1  |
| 2.1.   | Risk Indicators .....   | 1  |
| 2.2.   | Control Effectiveness Indicators.....                         | 2  |
| 2.3.   | Performance Indicators .....                                  | 2  |
| 2.4.   | Indicators generically.....                                   | 2  |
| 2.5.   | ‘Key’ Indicators .....  | 2  |
| 3.     | Role and Purpose: Using Risk Indicators.....                  | 3  |
| 3.1.   | Indicators and Risk Monitoring .....                          | 3  |
| 3.2.   | Using Indicators to Support Operational Risk Assessments..... | 3  |
| 3.3.   | Indicators, Risk Appetite and Governance.....                 | 4  |
| 3.4.   | Performance Management and Strategic Management.....          | 4  |
| 3.5.   | Regulation and Capital Assessments .....                      | 4  |
| 4.     | Selecting Risk Indicators .....                               | 5  |
| 4.1.   | The Desirable Characteristics of Risk Indicators.....         | 5  |
| 4.1.1. | Relevance .....   | 5  |
| 4.1.2. | Measurable.....   | 6  |
| 4.1.3. | Predictive .....  | 6  |
| 4.1.4. | Easy to Monitor.....  | 7  |
| 4.1.5. | Auditable.....  | 8  |
| 4.1.6. | Comparability .....   | 8  |
| 4.2.   | The Selection Process – Top-Down versus Bottom-Up .....       | 8  |
| 4.3.   | How Many Indicators are Enough? .....                         | 9  |
| 4.4.   | Composite or Index Indicators.....                            | 9  |
| 5.     | Thresholds, Limits and Escalation Triggers.....               | 10 |
| 5.1.   | Thresholds and Limits.....                                    | 10 |
| 5.2.   | Specialised Thresholds.....                                   | 11 |
| 5.3.   | Escalation Triggers .....                                     | 12 |
| 6.     | Managing Risk Indicators .....                                | 12 |
| 6.1.   | Starting Off .....  | 12 |
| 6.2.   | Adding or Changing Indicators.....                            | 12 |
| 6.3.   | Indicator Dimensions and “Buckets” .....                      | 13 |
| 6.4.   | Changing Thresholds and Limits .....                          | 14 |
| 6.5.   | Data Collection and Management.....                           | 14 |
| 6.6.   | Taking Action to Resolve Unacceptable Indicators.....         | 14 |
| 7.     | Reporting.....  | 14 |
| 7.1.   | To Whom? Levels of Reporting.....                             | 14 |

|         |  |    |
|---------|--|----|
| 7.2.    | Frequency of Reporting .....   | 16 |
| 7.3.    | Presenting Risk Indicators .....   | 16 |
| 7.4.    | Prioritising Risk Indicators .....                                       | 17 |
| 7.4.1   | Size.....  | 17 |
| 7.4.2   | Trends .....   | 18 |
| 7.4.3.  | Dependencies between Indicators .....                                    | 18 |
| 8.      | Appendices.....  | 20 |
| 8.1.    | Common Categories of Risk Indicator for All Major Industry Sectors ..... | 20 |
| 8.2.    | Specific Sample Indicators for Financial Institutions .....              | 22 |
| 8.2.1.  | Agency Services.....   | 22 |
| 8.2.2.  | Asset Management .....   | 23 |
| 8.2.3.  | Commercial Banking .....   | 24 |
| 8.2.4.  | Corporate Finance .....  | 24 |
| 8.2.5.  | Payments and Settlements.....  | 25 |
| 8.2.6.  | Retail Banking .....   | 25 |
| 8.2.7.  | Retail Brokerage .....   | 26 |
| 8.2.8.  | Trading and Sales.....   | 27 |
| 8.2.9.  | Corporate Services .....   | 28 |
| 8.2.10. | Insurance .....  | 29 |
| 8.3.    | Example Documentation.....   | 30 |
| 8.4.    | Example Report for Management .....                                      | 33 |
| 8.5.    | Example Report for Board .....   | 35 |
| 8.6.    | Composite Indicators .....   | 36 |
| 8.7.    | Web Resources.....   | 37 |

|                                      |                                       |
|--------------------------------------|---------------------------------------|
| Title: Key Risk Indicators           | Date issued: 2 <sup>nd</sup> Nov 2010 |
|                                      | Version: 1                            |
| File name: IOR KRI Guidance Nov 2010 | Update date: n/a                      |

## 1. Introduction

Risk indicators are an important tool within operational risk management, facilitating the monitoring and control of risk. In so doing they may be used to support a range of operational risk management activities and processes, including: risk identification; risk and control assessments; and the implementation of effective risk appetite, risk management and governance frameworks (see IOR Guidance on Risk Appetite and Risk Governance).

Despite their usefulness relatively little guidance exists on how to use risk indicators in an effective manner. Moreover it is an area that has proven to be particularly challenging for many organisations. Hence there is a need for further guidance in this area.

What follows is the IOR's perspective on current sound practices in relation to the use of risk indicators to support the management of operational risk. In so doing, this guidance covers the role and purpose of risk indicators, the elements of an effective risk indicator framework and some important practical considerations relating to the use of such frameworks within an operational risk management context.

## 2. Definitions

Indicators are metrics used to monitor identified risk exposures over time. Therefore any piece of data that can perform this function may be considered a risk indicator. The indicator becomes 'key' when it tracks an especially important risk exposure (a key risk), or it does so especially well (a key indicator), or ideally both.

More specifically a metric may be considered to be a risk indicator when it can be used to measure:

- The quantum (amount) of exposure to a given risk or set of risks.
- The effectiveness of any controls that have been implemented to reduce or mitigate a given risk exposure.
- How well we are managing our risk exposures (the performance of our risk management framework).

Expressed slightly differently, this implies that an organisation will typically make use of three different types of indicator: *risk* (exposure) indicators, *control effectiveness* indicators and *performance* indicators.

### 2.1. Risk Indicators

In an operational risk context a risk indicator (commonly known as a key risk indicator or KRI) is a metric that provides information on the level of exposure to a given operational risk which the organisation has at a particular point in time. In order to provide such information the risk indicator has to have an explicit relationship to the specific risk whose exposure it represents. For example, take the number of customer complaints, which is likely to be linked to the risk of process errors – 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 changes in the value of this indicator are likely to be associated with changes in operational risk exposure or operational loss experience.

Further examples of risk indicators include staff turnover (which may be linked to risks such as fraud, staff shortages and process errors), the number of data capture errors (process errors) and the number of virus or phishing attacks (IT systems failure). For further examples see Appendices (8.1).

## 2.2. Control Effectiveness Indicators

Control effectiveness indicators, usually referred to as key control indicators or KCIs, are metrics that provide information on the extent to which a given control is meeting its intended objectives (in terms of loss prevention, reduction, etc.). In so doing they can be used to measure the effectiveness of particular operational risk controls at a particular point in time.

In order to provide such information, the control effectiveness indicator has to have an explicit relationship to both the specific control and to the specific risk against which the control has been implemented. Examples of operational risk related control effectiveness indicators include the number of cases of customer identity misrepresentation detected (which may indicate deficiencies in customer information security controls), the number of network user access rights not reviewed within a specific period (indicating weaknesses in user access security controls) or the number of business continuity plans not tested/updated within the specified review period (indicating weaknesses in continuity planning controls).

## 2.3. Performance Indicators

Performance indicators, usually referred to as key performance indicators or KPIs, are metrics that measure performance or the achievement of targets. Although often considered more relevant to finance, accounting and general business management, they are applicable to operational risk both in regard to achieving specific targets set for exposure reduction, minimisation or mitigation and in establishing how well a business entity is doing in managing its operational risks. Examples of performance indicators are cumulative hours of IT system outage, the percentage of products/transactions containing faults/errors or the percentage of automated processes requiring manual intervention.

## 2.4. Indicators generically

While every organisation has its own terminology, the differentiation between risk, control effectiveness and performance indicators is largely conceptual, as a detailed examination of the examples provided previously will soon reflect. The reality is that the same piece of data may indicate different things to different users of that data, implying that the nature of an indicator changes depending on its use. Consider the following example, which illustrates the point:

In a financial services trading and sales operation, transactions are executed by a dealing team, typically an independent confirmation process re-confirms details of the transactions with the counterparty and then a settlements function settles the resultant obligations. If we have a metric that tracks the number of transactions that have not yet been confirmed, it is interesting to note how it changes in nature, depending on who is using the indicator, as illustrated below:

- To the confirmation function, the indicator represents a *control effectiveness* measure (KCI), in that it represents the number of transactions which have failed to be confirmed and thus require further work.
- To the dealing function, it can, at best, only represent a *performance* indicator (KPI), measuring the number of errors caused during the dealing process which are subsequently identified by the confirmation function.
- To the settlement function, it represents a *risk* indicator (KRI), in that unconfirmed transactions which enter the settlements process are more likely to result in settlement failures or default.

This example illustrates the changing nature of a metric, which suggests that the term “indicator”, rather than “risk indicator”, is more generic and as a result is used throughout this paper.

## 2.5. ‘Key’ Indicators

It is not always possible to determine a universal/fixed set of key indicators for any given organisation. This is because as its risk exposures change in their nature or severity so may the importance of particular key risk indicators (e.g. as new risks arise new indicators may need to be

added). The same applies to control effectiveness and performance indicators – as exposures, business cycles, targets and objectives change, so should the set of indicators being monitored change.

Care should also be taken when benchmarking a given set of key indicators against those monitored by other organisations. An organisation's risk exposures arise from its unique mix of business activities, corporate strategy and culture – meaning that few organisations have matching exposure profiles. Accordingly, the set of indicators which measure and monitor that exposure level are likely to be different. Hence the concept of a “one size fits all” set of key indicators set is not logical.

For more on the selection of risk indicators see Section 4.

### **3. Role and Purpose: Using Risk Indicators**

Indicators can be used for a number of purposes, both in the management of operational risk and also in a wider context in the overall management of an organisation. As explained above, the distinction between Risk, Control and Performance Indicators is often only slight and these areas can overlap, both in terms of usage and also terminology. Hence for simplicity this section will use the term risk indicator to mean all three.

#### **3.1. Indicators and Risk Monitoring**

Indicators can be used by organisations as a means of control to track changes in their exposure to operational risk. If selected appropriately indicators can provide a means for identifying:

- Emerging risk trends and issues on the horizon that may need to be addressed (via ‘leading’ indicators);
- Current exposure levels; and
- Events that may have materialised in the past and which could occur again (via ‘lagging’ indicators).

The frequency with which an indicator is measured is an important factor. Generally, the more often an indicator is updated, the more useful the data it represents will be. However there can be occasions where more frequent measurement of the indicator will show only small changes in the risk profile. In such circumstances it is important to consider the longer term trend of measures before arriving at conclusions as to the overall changes in operational risk exposure.

#### **3.2. Using Indicators to Support Operational Risk Assessments**

Indicators can be used to support risk assessments and also provide a way to track an organisation's risk exposures between full updates of its operational risk assessment process. Trends in indicators should provide an indication of whether an organisation's exposure to a particular risk is increasing or decreasing. Indicators that breach pre-assigned thresholds, limits or escalation triggers may signal a significant change in risk that requires prompt action (see Section 5).

Care should be taken when using indicators to support risk assessment activities as they may not always provide a full picture of an organisation's exposure to particular risks. Often a number of indicators may need to be monitored to gain insight into changes in exposure and data may not always be available to measure all the indicators as required. Hence the use of risk indicators should not be seen as a substitute for a proper risk and control assessment programme (see IOR Guidance on Risk and Control Self Assessment).

One potential solution to the problem of data shortages is to identify those areas of exposure deemed to be significant and to then only select indicators relevant to each of those areas. This then allows for the ongoing monitoring of such exposures, leading to a more up-to-date operational risk profile. For more on the selection of indicators see Section 4.

