MAB MAANDBLAD VOOR ACCOUNTANCY EN BEDRIJFSECONOMIE

Maandblad voor Accountancy en Bedrijfseconomie 96(5/6) (2022): 165–171
DOI 10.5117/mab.96.80730

Essay

Key Risk Indicators reloaded

Gerrit Jan van den Brink, Marc Leipoldt

Received 18 January 2022 | **Accepted** 12 May 2022 | **Published** 28 July 2022

Abstract

Although Key Risk Indicators have been a staple for Operational Risk Management reports in financial institutions for years now, they are rarely drivers for action and their relevance is waning. The authors argue that, for Key Risk Indicators to become more relevant, they should be recast as predominantly business (first line of defence) driven and made practical rather than theoretical. After describing the current state of Key Risk Indicators and the future for such indicators in case no action is taken, an ideal situation is outlined and five recommendations are presented that serve as practical steps towards that ideal state.

Relevance for practice

Financial institutions are increasingly working under challenging conditions putting the sustainability of their business models under pressure. At the same time, regulators are increasingly focusing on the sustainability of business models. Key Risk Indicators can be a useful tool to retain a grip on existing and emerging risk levels, provided Key Risk Indicators are part and parcel of the first line management review and responsibility.

Key words

Key Risk Indicators, financial Institutions, risk management, operational risk, operational resilience

1. Introduction

The financial sector is subject to a fast-changing business environment which requires strong risk measurement and risk management capabilities. Recent changes to the business environment that affect the risk profile of the business include:

1.1. Prolonged low interest environment

The low interest environment is a source of fundamental changes for the financial sector. Banks are experiencing lower interest income and Insurance companies had to lower guaranteed interest rates (e.g., to 0.25% in Germany) or to drop them completely. Pension funds are struggling to meet their targets (the largest fund in the Netherlands, ABP, is currently 20% behind the desired level).

The European Banking Authority (EBA 2021a) issued Risk Dashboards indicating a weighted Return on Equity ("RoE") for banks in the EU at its lowest point in the second quarter of 2020 at 0.5% rising to 7.4% a year later (EBA 2021a, page 16). This modest rise in RoE in European banks in 2020 is an improvement, but it is largely due to lower provisions for bad loans. Current business environment parameters, in particular COVID-19, the war in Ukraine and substantial changes required by the EU Green Deal put additional pressure on Financial Institutions ("FIs") to better manage risk and avoid associated costs. The EBA (EBA 2021b) already requires banks to include the climate change risk in their credit underwriting and monitoring processes. These requirements provide excellent opportunities to re-imagine Key Risk Indicators ("KRIs") to manage these topics.

1.2. Digitisation of the financial sector

Partly driven by the COVID-19 pandemic, innovations in (on-line) relationship management, new uses for Artificial Intelligence (AI) as well as other experimental technologies such as block-chain and robo-investment advice, unintended consequences and risks are emerging throughout the business processes. Certain unintended consequences, such as denying groups of people or companies banking facilities, can result in regulatory sanctions. The Dutch Central Bank (DNB 2019) has issued a note indicating their concerns and in their strategy paper (DNB 2021) this point was reinforced.

1.3. Circumstances affecting operational resilience

The COVID-19 pandemic led to specific supervisory guidance of the Financial Stability Institute (FSI 2021). In addition, the European Commission has issued the Digital Operational Resilience Act which comes into force in 2023. This act focuses on business continuity of operations, outsourcing management, IT-Security and IT-incident management.

Considering the rapid changes to the business environment, the stronger focus on the sustainability of the business models of FIs and the decreasing reaction window as a result of automation and digitisation, the authors believe that the concept of KRIs should be reinterpreted. KRIs must become an integral part of the business workflow and be incorporated into standard management tools. This approach will support the management of FIs to consider the changes to the risk profile of the business model and the consequently lower risk appetite which FIs can accept.

KRIs as a standard tool came on the scene as part of formalisation of Operational Risk Management ("ORM") in the Basel II regulation, starting in 1999 (BCBS 1999). Although the first draft of Basel II (BCBS 2001) was clear on the purpose of the ORM initiatives (namely to allow for better risk management), the focus soon moved to capital calculation, the bread and butter of Basel II. A range of qualitative methods were outlined in an implementation paper that went through a few editions, currently called "Principles for the Sound Management of Operational Risk" (BCBS 2020).

