

Risk Indicators: a way to Day-to-Day Riskmanagement

Dr. Gerrit Jan van den Brink

Abstract

Risk indicators are essential instruments for pro-active operational risk management. They should help to predict changes in the company's operational risk profile. The risk indicator have two targets: the prevention of operational risk events and the timely detection of unfavourable trends. A risk indicator needs some characteristics in order to meet those targets. The remaining reaction time plays an important role.

A first indication for the definition of risk indicators can be found in actual process descriptions, loss and self-assessment data and risk capital numbers.

Introduction

Banks focussed more strongly on operational risk recently. Operational risk is the risk of a loss caused by failures or inadequacies, which can occur due to four risk cause categories: people, systems, processes and external factors. The regulatory requirements which were published in the Basel Committee's International Convergence on Capital Standards and Capital Measures [Basel Committee on Banking Supervision, 2005] and the Sound Practices for the Management and Supervision of Operational Risk [Basel Committee on Banking

Supervision, 2003] have contributed to this new focus. Especially the Sound Practices (which are valid for all banks regardless the approach they choose for the regulatory capital calculation) prescribe the identification and assessment of operational risks. One of the possibilities to identify risk is the implementation of risk indicators.

Risk management requires a future-oriented focus. In an ideal world a bank wishes an empty loss database and self-assessment results, which show an insignificant operational risk profile. The implementation of risk indicators, however, is a prerequisite to touch in the direction of the ideal world.

In this article the process of risk indicator definition will be described. After showing the targets of risk indicators and their characteristics, the process will be described to find the right risk indicators.

Definition and Targets

Risk indicators can be defined as follows:

Risk indicators are parameters, which focus on business processes or process bundles to predict upcoming changes in the operational risk profile of those business processes or process bundles.

The most important word in the definition is the verb "predict". Risk indicators focus on the future and are therefore essential instruments for the organisation's risk management. The time window available for reactions is critical: the earlier a change in the risk profile is detected, the better. The longer the time window for reaction the bigger the chance to prevent any damage.

A causal analysis is therefore a key condition to define valid risk indicators. If only operational risk events are captured by a risk indicator, the risk is already manifest and in most cases a short time period to react remains. Damage cannot be prevented anymore in most cases.

Risk indicators should achieve the following targets:

- Operational risk events should be prevented
- Unfavourable trends should be detected in time.

The prevention of operational risk events can be effectively supported by an IT-application. The system executes periodical measurements and checks if the predefined thresholds have been exceeded. If a threshold has been exceeded, the responsible staff for the affected process receives automatically a message, to enable them to start remedial actions. Such solutions are more effective than those sending such messages to risk controllers. Especially in case of short reaction time periods, the message has to go to the people who can immediately act first.

Some risks, however, cause an event over a long time period, by infecting slowly but certainly. The risk indicator still moves in the "green zone" but its values are getting a bit worse time after time. Such an unfavourable trend can indicate a need for actions. For example motivation of staff can be mentioned. If the motivation index gets worse and worse, it is time to react, even if the values are still below the threshold. A considerable amount of time elapses, before the trust of staff has been regained. Decreasing motivation is closely linked to mistrust and frustration. It should be taken into account, that reactions on such trends take a considerable time before they become effective. The time window for reactions "closes" in this case already in the "green zone".

Risk indicator characteristics

The achievement of the described targets is determined by the characteristics of the various risk indicators. Some characteristics may seem to be a common place, but experience regarding the definition of risk indicators shows, that it is important to remember those during the definition of indicators.

Following characteristics can be identified:

- Risk indicators should be measured on a regular basis
- Risk indicators should reflect the risk
- Risk indicators need thresholds; management should be informed after

the excess of those thresholds to take actions

- Risk indicators should be measured on a timely basis
- Risk indicators should detect changes in the risk profile before the operational risk events become manifest
- Risk indicators should be measured efficiently

Measurement on a regular basis is necessary to prevent operational risk events and to detect unfavourable trends. A trend cannot be recognised (in time), if not a number of measurement results are available. The frequency, however, needs to be questioned. How often should a measurement be executed? There is no direct answer to this question. The following approach may help to become a clearer picture: Both the remaining time to react and the expected damage amount will play an important role. If the time window is rather narrow to react after the receipt of the threshold excess message, the measurement frequency should be increased. The exact increase of the measurement frequency, however, is determined by the expected loss and its standard deviation. If these values are high, the need for more frequent measurements becomes even higher.