### 3.3. Indicators, Risk Appetite and Governance

A primary benefit of using indicators lies in their ability to link current ‘real time’ exposure levels to risk appetite. By monitoring a set of appropriate risk indicators and by checking their actual values and trends against agreed limits/thresholds (see section 5) an organisation is able to see whether its operational risk exposures remain within its appetite for risk or exceeds it. Hence the monitoring of risk indicators is an important mechanism by which an organisation’s management can gain assurance that it remains within its stated appetite for operational risk. For more on the concept of risk appetite and its use, see the IOR Guidance on Risk Appetite.

The use of risk indicators also supports effective governance by providing a transparent, repeatable and consistent means for tracking both risk exposures and management activity (in the case of control and performance indicators – see Section 2). Once the specifications according to which an indicator’s values are to be calculated are determined, appropriate data sources identified and collection, submission and reporting frequencies agreed, the exact same data can be collected time after time – providing management with a reliable means to keep track of their organisation’s operational risk exposures along with the effectiveness of its risk management and control activities. Escalation triggers for particular indicators may also be agreed; whereby particularly key indicators or those with especially high/low values may be passed up the management chain for appropriate consideration and action once they have breached an agreed level (see Section 5 for more on escalation triggers). For example once staff turnover has breached 20% it might be passed to the Operational Risk Committee for consideration, moving up to Board level if it breaches 25%.

However, when using indicators to support risk appetite monitoring and governance it is worth considering the implications of ‘Goodhart’s Law’ which states that: *any observed statistical regularity will tend to collapse once pressure is placed upon it for control purposes*. Hence, once an indicator is made a target it may lose its relevance, which in the context of risk indicators, could be because management start to focus on managing the indicator rather than any associated risks or governance issues.

### 3.4. Performance Management and Strategic Management

Indicators can be used to support performance and strategic management as measures of how well an organisation is doing towards achieving its overall objectives as well as measuring the performance of those activities and/or processes that are critical to the achievement of its objectives. An example of this would be an organisation that wishes to improve levels of customer satisfaction and therefore may consider monitoring call abandonment rates and call waiting times in its customer contact centre. Another approach is to establish formal targets or budgets for specific indicators, then manage the data towards that figure, for example, the company has staff turnover in the range of 3% to 5% per annum and, for some strategic reason, wants staff turnover to be 2%. While thresholds would apply bands around the 3% to 5% range, a target value set at 2% and then monitored for variance is more effective in driving performance towards strategic objectives.

### 3.5. Regulation and Capital Assessments

The explicit use of risk indicators is generally not mandated in most industry sectors and for most risk types. However, in terms of regulatory sound practices principles, it is generally accepted that every organisation needs a mechanism to measure and monitor its current levels of operational risk exposure.

For those organisations concerned with calculating their regulatory and or economic capital requirements, such as in the financial services sector, risk indicators can be used to support this process. For example risk indicator data can be used to support scenario analysis and stress testing work by highlighting potential areas of weakness. However this is very much an emerging area where there is too little consensus on which to base sound practice guidance at the current time.

For financial institutions which calculate and hold operational risk capital under more advanced approaches, there is also a specific requirement to incorporate what are referred to as “business



environment and internal control factors”(BEICF) into their capital estimation and allocation processes. While the definition of BEICF differs from jurisdiction to jurisdiction, and in many cases is left to the individual organisation, these factors must: (1) be risk sensitive; (2) provide management with information on the risk profile of the organisation; (3) represent meaningful drivers of exposure which can be quantified; and (4) should be used across the entire organisation. While some organisations include the outputs of their risk and control self-assessment programmes under their internal definition of BEICF’s, indicators are the most appropriate mechanism to satisfy these requirements, implying that there is an indirect regulatory requirement to implement and maintain an active indicator programme.

## 4. Selecting Risk Indicators

### 4.1. The Desirable Characteristics of Risk Indicators

Any piece of data could conceivably be viewed as an indicator. However, the use of too much data can be as dangerous for an organisation as too little. Accordingly, it is imperative for the organisation to establish very specific characteristics for what will be adopted as indicators, separating broad data from specific metrics used to indicate changes in exposure levels. The broad characteristics of ‘good’ indicators are outlined in this section.

#### 4.1.1. Relevance

Indicators must have relevance to what is being monitored – risk indicators must monitor risk exposure levels, control effectiveness indicators provide insight into control effectiveness and performance indicators must measure performance. Accordingly, risk indicators should be linked to an organisation’s operational risk exposures and provide management with both a quantum as to current levels of exposure and the degree to which such exposures are changing over time.

In terms of relevance, there are three generic ways to look at indicators: indicators with a specific focus; indicators with general focus; and common or generic indicators.

- Specific focus indicators are highly focussed, typically on a single exposure area – an example would be the Sharpe Ratio, a measure of the risk-adjusted rate of return, defined as the difference between the total return or profit and the risk-free rate of return divided by the standard deviation of the return or profit, for a specific portfolio. This indicator is typically used to identify or monitor possible improper practices around a product or asset trading portfolio, indicating either a more/less risky strategy or an inappropriate mix of products/assets.
- General focus indicators usually cover a specific area of activity and provide a general impression of current exposure levels or activity. An example would be the number of prior period accounting adjustments – if this number increases significantly it indicates both potential workload issues for finance and accounting, as well as issues around the timing of entries being passed through by the business.
- Common or generic indicators can be used virtually anywhere in the business, usually by simply adding some specific context. A good example is customer or client complaints – by itself, it represents a risk measure which most organisations monitor closely (and indeed, a number of regulators demand this metric to be monitored and acted on). However, by adding context such as service levels (of customer facing staff), the metric suddenly becomes more focussed onto a specific business area (and potentially on product/service areas, locations, client types, etc), providing an enhanced perspective on particular exposure areas.

A crucial aspect to bear in mind when considering the relevance of an indicator is that relevance can change over time and can change as new exposures emerge and existing exposures are either mitigated or are no longer of consequence (see Section 2.5). One technique that can be used to check and maintain the relevance of selected indicators is to link updates to the indicator programme with the completion of risk and control self-assessments, drawing on the experience, knowledge and

understanding that business entities/areas have of their operational risk exposures and associated indicators. In this manner it may be useful to think of potential indicators from the following perspectives:

- Does it help identify existing risks?
- Does it help quantify or measure the risk?
- Does it help monitor the exposure?
- Does it help manage the exposure and its consequences?

The roles of different business entities/areas or individuals within the organisation should also be taken into consideration when determining relevance. In many cases, the business entity/area which possesses and can provide data for some specific indicator may have a different perspective on associated operational risk exposures to those business entities which use the data for exposure monitoring purposes – that is, the relevance of the indicator and its data over time should focus on the *information consumer*, not the *data provider*.

#### **4.1.2. Measurable**

Indicators must be capable of being measured with a high level of certainty and on a repeated basis. This implies that indicators should be numbers/counts (number of days, employees, etc.), monetary values, percentages, ratios, time duration or a value from some pre-defined rating set (such as that used by a credit rating agency). Indicators that are described by text are usually very subjective, can easily be misinterpreted and are subject to manipulation through the structure of the text employed. When implementing a new indicator, the measurement technique should be agreed amongst the stakeholders to ensure that everyone agrees what the value represents, how it is calculated, what is included or excluded and how variances in the values will be handled.

Selected indicators should reflect the following characteristics:

- Indicators must be capable of being quantified as an amount, percentage, ratio, number or count;
- Indicators must have values which are reasonably precise and are a definite quantity;
- Indicator values must be comparable over time; and
- Indicators should be reported with primary values and be meaningful without interpretation to some more subjective measure. The primary values can be aggregated to meaningful management information, if required.

#### **4.1.3. Predictive**

As indicated in Section 3.1 indicators can provide a leading, lagging, or current perspective of an organisation's operational risk exposures. Leading in that the indicator's nature reflects an expected change in exposure levels, lagging in that the exposure level has already changed and current, in that the indicator reflects a current change in exposure levels. It is important to bear in mind that the indicator data collection process itself almost invariably implies a historical perspective – by the time the data is collected, quality assured and distributed, time has elapsed and hence the data is “lagging”.

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. However, current and lagging indicators have an important role to play - current indicators provide a snapshot or current view of operational risk exposures and may identify a situation that requires attention to reduce exposure or minimise loss. Lagging indicators can be considered as more ‘detective’ in nature, providing important and useful information regarding the historical causes of loss or exposure. They can also be useful where losses are initially hidden from view, or where changes in historical trends may reflect changes in circumstances that may, in turn, have predictive value.

In reality, many indicators are both lagging and current. Consider the number of unresolved customer complaints – such complaints relate to issues that have already occurred (the lagging aspect), but which still needs to be addressed (the current aspect). Lagging and current indicators can also have a leading element to them that may need to be considered. For example, in the case of unresolved customer complaints an organisation's failure to address these could give rise to a costly lawsuit at some point in the future and or bad publicity, leading to reduced sales.

A misconception about leading indicators is the assumption that establishing or projecting future values from historical trends results in a leading indicator of risk. By itself trending does not produce leading indicators, it simply provides an indication as to where the exposure could be going (assuming everything else stays the same). It is however beneficial to measure indicators over time, in order to detect trends and to provide contextual information.

Truly leading indicators are rare and are usually related to causal drivers within the business environment within which the organisation operates – they tend to be measures of the state of people, process, technology and the market that affects the level of risk in a particular organisation. A leading or preventative indicator 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 particular activities. In themselves, such occurrences may not be loss events in their own right, but if their value starts to increase this may point to the potential for a higher frequency or severity of operational loss events.

In the case of fully predictive indicators, which predict what is going to happen, rather than simply infer that something is changing, single indicators by themselves are of little use, as they need context in order to become predictive. This implies the need for *composite* or *index-based* indicators, as described in section 4.4.

#### **4.1.4. Easy to Monitor**

In terms of ease of monitoring, indicators need to reflect two characteristics:

- The data used for the indicator should be simple and relatively cost effective to collect, quality assure and distribute.
- The data should be relatively easy to interpret, understand and monitor.

With regard to data provision, many organisations have made the fundamental error of developing automated interfaces to a wide range of core systems, with significant cost implications and on the erroneous basis that the identified set of indicators will never change. It is generally better to start with a small set of indicators and collect the data manually. This facilitates a good understanding of where the data is coming from, what it actually is and how it can be used. Once an indicator or set of indicators has proven themselves useful, then consider technology solutions to reduce the manual workload, but in a manner which allows the easy replacement and addition of new indicators.

A crucial aspect relating to the collection process is quality assurance. The collection cycle needs to incorporate specific deadlines for submission and should be auditable in terms of data sources and collection channels. There should also be an independent quality control process to ensure that erroneous or misleading data is not sent to management.

In terms of interpretation and understanding, good indicators are those that quickly convey the required message, without the need for comparison or reference to other information. In this regard, percentages and ratios are typically far more useful than the actual underlying information. Consider the staff turnover percentage or the percentage of customers who have incomplete files – in both examples management does not need to know how many staff or customers the organisation has, they can simply identify the change in values and accordingly the change in exposure by looking at the indicator, perhaps taking its trend over time into account. Unfortunately this also means that the organisation must collect the underlying data to calculate the percentages and ratios.

#### **4.1.5. Auditable**

In the same manner that indicators should be easy to understand and use, they must also be easy to verify. For good governance, an independent validation of the indicator selection process (including the manner in which data is sourced, aggregated and delivered to management) should be undertaken reasonably early in the lifecycle of the organisation's risk indicator programme. The organisation's internal audit function should normally perform such a validation.

Periodically over the lifecycle of any given indicator the appropriate information consumers should also undertake quality assurance checks to satisfy themselves that the date they receive remains accurate and, if relevant, is calculated correctly.

#### **4.1.6. Comparability**

In many cases, even indicators measured as percentages and ratios by themselves do not provide sufficient information to really understand the exposure levels that the indicator relates to. The issue being that a particular percentage or ratio may mean nothing if it cannot be compared to some sort of benchmark.