KRIs were mentioned in the latest BCBS consultative document (BCBS 2020, p. 1) lamenting the inadequate implementation of the KRIs. No specific recommendations, however, were provided.

Regulation around KRIs in the insurance and pension industry does not fundamentally differ from that in banks but the regulation around KRIs is even less well defined. EIOPA published a general statement on the management of operational risks in Institutions on Occupational Retirement Provision (IORP) which is similar to KRIs as suggested by the BCBS:

"Risk limits may also be set to notify an IORP of any breach of tolerable risks. Risk tolerance can be expressed in absolute terms, e.g. 'The IORP will not accept a delay in investing contributions that exceeds x days" (BCBS 2019, p. 5).

Another indicator for the relevance of KRIs in the insurance business can be found in publications of actuarial organisations and insurance advisors, see for example Phelan et al. (2020).

Although the regulation has been clear about the need for KRIs for twenty years, implementation remains weak. Perhaps the increasing regulatory focus on the sustainability of businesses may serve as a reboot for KRIs. Note that, in certain areas, KRIs have never been in dispute. This applies typically to real-time systems such as system breaks, reconciliation breaks, IT-outages and other environments with instant, high frequency data updates. Much risk related data, however, is not high frequency, is not collected instantaneously, is not assessed consistently, is only loosely combined into indicators, and, more significantly, is rarely acted upon.

In this paper, we describe the current state of KRIs, the future for KRIs if no action is taken, followed by an ideal version of KRIs and, finally, five recommendations that serve as a start towards that ideal state.[1]

2. The current state of KRIs

A first indication of the use status of KRIs can be gleaned from official disclosures by FIs. Companies disclose risk information in reports, such as Pillar 3 Reports for banks and Solvency and Financial Condition Reports ("SFCR") for insurance companies. It should be noted that not all FIs publish their KRI usage consistently, or at all. The overview (Table 1) provides a cursory overview. Table 1 illustrates that, although KRIs are mentioned by some FIs, little or no detail is provided.

Table 1. Overview of use of KRS in selected FIs.

Financial Institution	Use of key risk indicators	Source
Allianz Group	Quarterly based on top risk assessment	SFCR 2019, p. 40–41
Phoenix Holdings	Development and monitoring in the context of the Actuarial Function	SFCR 2020, p. 79
Standard Life International DAC	Identification of potential issues and snapshot of risk exposure	SFCR 2020, p. 28
DZ Bank Instituts-gruppe	Usage of Risk indicators mentioned	Aufsichtsrechtlicher Risikobericht 2020, p. 182
ABN AMRO	Part of the Risk Assessment methodology	Pillar 3 Report 2020 p. 17
KBC	KRI used for risk identification	Annual Report, p 58
Erste Bank	No reference in financial statements or website	Financial Statements 2020, Offenlegungsbericht 2020
Barclays	KRIs used to monitor risk appetite	Barclays PLC Pillar 3 Report 2020, p 206

2.1. Some reasons for suboptimal KRI implementation

Although many FIs have implemented KRIs in the last two decades, our experience at more than 20 FIs across

all continents supports the notion that most implementations are half-hearted and not very successful. COVID-19 induced changes to work practises, as well as increasing data-driven processes reinforce the need for good risk management data. Now that staff and third parties are predominantly working from home, management cannot easily pick up on verbal and non-verbal signs and KRIs can play a more prominent role in management and decision making.

The reasons for the low success rate for KRIs to date are varied. Some of the most prominent are discussed below.

1. KRI-deployment is haphazard

KRIs serve both operational and strategic needs which are different in nature.

Operational KRIs support direct process steering. Examples are the ageing of open nostro account items, the availability of IT-systems, loads on IT-servers, detection of intersystem breaks, cash availability in ATMs, etc. A shared characteristic of these KRIs is their continuous, near time calculation allowing rapid reactions to threshold breaches. Take the risk of a collision when parking a car. Here, the beeping sound when coming near proximate objects serves as an excellent KRI. This excellence comes from the continuous, immediate feedback, allowing instantaneous mitigating actions, thus avoiding a collision. These operational KRIs are flourishing and are not the main subject of this paper.