The measurement frequency also determines the effectiveness of a risk indicator, since the risk awareness of the responsible manager can cause undesirable behaviour. If the manager thinks, the measurement frequency is too low, he will not trust the messages resulting from the risk indicator system. Instead he will

build a shadow system to monitor the risk more frequently. If he thinks the measurement frequency is too high, he will start to neglect the messages resulting from the risk indicator system, since he thinks the monitoring is too fine tuned. If a real problem occurs, he may detect this too late. It may then be late to execute corrective actions.

The characteristic that the risk indicator *should reflect the risk*, seems to be unnecessary. However, if risk indicators of organisations are reviewed, it appears, that this characteristic is not always given. For example the following risk indicators in the financial industry can be mentioned:

- Transaction volumes
- IT-network traffic
- Number of open items on nostro-accounts.

Such risk indicators are often implemented, since measurements are already taking place and therefore no additional cost occurs. If the reflection of risk is checked, the vulnerability of those indicators mentioned is detected. The indicator "transaction volume" is used for performance measurement and cost allocation purposes. But what does the indicator tell about risk? If its value moves from 10,000 to 20,000, does this mean that the risk has been increased? The question cannot be solved by these values only. Everybody, however, perceives, that a risk increase could be possible based on these values, if the transaction processing capacity is completely exhausted. If the usage of the transaction processing capacity is measured, an indicator has been found, which is able to measure a

change in the risk profile. The same approach can be taken for the risk indicator "IT-network traffic".

The number of open items on nostro-accounts is also often used as a risk indicator. The risk to be monitored is the possibility that a bank already credits customer or counterparty accounts internally, although the amount was not credited to its nostro-account. This causes at least an interest expense and in case of fraud the full amount may be lost. However, the number of open items does not measure this risk. If the open items are just one day old, no risk is manifest. If the open items are for example 30 days old, interest losses have already occurred. Moreover the monetary value may also be lost due to fraudulent actions. To measure the risk the aging of the open nostro items is essential. The monetary volume should be aged as well, since if the value of an open item is EUR 50 the importance is totally different to an open item of EUR 1 billion.

The need for thresholds results from the prerequisite to detect changes in the risk profile early. The implementation of this requirement determines on the effectiveness of a risk indicator. Thresholds should fit to the risk appetite of the responsible process managers. If the manager thinks, that the threshold is too low, he will not pay enough attention to warnings issued by the risk indicator. This may cause an operational risk event and subsequent damage, which could have been avoided. If the manager thinks that the thresholds are too high, he will not trust the warning capability

and build its own monitoring instruments.

The threshold level is also determined by the available time to react. For example if database capacity needs to be enlarged, it takes time before such an action can be completed. Such database expansion cannot be executed during business hours and therefore a full day production needs to be considered as well. If an elapsed time of four hours for a database expansion is taken into account, it should be considered how much capacity is used per hour. These values will determine at which capacity usage level a threshold should be set, in order to avoid damages.

A timely measurement is also essential to stay within the reaction window. The importance is depicted in figure 1:

Reaction time determines the risk indicator quality

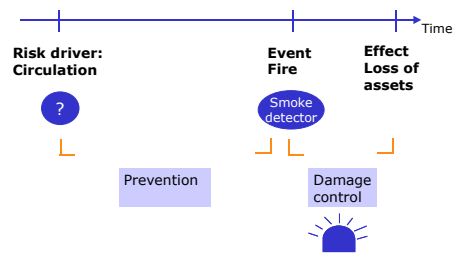


Figure 1

The reaction time window ends shortly before the risk event occurs. Sometimes even days remain to react; but in some cases only some minutes are left. Therefore actions should be aligned to the remaining reaction time.

The characteristic of a timely indication of changes in the risk profile of a financial institution is hard to guarantee. Especially if the elapsed time between the manifestation of the risk driver and the subsequent effect is short, changes in such risk drivers need to be identified at the earliest point in time as possible. For example changes in market volatility are messengers announcing an increase in transaction volumes.

The last characteristic describes the measurement efficiency of risk indicators. Risk indicators cause periodical expenses, since they need to be measured and sometimes the results come together in the risk indicator system by use of IT-interfaces. The expenses for risk indicators should not exceed the potential savings of standard risk cost and capital cost. In case of an excess, the risk acceptance is better for an economic point of view.

Risk indicator definition process

The successful implementation of risk indicators depend on the fulfilment of some conditions. Before a risk indicator project is started, the fulfilment of the conditions should be considered. The following three points should be investigated:

- Does a control culture exist in the involved organisational units?
- Are monitoring procedures already implemented in the organisational unit?
- Does a process description exist, are losses caused by risk events collected and

are self-assessments executed?