Using staff turnover as an example, if a business entity/area has staff turnover which over a one year period ranges from 3% to 5% on an annualised basis, is that acceptable? To help determine acceptability it is often necessary to compare or 'benchmark' the data against peers, either within the organisation itself or perhaps against peers within the same industry. In this manner current staff turnover levels can be put into a proper context, helping management to decide if any corrective or mitigating action is required.

An organisation's indicator identification and selection process should therefore specifically assess the level of comparability, both within the organisation and more broadly across the industry which the indicator reflects.

### **4.2. The Selection Process – Top-Down versus Bottom-Up**

There are two main approaches that organisations can use to select the indicators they wish to monitor: top-down or bottom-up. The top-down approach starts with senior management and/or directors who select the indicators that are to be monitored across the business, while the bottom-up approach allows business entity/area level managers to select and monitor their own sets of indicators. In both cases, the aim is to cover the most significant information requirements that each level of the organisation requires in order to achieve their strategic objectives.

Neither approach is automatically better than the other. A top-down approach can facilitate aggregation and senior management understanding, while a bottom-up approach ensures that business entity managers can select and monitor those indicators that are most relevant to their particular situation. In practice, many organisations employ a combination of the two and this is generally considered to be the best approach.

The selection process for top-down indicators could be conducted vertically (by business line) or horizontally (by department) depending on the organisation structure of the company. Top-down indicators should meet the following criteria:

- Reflect the operational risk profile of the division, business line, country or region or of the overall organisation, depending upon the level at which selected;
- Must facilitate aggregation across relevant business entities, product or service areas, countries or business lines, resulting in a meaningful and understandable metric at the relevant level of management;
- Should apply to all parts of the organisation structure below the level where they are being applied; and
- Are usually imposed by management and must be reported on, without choice.

Typically, the selection process for bottom-up indicators should take into account:

- The results of Risk Control Self Assessments (RCSA), ensuring that indicators are identified to facilitate the ongoing monitoring of identified risks and controls;
- The results of any regulatory examinations or audit findings to help facilitate the rectification of any control or monitoring deficiencies that may have been identified;
- Identified during the new product review process (mainly short term) to monitor and manage the operational risk during the implementation phase;
- The views of the appropriate risk owners (e.g. the relevant department managers or business line managers) or that of the local Operational Risk Manager, both during and between RCSA exercises;
- Any insights that may have been provided by recent loss events (for example in terms of the identification of significant new indicators); and
- Changes in the economic environment, which might mean that certain indicators become more important (e.g. indicators of fraud risk may become more important in a recession, etc.).

Note that due to local regulatory requirements, it is reasonably common for certain top-down indicators to be measured and reported on under a number of different calculation structures, for example, the definition of a full-time employee often differs between operating jurisdictions. In such a case, the local business entity may need to calculate and report locally on staff turnover and then re-calculate and report on staff turnover to “Group” using different criteria.

### 4.3. How Many Indicators are Enough?

There is no right or wrong answer for how many indicators should be set. Too few may not deliver a clear picture and too many may present an overly confusing picture. The following should be considered when deciding the number of indicators to be set:

- Number and nature of the key risks identified;
- Availability of the data necessary for the key indicators;
- The cost needed to extract the data for the key indicators; and
- The intended audience (local management, executive, board, etc.).

In terms of the last point concerning the intended audience it is usually appropriate to collect a more detailed set of metrics for the local management of a specific business area/entity than for executive management or the board. This is because local management will probably require a detailed set of indicators in order to help them monitor and control the day to day activities of their area/entity effectively, while executive management/boards, whose time is limited, should normally only focus on the most relevant metrics that relate to the most significant risks that may be threatening their organisation at the current time.

### 4.4. Composite or Index Indicators

*Please note: this section requires modelling skills and is for advanced users of key risk indicators. As a result you may wish to skip this section.*

As stated previously, two major fallacies relating to indicators are the so-called “Top 10” and the existence of “predictive” indicators. There is no common set of indicators which every organisation should monitor and report to its executive management, for the reasons provided previously. Equally, while trending indicator values over time may give an impression of where these values will go, assuming nothing changes, they certainly do not *predict* exactly what is going to happen and when it will do so.

However, existing research and experimentation underway within various industry segments indicates that the use of indicator “indices” or synthetic indicators created out of a composite set of underlying metrics may provide a more realistic mechanism for trying to predict future exposure levels (e.g.

customer or employee satisfaction indices that draw on metrics such as complaints, surveys, compensation claims, etc.). Although the initial work implies that such composite or index indicators may be capable of representing the overall level of exposure for a general area of risk (e.g. human resource risks) there is reasonable optimism that in time, with larger more comprehensive data sets to analyse, more predictive and focussed composite or index indicators may be possible.

An important requirement in developing composite indicators lies in understanding both the causal drivers of the exposure and the underlying relationships with specific data sets – so as to determine appropriate groupings of related indicators. Various statistical techniques can be used to achieve this, such as: factor analysis; linear or hyperbolic transformation techniques (with or without the use of T-values); weighted base indices; etc. Essentially to develop a composite indicator you need to identify all the contributing factors, establish the relationships between them, determine the base case or equilibrium level, then monitor deviation in the composite from the base case. For more on this emerging area see Appendix 8.5.

## **5. Thresholds, Limits and Escalation Triggers**

Implementing a set of indicators without any guidelines on how to interpret the data and what actions are required will not deliver much benefit to the organisation. The organisation needs to establish, for each relevant indicator being monitored, a set of threshold values or limits where, if the indicator's value breaches the threshold or limit, the organisation knows it needs to take action. Equally the establishment of thresholds and limits for specific indicators is an important part of an effective operational risk appetite framework.

However, the establishment of thresholds and limits in isolation of an informed understanding of the indicator and its values over at least a minimum period of time is equally likely to deliver little value and be little more than an academic exercise. It is strongly advocated that the organisation implement its indicator set, collect data for 6 months at the very least, but preferably 1 year, then assess the data and its trends over that time to establish the initial thresholds and limits. If possible, draw upon any publicly available information or benchmarks to assist in establishing the starting points for an organisation's thresholds and limits.

### **5.1. Thresholds and Limits**

The concept of a threshold or limit is to establish boundaries that, when exceeded, alert the organisation to a potentially significant change in risk exposure. As with any form of risk, limit indicators should have a set of thresholds or limits with an escalation structure attached to each threshold level. For example, assume that the level of open customer complaints is historically in a range between 50 and 100 per month, the organisation could establish the following threshold structure:

- At 100, local management threshold – implying that the local management of the unit(s) responsible for managing the open complaints log is informed and needs to take action.
- At 120, further local management threshold, accompanied by a divisional threshold – implying that the local management of the unit(s) responsible for managing the open complaints log is informed and needs to take action and that the direct divisional management above that unit is also informed (so that they can monitor the situation and take action where necessary).
- At 150, general alert threshold - local management of the unit(s) responsible for managing the open complaints log is informed and needs to take action, divisional management is informed and general management is informed (again so that they can monitor the situation and take action where necessary).

The key is to have the intervals between thresholds broad enough to allow the responsible individual or business entity/area to act before escalation kicks in, but narrow enough to ensure that critical issues are not addressed within an appropriate time frame.

Thresholds may take several different forms, including (1) a *cap* or upper boundary, where as soon as the indicator value exceeds the threshold value, the escalation process kicks in; (2) a *floor* or lower boundary, where as long as the indicator value is above the threshold value, nothing happens, but when it drops below that level, the escalation process starts; and (3) a *collar* or combination of a cap and floor/upper and lower boundary, where essentially the indicator values are expected to remain within the pre-defined range. In addition a more sophisticated indicator monitoring programme could include a variety of threshold types, including: percentage based; absolute number or value; deviations from a predefined value; etc.

It should be expected that over a period of time, as the organisation becomes more risk aware and the benefits of proactive risk management deliver value, indicator thresholds should be tightened. This implies that the organisation should periodically review not just the indicators it is using, but the thresholds applied to those indicators. However, if the thresholds are too narrow, they will result in false alerts and then over time, people ignoring the alerts altogether. Too broad, on the other hand, and the organisation learns too late that a major issue has suddenly emerged, with potentially significant adverse consequences.

To establish the initial threshold values decide first on whether a cap, floor or collar is required, then establish whether the threshold is an absolute number or value, a percentage, ratio or other derived value or some form of deviation or variance. Next, review historical data for the indicator in question and establish its ranges over time. Assess existing budgets or targets, relevant public information and the organisation's risk appetite and apply this information to the historical ranges. Next, evaluate where the first level of slight discomfort with the data range lies, then use this as the basis for establishing your first threshold. Monitor the next few data submissions against the threshold and adjust if necessary.

## 5.2. Specialised Thresholds

The thresholds described above are the primary monitoring system for indicators. These can however be augmented and strengthened by various forms of specialised thresholds, although it is suggested to start with a simple structure and only add more complicated structures once the primary monitoring mechanism is in place. Some examples of specialised thresholds include:

- Target or budget values – in addition to the boundary thresholds, these thresholds focus management's attention on where you want the indicator values to be, with target variance being monitored, rather than boundary exceptions. Returning to the open customer complaints indicator, we may set a target of striving not to have more than 30 open complaints at any time. The first boundary is set at 100, so a submission reflecting 60 open complaints does not alert anyone, but reflects a negative target variance of -30.
- Trend thresholds, where the movement of data submissions over a series of data collection periods can be a very useful early warning system, for example, if the number of open complaints reflects 50 in period 1, 60 in period 2, 70 in period 3 and 80 in period 4 there could be good reason for management alerts to be generated rather than waiting for the first level of 100 to be reached. Equally downward trends, cyclical trends and flat trends can all deliver useful advance warning.
- Repetitive threshold usage without threshold exception is another useful management tool, being aimed at managers who allow issues to grow until they are almost breaching the threshold, then taking action to manage the issue back within boundaries. An example here would be a threshold focussing on more than 4 data submissions within a 1 year time horizon which come within 10% of another existing boundary threshold.

The need for specialised thresholds is closely linked to an organisation's culture and the degree to which individuals are open about exposure levels. The more ingrained the level of risk awareness and disclosure, the less specialised thresholds are likely to be required to detect adverse situations.

### 5.3. Escalation Triggers

Having set one or more thresholds, the next step is to determine the response required when a threshold has been breached. This is commonly referred to as a trigger condition, which determines what action is to be taken and by whom. Where an organisation has implemented an escalating series of thresholds, it is likely that each threshold will result in some form of triggered notification to increasingly senior levels of management.

In the same manner as different boundary thresholds can be applied to different indicators, different trigger conditions can be established. The most basic is a “touch” trigger, where as soon as the boundary is reached, the trigger is initiated and alerts generated as appropriate. Other trigger conditions include “repetitive touch” where when the boundary is first reached nothing happens but if in the next data submission period the boundary is still in breach, then the alert is triggered. Triggers should be linked to risk appetite, to the degree of sophistication required in the warning system and must take into account the resource overhead (people, systems and cost) necessary to implement more sophisticated structures.

## 6. Managing Risk Indicators

### 6.1. Starting Off

The selection of risk indicators should normally follow a risk and control assessment so that there is auditable evidence on the selection process and the linkage between the assessed operational risk exposures and the metrics chosen to gauge the changing levels of these exposures.

Any risk indicator programme should be supported with proper procedures documenting:

- Appropriate governance arrangements (e.g. roles and responsibilities);
- The documentation that should be maintained on selected indicators (data requirements, data owners, etc.);
- Selection procedures (e.g. how, when and who can select indicators); and
- The on-going maintenance of selected indicators (in terms of changes to data sources, refinements to calculation formulae, etc.).

Where the organisation does not employ (or is yet to undergo) a detailed risk control assessment process, the selection of indicators can be based on expert judgement (i.e. on those areas of exposure where experienced business professionals and management agree the organisation faces specific risks). Care must however be taken to avoid selecting a set of indicators that have little or no relevance, as these will not deliver any value to either the business or management and the risk indicator programme will rapidly fall into disuse.