Strategic KRIs are supposed to alert management to changes in the risk profile. Broadly speaking, the risk profile is determined based on risk analysis, typically comprising a combination of forward-looking scenario-analyses, the history of risk events and information based on risk and control assessments. Most of all, strategic KRIs are derived from a deep understanding of process weaknesses, product complexity and environmental threats that may jeopardise business objectives. Few FIs have the ability to effectively translate heterogeneous risk data into meaningful KRIs.

2. KRIs are not relevant for (day-to-day) management

KRIs are often assumed to belong to the domain of the ORM department as part of their risk framework. As a practical implication the risk function drafts a project plan, assign responsibilities and actions which business managers are expected to implement. No wonder then that business management are less than keen to adopt KRs as meaningful management information. Often, existing information such as KPIs are dressed up as KRIs although both are very different and should not be mixed up. Under such conditions, KRIs have little impact on management actions, let alone business decisions. The whole KRI programme degenerates into a compliance fig leaf and ends up wasting of time and effort, further undermining the whole concept of KRIs.

3. Not all stakeholders are actively involved in defining KRIs

Thresholds are a key element of KRIs and are not easy to define. They are an expression of the company's risk appetite and assume that appropriate action is taken when the risk exposure exceeds the risk appetite.

The question of what to do when thresholds are breached is rarely given much attention in (the design phase of) KRI programmes. It should be noted that the strategic risks measured by KRIs are of low frequency. It is important to note that the low frequency is not a flaw. As in the credit and market risk practice, the risks that can be characterised as (very) low frequency but unacceptable impact require close monitoring. In the realm of ORM, however, managers might not have experienced these risks. If the reaction time window and the potential effectiveness of actions is not the manager's scope, they will be disinclined to accept the associated thresholds as relevant. If they are set too tightly, breaches will be frequent and not taken seriously. This may explain why thresholds are often set to unreasonably high levels, leading to a situation where the "traffic light is always on green".

4. KRI collection relies on too many manual interventions

This point especially holds true for the strategic KRIs. Much of the data used to determine the KRI-values is manually captured, processed and interpreted. Composite KRIs are aggregated[2] at department or location level, which diffuses the direct relationship between the measurement and the required action. Consequently, the information comes in late, its value for business decision is questionable and the process becomes inefficient, if not irrelevant. As a result, management might be less interested in the resulting information.

5. KRI usage remains at very low levels

KRIs and other data driven approaches are necessary for proper risk management but do not play a major role in practice, just as with risk and control assessments, once the novelty of the programme wears off, so does the interest in the KRI programmes wane quickly. The importance of real time observations and targeted analytics tools for ORM is discussed in Eceiza et al.(2020), especially for the areas of anti-money laundering, fraud detection, third party risk, process quality and regulatory risks.

3. What happens if KRI usage continues as-is?

If the issues mentioned above are allowed to continue, the acceptance of strategic KRIs as an ORM instrument will suffer substantially. KRI usage is likely to decrease and organisations will reduce the effort put into strategic KRIs to a minimum or even abolish them.

After the 2008 financial crisis, regulators[3] have shifted their focus from operational to strategic KRIs. Strategic KRIs require executives and boards to focus on structural weaknesses which implies a longer time horizon than the typical operational KRIs provide. In situations of crisis, however, the main focus is on short term issues only. Furthermore, opportunities might be overlooked in the phase of firefighting which seeds the next set of problems. Regulatory focus is helpful to keep financial institutions managing the changes to their risk profiles properly.

The forward looking element of KRIs is crucial. The question to ask is: Does this KRI tell me anything about a change to the risk profile that requires action? For example, a KRI measuring staff overtime reflects past excess hours, but clearly reflects future issues as well too: if overtime limits are continually breached, a series of knock-on effects may be expected.

If KRIs (continue to) fail to contribute to better management, this is likely to lead to a waning interest in them. That in turn may undermine the role of risk management as an integral part of business management. Given the recent changes in the operational models in FIs due to the COVID-19 restrictions and the desire of the majority of companies to move in the direction of more remote work, it has become more important to establish a strong data driven risk monitoring framework. KRIs are an important part of such a framework.

4. What would an ideal system of KRIs look like?

As is clear from the previous sections, the development and implementation of a KRI programme is far from straightforward. In part, this is due to a range of practical issues, but it is also the result of a mix of expectations. There is nothing wrong with high expectations per se, and in this section we will outline what may be expected from a KRI programme in an ideal world. And although not all KRIs are created equal (note the distinction between operational and strategic KRIs), we can identify the ideal circumstances for a successful KRI programme. Five characteristics stand out.