The control culture decides the success of the implementation of risk indicators. Culture can be hardly measured. Based on the following questions a picture can be drawn:

- Is transparency in the bank/organisational unit promoted?
- Is a clear strategy which also includes risk appetite and tolerance of senior management available?
- Is the implementation of a strategy monitored?
- Are errors seen as a moment to learn, order should involved staff take disciplinary actions into account if errors are discussed?
- Are remediation actions to solve weaknesses seriously planned and is the implementation monitored?

This question list is definitely not exhaustive, but the answers give a first picture regarding the robustness of the control culture. This cultures needs to be "lived" on all organisational levels, since higher level have always a example function for the lower ones.

If an existing monitoring procedure is in place, it is a first indication of future oriented management. Management obviously understands, that undesired changes in the values measured need counter actions. Moreover it is helpful if the risk indicator system can build on existing escalation procedures.

An analysis of loss data and self-assessment results together with risk capital value and process

descriptions show the vulnerability of processes or systems.

If losses with the same causes occurs more frequently in a process, a structural problem may be the issue. If this problem cannot be solved, monitoring by use of risk indicators can improve the situation. Insufficient process quality can be detected by use of self-assessments. If the quality issue is caused by an inherent problem, risk indicators again can be a solution. The risk capital can be decomposed to processes and organisational units showing the more risk full areas, in which the most serious weaknesses can be expected. In all cases risk indicators should not be implemented automatically, since the solution of a problem is still the most effective solution. Especially risk controller are quickly tempted to implement a risk indicator in such cases. It should be remembered that risk indicators cause initial and periodical expenses.

The definition of risk indicators need to be prepared carefully. This process starts with the selection of the workshop participants. These participants should have a sound understanding about the objects to be monitored. Therefore it is almost excluded, that a central risk management or controlling unit defines the risk indicators centrally, since it is not familiar with the details of all processes. The process manager's experience regarding the process inherent risks should not be underestimated. It is an important source for the definition of risk indicators. The end-to-end process view is important during the selection of

the risk indicators, since the risk drivers should be identified as early as possible in the process.

This requires an holistic perspective of both the workshop participants and the moderator.

It is often questioned, if each organisational unit needs to handle the definition process on its own. Would it not be better, if a central organisation would define a collect a central library of possible risk indicators from which each organisational unit could take advantage? Moreover, if risk indicators would not be defined centrally, in which way could consistency be guaranteed also for aggregation possibilities? A uniform definition is also essential for the benchmarking among organisational unit. Currently various banks are building up a common risk indicator library with the future target to benchmark externally. It looks alike, if all arguments would be in favour of a central library of uniform defined risk indicators and let the organisational units just select the ones fitting to their needs. The negative side of such an approach, however, is the missing investigation of the inherent risks and therefore risk drivers may not be detected, which will then not be monitored.

In figure 2 the definition process has been depicted:

How are Key risk indicators defined?

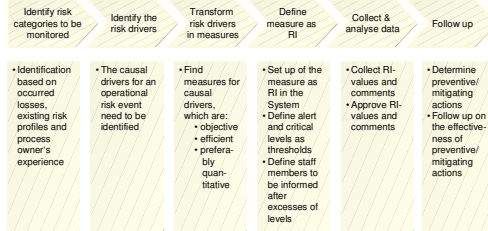


Figure 2

At the start the object to be monitored is determined. It can be just one specific internal control measure (like the nostro account reconciliation), a process or an organisational unit. The selection is based on existing risk profiles.

As already described before the risk drivers are determined in the second step, which need to be made measurable in the third step. The measurability determines the success of a risk indicator. A quantitative measurement is to be preferred above a qualitative assessment, since it is mostly deductible from existing data. Moreover a quantitative measurement is mostly more objective.

The first three steps are the most important ones. Afterwards the risk indicator and its attributes have to be defined. In the fifth step the monitoring phase can be started, in which values are collected, compared to the thresholds and regularly analysed by a risk controller. It is also important, that warning signals are followed up, in order to ensure that the actual risk profile is aligned to the risk appetite and tolerance. In such cases the targets of the measurement by

use of risk indicators have then been completed.

Literature

[Basel Committee on Banking Supervision 2003] Basel Committee on Banking Supervision, Sound Practices for the Management and Supervision of Operational Risk, www.bis.org

[Basel Committee on Banking Supervision 2005] Basel Committee on Banking Supervision, International Convergence on Capital Standards and Capital Measures, www.bis.org

Author

Dr. Gerrit Jan van den Brink is Head of Operational Risk Control in Dresdner Bank AG. He is a lecturer at the Johann-Wolfgang Goethe Universität and the Hochschule für Bankwirtschaft in Frankfurt am Main.