### 6.2. Adding or Changing Indicators

From a governance perspective it is recommended that the process to add, change or remove specific indicators is evidenced by proper documentation, including who needs to do what with regard to existing data, the collection of new data and changes to reports.

The procedure for making changes to the indicator set being employed should address, amongst others, the following issues:

- The frequency with which risk indicators should be reviewed;
- Who has the authority to approve the addition, change or removal of particular risk indicators, bearing in mind that different individuals may be responsible for different areas of risk;
- Whether changes can be made on a top down and/or bottom up basis;
- When removing a previously monitored indicator, what will happen to the data that has been



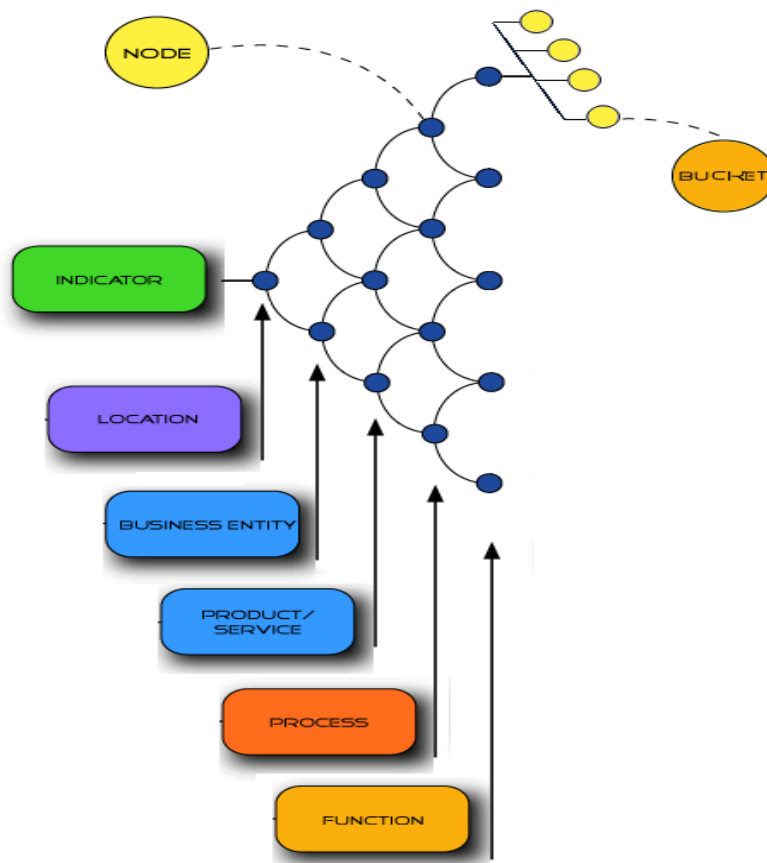
- collected (will it be retained or deleted?);
- When replacing an existing indicator with another, similar indicator, whether past data should be recalculated or amended and applied to the new indicator;
- The introduction of indicators relating to new product or new business activities. Including how long such indicators should be monitored for post implementation; and
- The introduction of indicators following recommendations by department manager(s), regulators and/or auditors (both internal and external).

### 6.3. Indicator Dimensions and “Buckets”

The indicator data collected by an organisation should usually be sub-divided into some form of sub-grouping, such as: customer type; transaction type; location; product type; etc. For example, if the indicator measures open customer complaints the organisation may wish to monitor the following dimensions: by business entity/area and within business entities/areas; by customer type and within customer type; and by complaint type. The data should be collected at the lowest level of detail and then aggregated up the structure to each level of ‘parent node’ (see diagram below).

For certain indicators, it is helpful to divide the indicator’s values into ‘buckets’ – relating to time, value, criticality/priority or some other data-specific perspective. Typically, these ‘buckets’ exist at the end of the dimensional nodes, so in the open customer complaints indicator described above, at complaint type, we may measure the number of open complaints according to how long the complaint has been open, for example, less than 7 days, 7 to 14 days, 14 to 21 days, 21 to 31 days and greater than 31 days. The sum of the values across all the buckets equals the value of the dimensional node for any specific complaint type.

Dimension nodes and buckets can be illustrated using the following diagram:



#### **6.4. Changing Thresholds and Limits**

Changes to thresholds and limits are quite a common occurrence. Changes can be particularly common for new indicators where relatively little data is available initially (see Section 5). However despite this a clearly defined procedure and governance process is required for setting and changing limit/threshold levels, addressing many of the same issues identified in Section 6.2 above (e.g. who can propose and sign off changes).

#### **6.5. Data Collection and Management**

As part of the selection and specification process, the frequency of data measurement and the frequency of data reporting should be decided upon. In many cases data will be collected far more frequently than it will be reported, especially with top-down imposed indicators. As an example the business may track the number of transactional operational errors on a daily basis, but report a monthly total to management. In this case the measurement frequency is daily and the reporting frequency is monthly. Using the reporting frequency the set of expected data submissions for each reporting cycle should be established, with the following information included:

- Source of information for each indicators;
- Responsible person (and department) providing the data;
- Frequency of data measurement; and
- Scheduling, lead times and cut-off times.

As far as possible existing management information should be used, as this reduces overhead and is cost effective. While it is possible and even desirable, in the case of a recently implemented risk indicator framework, to manually build and monitor indicators, sound practice would indicate that, where possible, the data measurement process and build extraction routines of a fully mature framework should be automated to obtain data directly from source systems, as this reduces dependency on people and minimises the potential for errors. If automation is not practical or possible other options include the use of spreadsheets (including macros and pivot tables for data compilation and manipulation) or manual data collection procedures. All forms of data collection should be evidenced by audit trails.

In some cases, the frequency of reporting is also dependent on the frequency of the exposure being monitored. For example, while the risk of regulatory sanction or fine may be potentially high, if there are no frequently reported incidents the reporting frequency could be set to a quarterly basis.

When reporting indicator values, data providers should be required to provide commentary on any unusual aspects of the data and to establish corrective action plans where thresholds are exceeded or targets are not being achieved.

#### **6.6. Taking Action to Resolve Unacceptable Indicators**

Where a data submission for a given indicator results in a threshold being exceeded or a target variance to occur it would be appropriate for specific action plans to be established to rectify the situation. Action plans should always have a specific owner, be allocated to a specific individual to execute and have a definitive target completion date. These action plans should then be managed on an ongoing basis to ensure the appropriate corrective action is implemented on a timely basis.

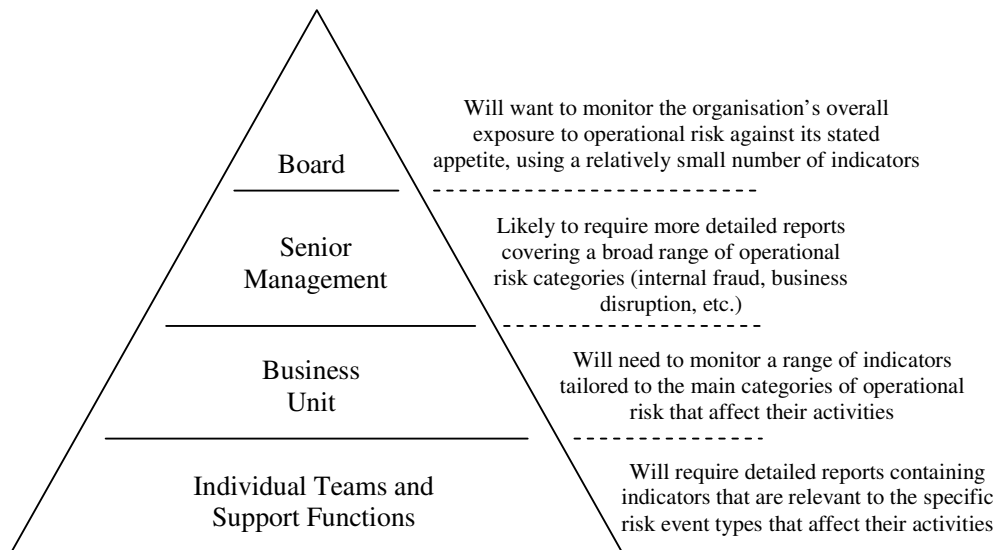
### **7. Reporting**

#### **7.1. To Whom? Levels of Reporting**

An effective monitoring process is essential for managing operational risk. It can assist in the early detection and correction of emerging operational risk issues. It can also serve as a basis for assessing operational risk and related mitigation strategies and creating incentives to improve operational risk management throughout the institution.

Hence risk, control and performance indicators are of little use if they are not reported to an organisation's decision makers. Operational risk indicator reports may be produced at all levels of decision making from board level to the managers of individual business lines and functions.

The following diagram illustrates the main levels of operational risk reporting that most organisations may wish to consider:



The scope, content and presentation of a report will depend on the requirements of the intended audience and where possible reports should be developed in conjunction with them. However central co-ordination can help to ensure that a consistent view of information is delivered so that reports can be compared across business lines and functions and or aggregated for senior management. In larger organisations documented procedures for indicator reporting may also be necessary to ensure consistency.

Some features of a sound indicator report/reporting process include:

- **Relevance** – as indicated in Section 4.1.1 indicators must be relevant. Care must be taken to avoid producing overly detailed reports with large numbers of indicators;
- **Simplicity** – reports should not be overly complex and contain jargon terms, large tables of data or complex mathematical formulae. Where possible the simplest possible graphs and charts should be used (see also 7.3 below);
- **Timeliness** – reports should be produced in a timely manner so that they can be acted upon whilst the data they contain is still relevant;
- **Accuracy** – inaccurate metrics will provide a false picture of an organisations exposure to operational risk and may mean that it ends up over-exposed or investments too much reducing certain risks. Processes should be in place to check the accuracy of reported metrics on an ongoing basis;
- **Trending** – reports should make clear the historical trends of the chosen indicators to provide some indication of their volatility and or where they may be heading;

- Clear escalation procedures – so that the recipients of a report know when to escalate areas of concern to more senior management; and
- Compliance – with any regulations that may exist, where appropriate.

## 7.2. Frequency of Reporting

There is no right answer to the frequency of reporting. It will depend on the nature of the risks, indicators and environment. Reporting should be linked to the timeliness of decision making and action formulation and reports of different frequency will be required to suit specific audiences.

The table below outlines some of the more common frequencies that can be used for indicator reporting.

| Interval  | Benefits   | Suitable to   | usual audience  | Drawbacks   |
|-----------|--|---|---|---|
| Daily     | Allow instant indication of risk issues on day-to-day business                               | Volume, control breaks, fails etc for routine business activities                   | Line Management, Business Management  | Lack of in-depth analysis   |
| Weekly    | Good for tracking the status of the common issues in a short period of time                  | Volume, control breaks, fails etc for routine business activities                   | Line Management, Business Management  | Have to assess whether it contains the events happening during the week or just at a snapshot |
| Monthly   | Align with other monthly MIS reporting and regarded as a good timing to meet with Management | Including the above but also include other non transaction related activities       | Line Management, Business Management, Corporate Management                  | Lack of sense of urgency  |
| Quarterly | Align with announcement of quarterly results and prepare for committee meetings              | Can also consider specific KRI to meet the regulatory requirement                   | Line Management, Business Management, Corporate Management, Audit Committee | Too high level to review granularities, lack of sense of urgency                              |
| Yearly    | Align with year end financial results  | Those KRI mainly for presenting the high level operational risk profile of the Firm | Line Management, Business Management, Corporate Management, Executive Board | Too high level to review granularities, lack of sense of urgency                              |

## 7.3. Presenting Risk Indicators

An indicator report should be presented in a user friendly manner with appropriate visual aids and use clear and simple language. The presentation can be in the form of:

- Country or regional view reports;
- Organisation wide reports;
- Business specific reports; and
- Special theme reports (i.e. focus on a specific control topic e.g. fraud, information security, etc).