Characteristic 1. A clear understanding of what is measured by the KRI

There are three types of strategic KRI measurements:

A. KRIs that measure the level of a well understood risk
B. KRIs that measure the change in the level of a well understood risk
C. Composite KRIs (combining several type A and type B KRIs)

The expectation that all KRIs are of type A has led to a simplistic approach adopting simplistic thresholds and effectively relegated KRIs to a system of simplistic gauges as if measuring risk is no more than a simple readout. The 'well understood' places some severe restrictions on the usual hand waving that defines many KRIs. Well understood means that the metric used operates in a simple domain where the characteristics of the process are well defined and changes can be picked up by the indicator in question.

There are plenty of risks that can be measured this way. They are typically operational gauges that are regularly used by any process owner who wants to know what is going on in their process.

However, risk management has a broader remit to include changes in the risk profile. Therefore, the risk monitoring system should be geared to detect changes in the internal and external environment affecting the risk level. Two elements are of special interest: changes in risk triggers (such as increased risk for cyber security breaches) or changes to risk exposures (such as a change in transactional volume).

KRIs of type C are a much less common sight, although a mature KRI programme should include them. A mature KRI-monitoring system requires both types.

Characteristic 2. A keenly awaited batch of new KRI information

The definition of an excellent KRI report is one that is keenly awaited, seriously studied and actively discussed and acted upon by both the business and the risk function. That this is possible is evidenced by reports that are produced in the wake of an ongoing crisis. During turbulent times, it is not uncommon to have daily and intraday updates. That is information people will appreciate. Information that is one day out, let alone one week or a month out is progressively useless. Let alone those pesky HR related KRIs that measure staff turnover since last quarter. That does not provide the 'stop the press' moment that KRI proponents claim to deliver.

Characteristic 3. KRIs that allow corrective action

A KRI that trails behind may still have some use provided it allows for some non-trivial action. Nobody expects a new raft of actions every day, but if KRIs are not leading to the occasional in-depth debate and action, then the efforts spent in collecting KRIs is wasted. Part of this problem lies in the design and expectations of KRIs. Too often, KRI breaches are expected to lead to immediate knee-jerk actions. That should only be expected in situations with a reasonably small reaction window. A KRI such as detecting the presence of a child on an airport baggage conveyor belt may trigger an emergency stop. But in most processes, such detection schemes are not labelled KRIs.

Having said that, in the absence of an immediate response, there is one action that is recommended for any KRI breach: "investigate". That is really it. If KRI breaches do not lead to either an immediate and well-understood simple remediation or a formal investigation, then the KRI is not worth collecting. One implication of this is that, ideally, the set up for such investigation actions is created as part of the longside creation of the KRI itself.

Characteristic 4. KRIs that are routinely collected

Although it takes effort to set up KRIs and to prepare the ground for action in the case of breaches, by far the biggest effort is spent in collecting data on KRIs, processing it, analysing it for first order and second order changes and ultimately reporting on it. For those reasons, ideal KRIs would be routinely collected, stored and reviewed. To be sure, special situations may warrant a temporary KRI collection, e.g. for a change project or a particularly hazardous situation, such as an IPO. Here also, the collection of KRI should be part of standard data collection and analysis.

Characteristic 5. KRIs that are deployed close to the decision makers

The closer the KRI information (both the collection and the analysis) is to the decision maker, the better the chances are that KRI data will be used for actual process management. If KRI data is collected and/or analysed by what is perceived as a third party (like the risk department) or on behalf of a third party (such as KRIs collected for an oversight body), the KRI is less likely to be used in the real world.

Some examples for KRIs matching the characteristics described above are:

- KRIs related to suspense accounts:
  - Amount related to open items in suspense accounts and the first order difference with the previous reporting period;
  - The number of suspense accounts and the first order derivative with the previous reporting period.
- IT-operations KRIs:
  - Freely available disk space and the first order derivative with the previous reporting period;
  - Number of security patches to be deployed;
  - Number of performance patches to be deployed;
  - A selection of alerts from Network traffic monitoring tools.

The examples mentioned above are examples of KRIs that are directly related to operations. They are highly relevant to manage risks and signal unintended errors, internal and external fraud, problems with systems availability, cybercrime and business discontinuity. Note that monitoring and action on these KRIs is a first line responsibility. The risk management function may be involved with cross referencing the KRIs with other risk data, with aggregation and reporting on appropriate follow up.