In general, reporting should be exception based, typically focusing on those indicators that:

- Have breached agreed thresholds/limits;
- Trending in an adverse way and are expected to breach agreed thresholds/limits; and/or
- Have remained within agreed limits for an extended period of time (suggesting that limits/thresholds may not be sensitive enough).

For more on the prioritisation of indicators see Section 7.4 below.

Judgement on the part of the Operational Risk Manager on what to include or exclude from a report may also be necessary to help information consumers reach the right conclusions. However, information consumers and auditors should be able to access data on all available indicators, on request, so that they can satisfy themselves that the most appropriate indicators have been presented. The provision of suitably detailed narrative to support the figures is critical to ensure that information consumers are able to interpret the reports that they receive and use them to support decision making. In particular, brief and relevant commentary should be provided to explain abnormal items and data trends.

To maximise clarity it is recommended that a dash board type of indicator report should be used, providing a mixture of line and bar graphs (to show trends), charts (e.g. pie charts) and data tables for illustration. Temperature and speedometer style gauges along with coloured trend arrows can also be used as a simple way of showing whether an indicator, or group of indicators, are within their red, amber or green zones. For some examples of dashboard style reports see Sections 8.3 and 8.4 below.

#### **7.4. Prioritising Risk Indicators**

The prioritisation of risk indicators helps information consumers to focus on those indicators, and their associated operational risks, that are most significant for their organisation. Prioritisation can be automated to an extent, for example via the use of thresholds and limits however judgement on the part of the operational risk manager (or whoever puts together risk indicator reports) is often also required.

While judgement may be required, care should be taken when exercising it. Organisations should consider agreeing some general criteria for the prioritisation of risk indicators, bearing in mind that the level of prioritisation may differ depending on the level at which indicators are being reviewed within an organisation. For example, in the case of larger diversified organisations the level of significance given to a particular indicator may be greater at the business entity level than at the overall organisational level. Hence different levels of management may need to agree different criteria for the prioritisation of particular indicators and their associated risks.

Outlined below are some of the main factors that are likely to affect the priority given to particular indicators.

##### **7.4.1 Size**

The absolute or relative size of an indicator is likely to be a major factor in determining its significance. The setting of limits and thresholds has a fundamental role to play in this (see Section 5). In particular limits and thresholds may be set to help show whether an indicator is 'red', 'amber' or 'green'. Indicators that are within their amber zone should normally be given greater priority than those that are green, with even greater priority being given to red indicators. The table below illustrates the normal significance and response criteria that are assigned to red, amber or green indicators. Note that for indicators that are assigned a single limit (indicating zero tolerance for values above or below this limit) there may be a case to present such indicators as being either red or green.

|              |   |
|--------------|---|
| <b>Red</b>   | <ul style="list-style-type: none"> <li>■ The value of this indicator is far too high/low suggesting that the organisation may be exposed to significant risk.</li> <li>■ Immediate action is required on the part of management to manage the risk(s) in question.</li> </ul>   |
| <b>Amber</b> | <ul style="list-style-type: none"> <li>■ The value of this indicator is higher/lower than normal suggesting that the organisation may be exposed to an elevated and potentially significant level of risk.</li> <li>■ Management attention is required to determine whether action needs to be taken in the near future.</li> </ul> |
| <b>Green</b> | <ul style="list-style-type: none"> <li>■ The value of the indicator is within normal parameters, suggesting that the organisation is not exposed to significant risk.</li> <li>■ No action is required – the indicator and its associated risks are under adequate control.</li> </ul>  |

### 7.4.2 Trends

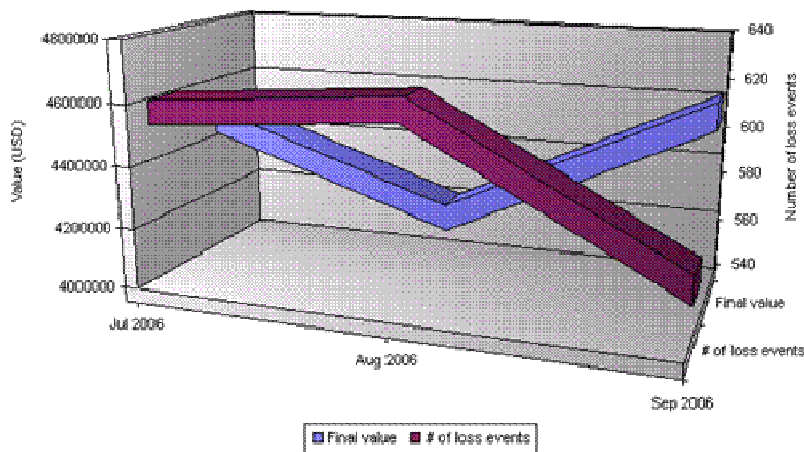
By monitoring trends in the value of operational risk indicators organisations can determine whether they are likely to breach agreed limits/thresholds in the near future, The monitoring of trends thus allows an organisation to become more pro-active in its risk management, for example by taking action to avoid the breach of assigned limits/thresholds, rather than simply reacting to identified breaches. Trends over time also provide a useful measure of whether specific risks are increasing or decreasing and can be used to warn management of inefficient or absent controls or stress in the business environment.

Hence even though an indicator may be within its green range it may be appropriate to prioritise it where its trend suggests that the associated level of risk is increasing.

### 7.4.3. Dependencies between Indicators

It is often very useful to depict indicator data in pairs or groups, in order to gain a more complete perspective on specific risk exposures. Consider the following diagram:

**Aggregated value and number of loss events for Jul 2006 to Sep 2006 in (USD)**



Here, two indicators have been plotted against each other – the first reflects the number of loss events and the second the value of the same loss events. What is now immediately apparent is that in the second measurement period, the number peaked then started to drop, while the value was at its lowest and then started to rise. Examining these two indicators independently would not necessarily provide the same overall picture of the organisation's exposure.

Similar approaches can be used to compare percentages or ratios with the underlying actual values on which they are based, error rates against transactional volumes, etc.

## **8. Appendices**

### **8.1. Common Categories of Risk Indicator for All Major Industry Sectors**

Outlined below is a table that indicates the main areas of operational risk that are relevant for each industry sector along with the types of indicators that are applicable. This could be used as a starting point for determining an initial set of risk indicators.



Key Risk Indicators

Institute of Operational Risk – Sound Practice Guidance

| Industry sector                   | Common operational risk events  | Basel II risk events                |                                     |                |                |                                       |                           |   |                      | Type of applicable KRI |                    |                  |                  |                 |                      |                 |                                   |                 |                            |
|-----------------------------------|---|-------------------------------------|-------------------------------------|----------------|----------------|---------------------------------------|---------------------------|---|----------------------|------------------------|--------------------|------------------|------------------|-----------------|----------------------|-----------------|-----------------------------------|-----------------|----------------------------|
|                                   |   | Clients Products Business Practices | Execution, Delivery & Process Mgmt. | External Fraud | Internal Fraud | Business Disruption & System Failures | Damage to Physical Assets | Employment Practices & Workplace Safety | Legal and Regulatory | Processing error       | System performance | Customer service | Staff monitoring | Quality control | Information Security | Litigation      | Governance and management control | Incident driven | External threat monitoring |
| Agriculture                       | (a) Extreme weather<br>(b) Pollution<br>(c) Quality scandal                         | High                                | High                                | Medium         | Medium         | High                                  | High                      | Medium                                  | Medium               | Very applicable        | Applicable         | Applicable       | Applicable       | Very applicable | Less applicable      | Applicable      | Applicable                        | Very applicable | Very applicable            |
| Aviation and Transportation       | (a) Extreme weather<br>(b) Industry accident<br>(c) Labour strike                   | High                                | High                                | Medium         | Medium         | High                                  | High                      | High                                    | High                 | Very applicable        | Very applicable    | Very applicable  | Very applicable  | Very applicable | Applicable           | Applicable      | Very applicable                   | Very applicable | Very applicable            |
| Biotech, Nanotech, Life Science   | (a) Laboratory accident<br>(b) Intellectual right dispute                           | High                                | High                                | Medium         | Medium         | Medium                                | High                      | Medium                                  | High                 | Very applicable        | Very applicable    | Applicable       | Applicable       | Very applicable | Very applicable      | Very applicable | Applicable                        | Very applicable | Applicable                 |
| Construction and Infrastructure   | (a) Industry accident<br>(b) Natural disruption                                     | Medium                              | High                                | Medium         | Medium         | High                                  | High                      | High                                    | High                 | Very applicable        | Applicable         | Applicable       | Very applicable  | Very applicable | Applicable           | Applicable      | Applicable                        | Very applicable | Very applicable            |
| Consumer                          | (a) Product design fault<br>(b) Labour strike                                       | High                                | High                                | Medium         | Medium         | High                                  | Medium                    | Medium                                  | High                 | Very applicable        | Applicable         | Very applicable  | Very applicable  | Very applicable | Applicable           | Applicable      | Applicable                        | Applicable      | Applicable                 |
| Defence/Security                  | (a) Industry accident<br>(b) Leakage of sensitive know-how                          | Medium                              | High                                | Medium         | Medium         | High                                  | High                      | Medium                                  | High                 | Very applicable        | Very applicable    | Applicable       | Applicable       | Very applicable | Very applicable      | Applicable      | Very applicable                   | Very applicable | Very applicable            |
| Energy                            | (a) Industry accident<br>(b) Political interference<br>(c) New substitute           | Medium                              | High                                | Medium         | Medium         | High                                  | High                      | High                                    | High                 | Very applicable        | Applicable         | Applicable       | Applicable       | Very applicable | Applicable           | Applicable      | Applicable                        | Very applicable | Very applicable            |
| Financial Services                | (a) Burden of regulation<br>(b) System failure<br>(c) Inappropriate risk management | High                                | High                                | High           | High           | High                                  | Medium                    | High                                    | High                 | Very applicable        | Very applicable    | Very applicable  | Very applicable  | Very applicable | Very applicable      | Very applicable | Very applicable                   | Applicable      | Applicable                 |
| Food & Beverage                   | (a) Quality scandal<br>(b) Pollution  | High                                | High                                | Medium         | Medium         | High                                  | High                      | Medium                                  | Medium               | Very applicable        | Applicable         | Applicable       | Applicable       | Very applicable | Applicable           | Very applicable | Applicable                        | Applicable      | Applicable                 |
| Heavy Industry                    | (a) Industry accident<br>(b) Labour strike  | Medium                              | High                                | Medium         | Medium         | Medium                                | High                      | High                                    | Medium               | Very applicable        | Applicable         | Applicable       | Very applicable  | Very applicable | Applicable           | Applicable      | Very applicable                   | Very applicable | Very applicable            |
| Hospital and Health Care          | (a) Industry accident<br>(b) Labour strike  | High                                | High                                | Medium         | Medium         | High                                  | High                      | High                                    | High                 | Very applicable        | Applicable         | Very applicable  | Very applicable  | Very applicable | Applicable           | Very applicable | Very applicable                   | Very applicable | Very applicable            |
| Housing                           | (a) Price bubbles<br>(b) Industry accident  | High                                | High                                | Medium         | Medium         | High                                  | High                      | High                                    | Medium               | Very applicable        | Applicable         | Applicable       | Applicable       | Very applicable | Applicable           | Very applicable | Applicable                        | Very applicable | Very applicable            |
| Manufacturing                     | (a) Labour strike<br>(b) Product design fault                                       | High                                | High                                | Medium         | Medium         | High                                  | High                      | High                                    | Medium               | Very applicable        | Applicable         | Applicable       | Applicable       | Very applicable | Very applicable      | Applicable      | Applicable                        | Applicable      | Applicable                 |
| Public Utilities                  | (a) Industry accident<br>(b) Labour strike  | Medium                              | High                                | Medium         | Medium         | High                                  | High                      | Medium                                  | High                 | Very applicable        | Very applicable    | Applicable       | Very applicable  | Very applicable | Applicable           | Applicable      | Very applicable                   | Very applicable | Very applicable            |
| Technology, Media and Telecommuni | (a) Technology obsolete<br>(b) Leakage of sensitive know-how                        | High                                | High                                | Medium         | Medium         | High                                  | High                      | Medium                                  | High                 | Applicable             | Very applicable    | Applicable       | Applicable       | Applicable      | Very applicable      | Very applicable | Very applicable                   | Applicable      | Applicable                 |
| Tourism                           | (a) Terrorism<br>(b) Pandemics<br>(c) Political unrest                              | High                                | High                                | High           | High           | High                                  | Medium                    | Medium                                  | Medium               | Applicable             | Less applicable    | Very applicable  | Applicable       | Applicable      | Applicable           | Applicable      | Very applicable                   | Very applicable | Very applicable            |

## 8.2. Specific Sample Indicators for Financial Institutions

The following sets of indicators per business area are provided for consideration.

### 8.2.1. Agency Services

| Name  | Nature           | Description  |
|---|------------------|--|
| Corporate Actions - Number of Corporate Action Mandates under Management                                  | Leading, Current | The total number of approved corporate action mandates under management at the point of measurement.   |
| Corporate Actions - Number of Voluntary Corporate Action Letters of Instruction or Direction not Executed | Leading, Current | The number of letters of instruction or direction received from non-discretionary voluntary mandate owners in response to our request for instruction regarding a set of corporate action events which are scheduled to occur within the foreseeable future, which currently have not yet been executed. |
| Custody - Frequency of Inventory Checks   | Current          | The average number of safe custody and safe deposit box inventory checks per month during the preceding 12 calendar months.  |
| Custody - Number of Securities Received but not yet Registered in Customer's Name                         | Current          | The number of non-bearer securities received into safe custody by the organisation on behalf of customers or clients during the preceding 14 business days and not yet registered in the customer's name as beneficial owner.  |
| Custody and Actions - Ratio of Errors to Manual Transactions  | Current, Lagging | The total number of errors detected during the preceding 3 calendar months, divided the number of manual custody and corporate action transactions processed.  |
| Customer Mandates - Number of Breaches Not Disclosed to Customers within Threshold                        | Current, Lagging | The total number of detected breaches of customer mandates by the organisation, its employees, agents or representatives not yet disclosed to the relevant customer or client and beyond disclosure threshold.   |
| Fee and Charge Reversals - Number   | Current, Lagging | The total number of fee or charge reversals booked during the preceding 3 calendar months across all entities within the organisation.   |
| Payment and Settlement Disputes - Number Open with Customers and Counterparties                           | All              | The total number of open payment and settlement disputes with customers, clients and counterparties at the point of measurement.   |
| Transaction Maintenance - Number of Maintenance Events Missed   | All              | The total number of transaction maintenance events during the preceding 6 calendar months that were not completed by the scheduled completion date.  |

### 8.2.2. Asset Management

| Name  | Nature           | Description  |
|---|------------------|--|
| Accredited Advisory Staff - Number with Out of Date Accreditation   | All              | The number of accredited advisors representing or acting on behalf of the organisation whose advisory license or accreditation is out of date at the point of measurement.   |
| Best Execution - Number of Best Execution Exceptions  | Leading          | The number of transactions not executed at the best price or terms available, or not following best practices intended to ensure they are, which were identified during the preceding 3 calendar months.   |
| Customer and Client Product Usage - Percentage of Product Suitability Approvals Outstanding                       | Leading, Current | The total number of currently outstanding customer and client product suitability approvals for products already offered to customers and clients, as a percentage of the total number of customer and client relationships.                                       |
| Dealers, Traders and Investment Managers - Number of License Exceptions   | Current          | The number of transactions executed by approved dealers, traders and investment managers during the preceding 12 calendar months that did not comply with restrictions imposed by their trading licenses or where the individual lacked a current trading license. |
| Front-Running - Number of Instances Detected  | Lagging          | The total number of instances of front-running detected by the organisation during the preceding 3 calendar months.  |
| Investment Guidelines - Number of Guideline Breaches Detected   | Current, Lagging | The number of breaches of investment guidelines detected by the organisation during the preceding 12 calendar months.  |
| Investment Guidelines - Number of Portfolios without Guidelines   | Leading, Current | The number of investment portfolios currently under the management of the organisation for which no formal investment guidelines have been agreed with the customer.   |
| Investment Management - Concentration Growth of Investments in New or High Risk Investments, Vehicles or Products | All              | The growth by value in the composition of the value of a portfolio under management represented by investments, vehicles and products that are either new or deemed to be high risk, during the preceding calendar month.  |
| Orders and Instructions - Number Executed without Required Authorisation  | Current, Lagging | The total number of orders and instructions executed without the required authorisation during the preceding calendar month.   |
| Transaction Volumes - Number of Disputed Transactions   | Current, Lagging | The total number of open transactions currently disputed by the customer, client or counterparty.  |

### 8.2.3. Commercial Banking

| Name   | Nature           | Description   |
|--|------------------|---|
| Branches, Disposal Points and Operations in High-Risk Countries - Number                       | All              | The number of currently active branches, disposal points and operations located in countries deemed to be high-risk.  |
| Collateral Agreements - Number Missing or Not Executed after Exemption Period                  | All              | The number of collateral agreements currently missing or not executed and beyond the organisation's maximum exemption period.   |
| Credit Facility Applications - Number Approved Based on Financial Reports Older than Threshold | Leading, Current | The number of credit facilities approved during the preceding 12 calendar months where at least one supporting financial report or document was older than a pre-defined threshold.   |
| Credit Facility Reviews - Number not Performed within Policy Threshold                         | All              | The total number of credit facilities that are currently beyond the pre-defined threshold for review and have not been reviewed.  |
| Customer and Client Relationships - Number of Relationships not Reviewed within Threshold      | All              | The number of existing customer and client relationships that are beyond the pre-defined threshold for review and have not yet been reviewed.   |
| Customers and Clients - Number of Financing Relationships based on Movable Underlying Assets   | Current, Lagging | The total number of customer and client financing relationships where the underlying asset subject to the financing is mobile or readily transportable.   |
| Mortgages, Commercial Property and Home Loans - Number of Interest Claims Settled              | Lagging          | The total number of interest claims raised against the organisation due to the late registration of a mortgage loan, delays in closure due to lost or misplaced title deeds or other processing delays, which were settled by the organisation during the preceding calendar month. |
| Payments - Number with Settlement Instructions Deviating from Standing Settlement Instructions | Current, Lagging | The total number of payments generated during the preceding calendar month with standing settlement instructions that were superseded by special instructions.  |
| Payments - Ratio of Payments by Manual Payment Methods to Electronic Payment Methods           | Current          | The ratio of transactions settled using non-electronic payment methods to those using electronic payment methods during the preceding business day.   |
| Workouts - Number of Credit Defaults Awaiting Workout  | Current          | The total number of credit defaults formally handed over for workout and recovery where workout has not yet commenced.  |

### 8.2.4. Corporate Finance

| Name  | Nature           | Description   |
|---|------------------|---|
| Accredited Advisory Staff - Number with Out of Date Accreditation                         | All              | The number of accredited advisors representing or acting on behalf of the organisation whose advisory license or accreditation is out of date at the point of measurement.  |
| Corporate Finance Deals - Number of Deals Executed without Timely Regulatory Filings      | Lagging          | The number of corporate finance transactions executed during the preceding 6 calendar months without timely regulatory filings before or during the execution process.  |
| Corporate Finance Deals - Number of Post-Execution Reviews not Performed within Threshold | Current, Lagging | The number of post-execution reviews of corporate finance transactions not performed within threshold.  |
| Custom or Structured Transactions - Number Modified or Terminated                         | All              | The total number of custom or structured transactions executed by the organisation with its customers and clients that were modified or terminated during preceding 6 calendar months.                                |
| Insider Trading - Number of Instances Detected  | Lagging          | The total number of instances of insider trading detected by the organisation during the preceding 3 calendar months.   |
| Limit Breaches - Number of Legal Lending Breaches   | Lagging          | The number of breaches of legal and regulatory lending limits during the preceding calendar month.  |
| Special Purpose Vehicles - Number not Reviewed within Threshold Period                    | Current, Lagging | The total number of special purpose vehicles (SPV's) in use or under administration that are currently beyond the threshold for review and have not been reviewed.  |
| Special Purpose Vehicles - Percentage Involvement per Vehicle                             | Current, Lagging | The current percentage of involvement for each special purpose vehicle in which the organisation has an interest.   |
| Staff - Number of Staff with Inappropriate or Unnecessary Access to Proprietary Research  | All              | The number of staff who, during the preceding 12 calendar months, had unnecessary or inappropriate access to the organisation's proprietary research, regardless of whether that access resulted in any improper use. |

### 8.2.5. Payments and Settlements

| Name   | Nature           | Description   |
|--|------------------|---|
| Automated Clearing House Returns - Number                                    | All              | The number of files returned by all automated clearing facilities during the previous business day.   |
| Cash Breaks - Number over Threshold  | Current, Lagging | The total number of cash breaks on the organisation's clearing and/or Nostro accounts that are currently older than the organisation's predefined threshold.  |
| External Payment System Outages - Number                                     | All              | The number of outages of external payment systems to which the organisation has interfaces and/or interdependencies, during the preceding 12 calendar months. |
| Legal Entity Payment Mismatches - Number                                     | Lagging          | The number of payment mismatches detected during the preceding calendar month across legal entities within the organisation.                                  |
| Nostro Breaks - Number of Open Items   | All              | The total number of open Nostro breaks at the point of measurement.   |
| Payment and Settlement Fails - Total Number of Fails                         | All              | The total number of settlement fails during the preceding business day.   |
| Payment and Settlement Fails - Total Value of Fails                          | All              | The total gross value of settlement fails during the preceding business day.  |
| Payment System Outages - Number  | All              | The number of outages of the organisation's payment systems during the preceding calendar month.  |
| Payment Volumes - Percentage of Daily Settlement Volume Eligible for Netting | Lagging          | The percentage of settlements during the preceding business day that were eligible for netting.   |
| Payments - Number Generated without Standing Settlement Instructions         | All              | The total number of payments generated during the preceding calendar month that did not have applicable, predefined, standing settlement instructions.        |

### 8.2.6. Retail Banking

| Name  | Nature           | Description   |
|---|------------------|---|
| Branches and Disposal Points - Total Number of Robberies                                      | Lagging          | The total number of robberies by external parties across all the organisation's branches and disposal points during the previous calendar month.  |
| Brokers, Agents and Intermediaries - Number of Introduced Customer Applications Rejected      | All              | The total number of new customer or client applications introduced to the organisation by brokers, agents and intermediaries during the preceding 12 calendar months that the organisation rejected.  |
| Card Transactions Disputed - Number Open  | Current, Lagging | The total number of card transactions disputed by customers and clients that currently remain open.   |
| Cards - Number of Stolen Cards Reported   | Current, Lagging | The total number of cards issued by the organisation to its customers and clients that have been reported stolen during the preceding 3 calendar months.  |
| Customer and Client Accounts - Number of New Accounts Opened                                  | Leading, Current | The number of new retail account relationships opened during the preceding month.   |
| Customer and Client Relationships - Number of Instances of Returned Mail                      | Current, Lagging | The total number of customer or client relationships where mail has been returned by the postal services as undeliverable or refused during the preceding 3 calendar months.  |
| E-Crime - Number of E-Banking Accounts Compromised by Phishing or Trojans                     | Current, Lagging | The number of customer and client e-banking accounts which have been compromised specifically through phishing and/or trojans.  |
| Forged Cheques/Checks and Drafts Presented - Number   | Leading, Current | The number of instances of forged cheques/checks and drafts being presented to the organisation for payment that were detected during the preceding 3 calendar months. It includes both successful forgeries where value was extracted from the organisation and failed attempts. |
| Mortgages, Commercial Property and Home Loans - Percentage of Approved Loans not yet Taken Up | All              | The percentage of approved loans granted or on which instructions are issued over the preceding calendar month which have not yet been taken up by the customer or which have been rejected by the customer.  |
| Staff - Percentage of Staff not Completed Primary Fraud Detection Training                    | Current          | The number of staff who have not yet completed all primary fraud-detection training required for their job function and grade, as a percentage of the total number of permanent employees.  |