5. Some practical steps on the road to revitalised KRIs

Starting with the Basel II inclusion of KRIs in the ORM toolkit, many FIs have had a stab at formally introducing KRIs. Alongside the KRIs that always existed but weren't called that, a smörgåsbord of indicators has emerged, some of which are useful, some of which are useless and some of which are downright misleading. The section above outlined an ideal system of KRIs. This section addresses each of the five elements of the ideal system of KRIs and suggests how to get started along each dimension.

1. A clear understanding of what is measured by the KRI

Recommendation 1: Embellish the KRI with narrative and explain what it is good for. In addition to recording random statistics, be explicit about what the KRI measures. Note that we do not mean paraphrasing the input, but explaining the mechanism how this data helps manage a process or alert the owner to a developing situation. Here, more is more, because so often KRIs are collected without a good understanding what this particular KRI is good for.

2. A keenly awaited batch of new KRI information

Recommendation 2: Add ownership to the KRI. It makes a lot of sense to not only record KRI data but also to note who needs to receive this data and who has control over the process that it relates to. As a rule of thumb, if a KRI does not have an explicit owner, it is not worth recording.

3. KRIs that allow corrective action

Recommendation 3: Select an uncomplicated KRI. Many KRIs lead a mundane life without ever getting triggered. For the KRIs that do trigger action, nine out of ten times these actions are not spectacular. They are not unlike a timer on an oven, alerting the user of an increased risk of burning your dinner. That allows you to turn off the oven and save the day. Not everyone will equate that timer to a KRI, but it is.

4. KRIs that are routine collected

Recommendation 4: Reuse existing information to create the first set of KRIs. Nobody likes to spend time collecting useless information. A good way to start a KRI programme is therefore to use what is already available and put another spin on it. That creates more buy-in than requesting staff to collect additional information on top of the MIS and process data that is readily available.

5. KRIs that are deployed close to the decision makers

Recommendation 5: KRI programmes must be demand based. Since the best KRIs allow corrective action, are routinely collected/studied and are not complicated, the best way to get started is to ensure that the KRI programme does not run over multiple departments. Hence, the first line should be fully in charge of its KRI programme.

6. Conclusions

As outlined above, the distinction between operational and strategic KRIs is helpful to ensure focus of the various governance bodies in FI. This approach might improve the relevance for the readers and therefore keep them interested. The usage of KRIs will then be better embedded and the Boards and Risk Committees have a measurement tool to monitor the sustainability of the FI's business models which will ease the discussions with stakeholders, including regulators.

Considering the increasing constraints facing FIs (low or zero interest rate environments, lower margins, more substantial regulation and increased reputation risk), early warning signals become more and more important to enable Boards and (senior) management to take appropriate actions.

Further enhancement to operational and strategic KRIs must support hybrid operating models, including enhanced levels of outsourcing. KRIs will function as sensors in the business to raise the alarm when (strategic) objectives are in danger or stakeholder interests are endangered.

The authors argue that the establishment of strategic KRIs requires a dedicated effort, clearly aligning the FI's risk exposure to its risk appetite.

- **Dr. Gerrit Jan van den Brink RA** is owner of Risk Sigma GmbH, advising on risk management, ESG and data topics. He is lecturer at various Universities and Institutes in Germany and the Netherlands.
- **Drs. Marc Leipoldt** is Owner of Global Risk Advisory Services.

Acknowledgements

The authors want to thank the anonymous reviewers for their valuable comments and helpful recommendations.

Notes

1. Readers who would like references to academic papers, or at least a seminal article regarding KRI literature will be disappointed. No such corpus exists. The Institute of Operational Risk provides a decent overview of the theory and practice of KRIs (IOR 2010). Scattered references are made in various publications about the importance of KRIs, but they rarely exceed a few pages of examples.
2. Aggregation of KRIs is regularly promoted by various scorecard-like risk management systems. Due attention needs to be paid the various scales on which KRIs are measured and therefore aggregation often is only allowed over the status (e.g. red - amber - green zone) as the various values can only be aggregated according to the lowest scale which is the ordinal scale in most circumstances.
3. E.g. ECB 2018 (see https://www.bankingsupervision.europa.eu/press/pr/date/2018/html/ssm.pr180918/ssm.pr180918_FAQ.en.html).

References

- Algemeen Burgerlijk Pensioenfonds (2021) Actuele Financiële Informatie (30 november 2021). https://www.abp.nl/over-abp/financiele-situatie/actuele-financiele-situatie
- BCBS [Basel Committee on Banking Supervision] (1999) Consultative paper issued by the Basel Committee on Banking Supervision. Basel Committee Publications - A New Capital Adequacy Framework - Jun 1999.
- BCBS [Basel Committee on Banking Supervision] (2001) Consultative Document Operational Risk, Supporting Document to the New Basel Capital Accord. https://www.bis.org/publ/bcbsca07.pdf
- BCBS [Basel Committee on Banking Supervision] (2016) Consultative Document Standardised Measurement Approach for operational risk. https://www.bis.org/bcbs/publ/d355.pdf
- BCBS [Basel Committee on Banking Supervision] (2020) Consultative Document, Revisions to the principles for the sound management of operational risk. https://www.bis.org/bcbs/publ/d515.htm
- Chernobai AS, Rachev ST, Fabozzi FJ (2007) Operational Risk A Guide to Basel II Capital Requirements, Models and Analysis, John Wiley & Sons, Wiley Finance.
- DNB [De Nederlandsche Bank] (2019) General principles for the use of Artificial Intelligence in the financial sector. https://www.dnb.nl/media/voffsric/general-principles-for-the-use-of-artificial-intelligence-in-the-financial-sector.pdf
- DNB [De Nederlandsche Bank] (2021) DNB 2025, DNB Vision and Strategy, Working on trust in a rapidly changing world. https://www.dnb.nl/media/jeslcpxj/dnb2025-dnb-vision-and-strategy_tcm47-387985.pdf
- EBA [European Banking Authority] (2021a) Risk Dashboard, Q2 2021. https://www.eba.europa.eu/risk-analysis-and-data/risk-dashboard
- EBA [European Banking Authority] (2021b) Final Report, Guidelines on loan origination and monitoring. https://www.eba.europa.eu/regulation-and-policy/credit-risk/guidelines-on-loan-origination-and-monitoring

- Eceiza J, Kristensen I, Krivin D, Samandari H, White O (2020) The future of operational risk management in financial services. https://www.mckinsey.com/business-functions/risk-and-resilience/our-insights/the-future-of-operational-risk-management-in-financial-services
- EIOPA [European Insurance and Occupational Pensions Authority] (2019) Opinion on the supervision of the management of operational risks faced by IORPs. https://www.eiopa.europa.eu/document-library/opinion/opinion-supervision-of-management-of-operational-risks-faced-iorps_en
- European Parliament and European Council (2013) Capital Requirements Regulation (CRR): REGULATION (EU) No 575/2013 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 26 June 2013 on prudential requirements for credit institutions and investment firms and amending Regulation (EU) No 648/2012. https://www.eba.europa.eu/regulation-and-policy/single-rulebook/interactive-single-rulebook/601
- FSI [Financial Stability Institute] (2020) Covid-19 and operational resilience addressing financial institutions' operational challenges in a pandemic, FSI Brief No 2. https://www.bis.org/fsi/fsibriefs2.pdf
- Girling PX (2013) Operational Risk Management, A complete Guide to a Successful Operational Risk Framework, John Wiley & Sons, Wiley Finance. https://doi.org/10.1002/9781118755754
- Grüter M (2006) Management des operationellen Risikos in Banken, Fritz Knapp Verlag.
- Hoffman DG (2002) Managing Operational Risk: 20 Firmwide Best Practice Strategies, John Wiley & Sons, Wiley Finance.
- IOR [Institute of Operational Risk] (2010) Operational Risk Sound Practice Guidance Key Risk Indicators. http://www.ior-institute.org/public/IORKRIGuidanceNov2010.pdf
- Movshyn L (2005) Key Risk Indicators im Management operationeller Risiken, Bankakademie Verlag.
- Phelan E, Vosvenieks F, Cleeson C, Stack E, Maher G (2020) Design, Callibration & Reporting of effective Key Risk Indicators. Milliman Briefing Note, 2020. https://www.milliman.com/en/insight/design-calibration-reporting-of-effective-key-risk-indicators
- Van den Brink GJ (2008) Risikoaggregation in Kreditinstituten in Risikoaggregation in der Praxis, Springer Verlag. https://doi.org/10.1007/978-3-540-73250-1_11