**8.2.7. Retail Brokerage**

| Name  | Nature           | Description  |
|---|------------------|--|
| Confirmations - Number of Unmatched Confirmations for Over-the-Counter Transactions with No Previous Cashflow | All              | The total number of confirmations generated where no inbound confirmation has yet been received from the counterparty, the underlying transaction is an over-the-counter (OTC) one, and no cashflow has occurred.  |
| Customer and Client Product Usage - Percentage of Product Suitability Approvals Outstanding                   | Leading, Current | The total number of currently outstanding customer and client product suitability approvals for products already offered to customers and clients, as a percentage of the total number of customer and client relationships.   |
| Customer and Client Relationships - Number without Adequate Background and Reference Checks                   | All              | The total number of current customers and clients that have not yet been through the organisation's background and reference checking procedure at the point of measurement.   |
| Customer Mandates - Number of Breaches Detected   | Current          | The total number of breaches of customer mandates by the organisation, its employees, agents or representatives detected during the preceding calendar month.  |
| Customers and Clients - Frequency of Changes to Standing Settlement Instructions                              | Current, Lagging | The average number of changes per month to a customer or client's standing settlement instructions, during the preceding 12 calendar months.   |
| Customers and Clients - Number of Customer Money Segregation Breaches   | Lagging          | The number of breaches of customer and client money segregation policies and procedures arising from the processing of payments, during the preceding calendar month.  |
| Dealers, Traders and Investment Managers - Number of License Exceptions                                       | Current          | The number of transactions executed by approved dealers, traders and investment managers during the preceding 12 calendar months that did not comply with restrictions imposed by their trading licenses or where the individual lacked a current trading license.                 |
| Dealers, Traders and Investment Managers - Percentage of Total without Dealing Mandates                       | All              | The number of approved dealers, traders and investment managers who currently have no formal dealing mandate defining the limits on their delegated dealing, trading and/or investment authority, as a percentage of the total number of dealers, traders and investment managers. |
| Fee and Charge Reversals - Number   | Current, Lagging | The total number of fee or charge reversals booked during the preceding 3 calendar months across all entities within the organisation.   |
| Limit Breaches - Number of Dealing and Trading Limit Breaches   | All              | The total number of dealing and trading limit breaches detected during the preceding 6 calendar months.  |

**8.2.8. Trading and Sales**

| <b>Name</b>  | <b>Nature</b>    | <b>Description</b>   |
|--|------------------|--|
| Best Execution - Number of Best Execution Exceptions   | Leading          | The number of transactions not executed at the best price or terms available, or not following best practices intended to ensure they are, which were identified during the preceding 3 calendar months.   |
| Confirmation Mismatches - Total Number   | All              | The total number of transactions within the matching process with mismatched transaction details or legal terms that currently remain unmatched.   |
| Confirmation Mismatches - Total Value of Mismatched Transactions                                     | Current, Lagging | The total value of transactions within the matching process with mismatched transaction details or legal terms that currently remain unmatched.  |
| Dealers, Traders and Investment Managers - Percentage of Total without Dealing Mandates              | All              | The number of approved dealers, traders and investment managers who currently have no formal dealing mandate defining the limits on their delegated dealing, trading and/or investment authority, as a percentage of the total number of dealers, traders and investment managers. |
| Dealing and Trading Locations - Percentage of Transaction Volume using Non-Central Trading Platforms | All              | The total volume of transactions executed using non-centralised dealing and trading platforms during the preceding 6 calendar months, as a percentage of the total number of transactions executed during the period.  |
| Dealing Mandates - Number of Breaches Detected   | Current          | The total number of breaches of dealing mandates by the organisation or its dealers, traders and investment managers detected during the preceding calendar month.   |
| Limit Breaches - Number of Dealing and Trading Limit Breaches  | All              | The total number of dealing and trading limit breaches detected during the preceding 6 calendar months.  |
| Manual Deal Slips - Number Unaccounted For   | All              | The total number of manual deal slips issued for use during the preceding 12 calendar months that currently cannot be accounted for.   |
| Models and Methodologies - Number Developed by End-users not Reviewed within Threshold               | Current, Lagging | The total number of models and methodologies developed by end-users the organisation currently has available for use that have not yet been reviewed and are beyond threshold.   |
| Pricing - Number of Transactions Identified Priced outside of Permitted Deviations                   | Leading, Current | The number of transactions executed at rates or prices outside the organisation's permitted deviation from market reference prices during the preceding 6 calendar months.   |

### 8.2.9. Corporate Services

| Name   | Nature           | Description  |
|--|------------------|--|
| Access Rights to Applications by Staff - Frequency of Access Right Reviews                     | All              | The average number of reviews per month of staff access rights to business applications during the preceding 12 calendar months.   |
| Accounting - Number of Amendments to the Charts of Accounts                                    | Leading, Current | The number of changes made to charts of accounts of the organisation during the preceding 12 calendar months.  |
| Assets in Transit - Total Value  | Current, Lagging | The total value of assets in transit at any point during the preceding business day.   |
| Business Continuity Management (BCM and BCP) - Number of Plans not Authorised beyond Threshold | All              | The number of Business Continuity Plans (BCP) which have been reviewed but which have not yet been re-authorised, and are beyond a pre-defined time limit for reauthorisation, as well as the number of Business Continuity Plans (BCP) which have been prepared for the first time, but which have not yet been authorised and are beyond the pre-defined time limit for authorisation. |
| Critical System Changes - Number of Emergency Software Changes                                 | Current          | The number of emergency software changes made to critical systems during the preceding 12 calendar months.   |
| Critical System Outages - Average Duration   | All              | The average duration, expressed in minutes, of unscheduled critical system outages per month, during the preceding 12 calendar months.   |
| Information Technology Support Requests - Number Outstanding beyond Threshold                  | Current          | The number of information technology support requests currently outstanding and beyond threshold.  |
| Litigation Cases - Number Closed   | Current, Lagging | The total number of litigated customer and client compensation cases that were closed or withdrawn during the preceding 3 calendar months.   |
| Offices and Operations - Number of Field Visits to Remote Locations                            | Leading, Current | The number of visits by senior management based in centralised locations to remote locations during the preceding 12 calendar months.  |
| Physical Security - Number of Physical Security System Activations                             | Leading, Current | The number of instances during the preceding 12 calendar months that physical security systems and environmental problem detectors on the organisation's property and premises gave alarm for any reason.  |
| Policy and Procedure Breaches - Number of Detected Instances of Inadequate Segregation of Duty | Current, Lagging | The number of segregation of duty policy breaches detected during the preceding 12 calendar months.  |
| Project Management - Number of High-Risk Projects  | All              | The number of projects currently in progress which have been rated or are considered as being high-risk.   |
| Property and Facilities - Number of Health and Safety Incidents Reported                       | Leading, Current | The number of incidents relating to health and safety at the organisation's properties and premises that were reported during the preceding 12 calendar months.  |
| Regulatory Reports - Number of Errors  | Current, Lagging | The total number of reports or statements provided to regulators in which errors were detected after the reports had been submitted, during the preceding 12 calendar months, across all jurisdictions and legal entities within the organisation.   |
| Staff - Number of Staff with Non-Compliance of Holiday Regulations                             | Current, Lagging | The number of employees who currently are out of compliance with the organisation's vacation or holiday regulations and beyond threshold.  |



**8.2.10. Insurance**

| <b>Name</b>   | <b>Nature</b>    | <b>Description</b>  |
|---|------------------|---|
| Claims Assessor - Number of Assessor Appraisals not Completed Within Threshold                    | Lagging          | The number of claims assessors who were given an appraisal within the given threshold, during the preceding 12 calendar months.   |
| Complaints from Customers, Clients or Policy Holders - Number Received regarding Claims Assessors | All              | The number of policy holder complaints with respect to the work of the claims assessors.  |
| Insurance Claims - Average Number of Claims Per Client  | Lagging          | The total number of claims received over the preceding 12 calendar months divided by the total number of clients, representing the average number of claims per client.                                       |
| Insurance Claims - Percentage of Claims Received Flagged as Suspicious                            | Current, Lagging | The percentage of all claims received during the preceding 12 calendar months which were flagged as suspicious.   |
| Insurance Policies - Number of New Policies Issued with Unapproved Variances or Terms             | All              | The number of insurance policies issued during the preceding 12 calendar months which contained unapproved variances to standard procedures or terms and conditions which had not been specifically approved. |
| Insurance Proposals - Number of Non-Standard New Business Proposals Made                          | Lagging          | The number of proposals for new insurance business made to clients during the preceding 12 months that related to non-standard cover or to custom or bespoke insurance policies.                              |
| Reinsurance Claims - Number Disputed  | Current, Lagging | The total number of reinsurance claims made by the organisation in the preceding 12 calendar months that were disputed by the reinsurer.  |
| Reinsurance Treaties - Number of Changes in Conditions that Cannot be Passed on to Policies       | Leading, Current | The indicator captures the number of changes in reinsurance conditions during the past 12 calendar months that cannot be passed on to existing policies.  |
| Reserves - Number of Errors in Calculating Claims Reserves  | Leading, Current | The number of detected errors in the calculation of claims reserves.  |
| Risk Assessor - Number of Assessors not Completed Primary Risk Assessment Training                | Current          | The number of risk assessors who have not yet completed all primary risk assessment training required for their job function and grade.   |

### 8.3. Example Documentation

A sample specification for how indicators can be documented is provided below using customer complaints as an example:

| <b>Definition</b>     |  |                             |                 |
|-----------------------|--|-----------------------------|-----------------|
| Number:               | 10135  |                             |                 |
| Name:                 | Complaints from Customers, Clients, Beneficiaries and Counterparties - Number Open   |                             |                 |
| Description:          | The number of formal complaints raised by customers, clients, counterparties and beneficiaries that currently remain open. |                             |                 |
| Nature:               | Leading, Current   |                             |                 |
| Type:                 | Exposure Frequency   |                             |                 |
| Causal Type:          | Business Conditions  |                             |                 |
| Rationale/Comments:   | Indicator measures the total number of formal complaints remaining open at the measurement point.                          |                             |                 |
| Rating:               | 2 - Internal Comparability   | Yes - Externally Comparable | 2 - Ease of Use |
| Version:              | 1.3  |                             |                 |
| Version Release Date: | 18/05/2009   |                             |                 |
| <b>Specification</b>  |  |                             |                 |
| Value Format:         | Count  |                             |                 |
| Dimensions:           | Business Unit<br>Complaint Type<br>Country<br>Customer or Client Type  |                             |                 |

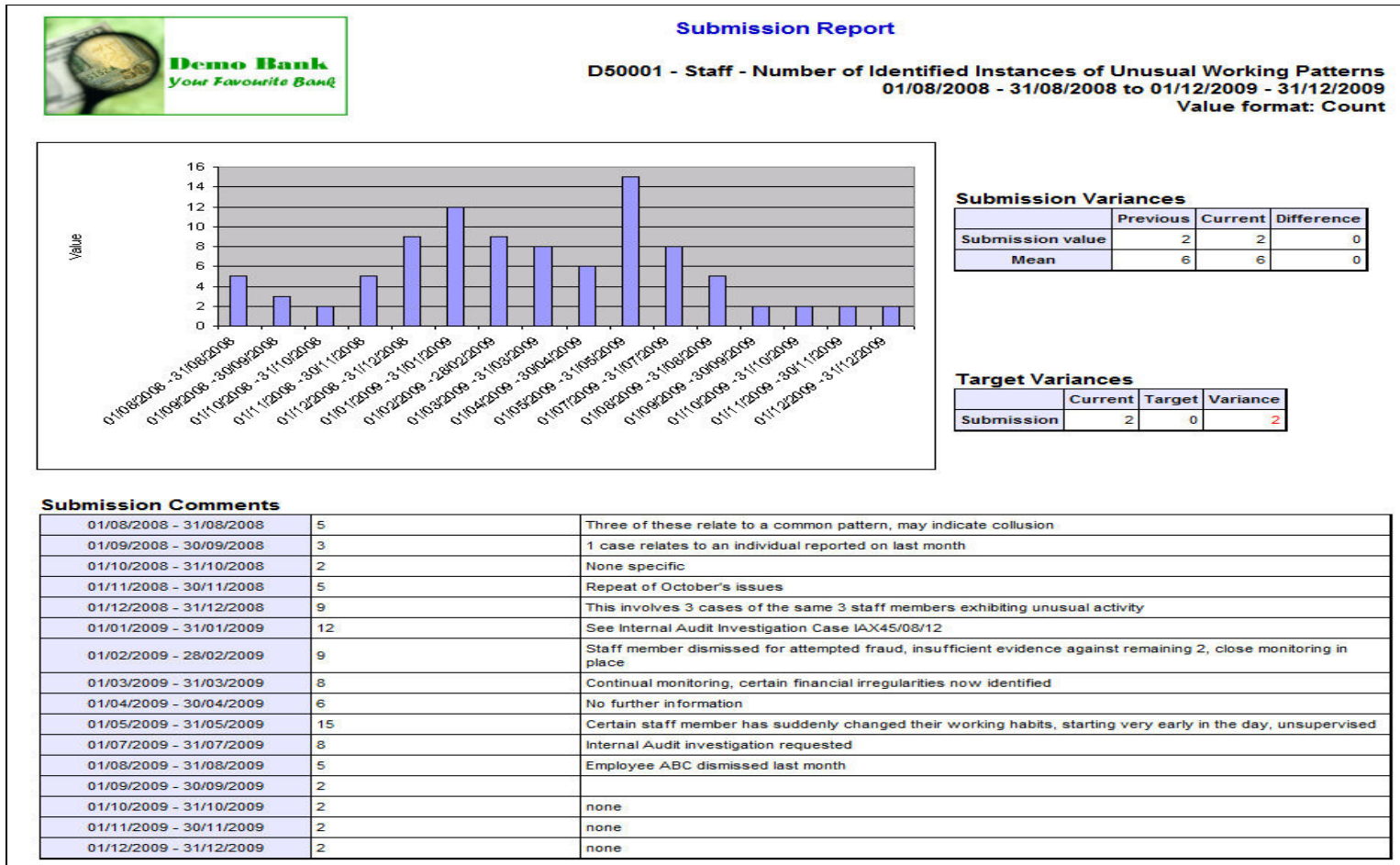
|                        |   |
|------------------------|---|
|                        | Location<br>Product or Service Group  |
| Buckets:               | Indicator values should be divided into time-band buckets reflecting length of time the complaint has been open.  |
| Bucket Variants:       | None specific   |
| Currency Conversion:   | Not applicable  |
| Measurement Rules:     | Include all formal complaints received in writing from all customers, clients, counterparties and beneficiaries that currently remain open, regardless of nature or severity, or the length of time since the complaint was received. Treat multiple counts of a single infraction received in either a single or multiple notifications as one instance. Treat multiple infractions received in a single notification as separate instances. Include open complaints from former customers, clients, counterparties and beneficiaries. |
| Underlying Indicators: | None  |
| Calculation Method:    | Count the number of complaints meeting measurement criteria. The indicator value should be calculated for each dimensional node listed above, using the aggregation method and scaling rules given below.   |
| Calculation Formula:   | None  |
| Benchmark Rules:       | The indicator value should be scaled for benchmarking by the number of customers and clients.   |
| Aggregation Method:    | Simple summation using the dimensional nodes listed.  |
| Aggregation Rules:     | None specific   |
| Scaling Denominator:   | 30056 - Customer and Client Relationships - Total Number of Relationships   |
| Scaling Rules:         | The indicator will be scaled by each 1,000 customer and client relationships. Divide the indicator value by KRI 30056 and multiply the result by 1,000, rounding the result to 2 decimal places. Aggregate before scaling. Numerator and denominator must be at the same level of aggregation.  |
| <b>Guidance</b>        |   |
| Usage:                 | Internal and Benchmarking   |

|                        |  |
|------------------------|--|
| Measurement Frequency: | Weekly   |
| Reporting Frequency:   | Monthly  |
| Frequency of Change:   | Ad-hoc   |
| Limitations on Scope:  | None specific  |
| Collection Level:      | Branch/Operating Entity  |
| Definition Threshold:  | None specific  |
| Variants:              | None specific  |
| Direction Information: | A greater value suggests greater risk.                         |
| Trend Information:     | Increasing indicator values over time suggest increasing risk. |
| Control Indicator:     | Yes  |
| SoX Indicator:         | Yes  |
| Source:                | Relationship Management function or Operations.                |
| Industry Nature:       | Financial Services Generic                                     |
| Original Release Date: | 22/05/2003   |


Source: KRiEX.org – The KRI Library, Risk*Business* International Limited 2003 - 2010

### 8.4. Example Report for Management

The following provides some examples of management reports.



This report shows the values submitted for a specific indicator over a time series, including submission comments and variances.



### Submission Exception Report

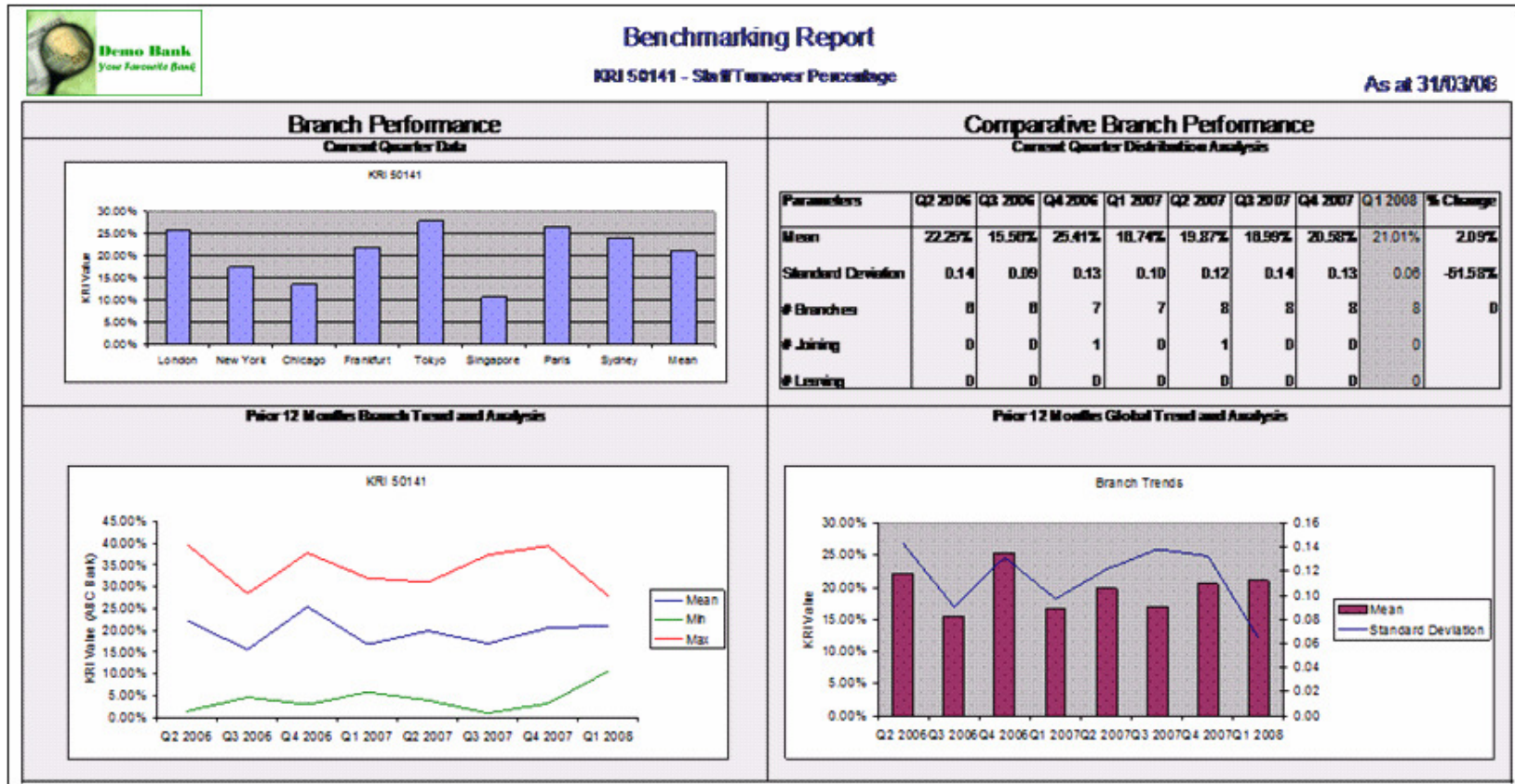
**D50001 - Staff - Number of Identified Instances of Unusual Working Patterns**  
**01/08/2008 - 31/08/2008 to 01/12/2009 - 31/12/2009**  
**Value format Count**

| Indicator   | Measurement Period      | Submission | Threshold Type | Threshold Limits |       | Variance | Commentary                             |
|---|-------------------------|------------|----------------|------------------|-------|----------|--|
|   |                         |            |                | Lower            | Upper |          |  |
| D50001 - Staff - Number of Identified Instances of Unusual Working Patterns | 01/07/2009 - 31/07/2009 | 8.00       | Cap            | .00              | 5.00  | 3.00     | Internal Audit investigation requested |
| D50001 - Staff - Number of Identified Instances of Unusual Working Patterns | 01/08/2009 - 31/08/2009 | 5.00       | Cap            | .00              | 5.00  | .00      | Employee ABC dismissed last month      |

This report shows threshold exceptions for the same indicator as included in the previous report example.

### 8.5. Example Report for Board

The following report reflects a comparative analysis of the same indicator across numerous branches as could be reported to Board level.



## 8.6. Composite Indicators

Some potential composite indices are:

- Process quality index
- Business unit risk index
- Error correction cost index
- Technology stability index
- Client satisfaction index
- Employee satisfaction index
- Litigation exposure index
- Ethical quality index
- Asset protection index

To compile a composite index on the error correction cost, the first step is to identify the underlying indicators that measure the underlying causal and risk drivers impacting error rates, for example:

- Historical error rate
- Historical staff availability levels
- Transaction volumes over time, including cyclicity information
- Transactional volatility over time
- Historical average transactional value
- Average cost of error correction

Using factor analysis, a base case index can be constructed, on which a variance in any single contributing factor or any combination of factors can be applied to see where the potential cost of error correction will go. This information can then be used as an input into staff vacation planning, timing of vacation, training or other absence from the workplace, assessing the potential benefits of training expenditure, etc.

In theory, the 'formulas' for these composite indices could also be agreed externally amongst peer organisations and hence, the indices could be benchmarked; however, in practice, 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 indices will need to be tested and possibly refined over time in the light of actual experience.



## 8.7. Web Resources

[www.kriex.org](http://www.kriex.org)

In 2003, the Risk Management Association, in conjunction with Risk*Business* International Limited, launched an initiative aimed at furthering the use of KRIs across the financial services industry. This followed the publication of several whitepapers by international rating agencies regarding the inclusion of operational risk effectiveness capabilities into an organisation's credit rating, as well as the publication of the then draft Basel II guidelines which suggested that standardised indicators could be used to adjust an organisation'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;
- 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
- To facilitate the formal comparison of such exposures between peer groups, using the standardised specifications in an anonymous manner.

Over 2,500 banking-specific and 1,500 insurance-specific indicators are now maintained and provided through a subscription-based online repository of indicators. Examples of indicators from the KRI Library are included in Appendix 8.1.