Risk Management Association

Key Risk Indicators for Community Banks

Risk and assurance functions use Key Risk Indicators (KRIs) to track early signals of increasing risk exposure in various areas of the enterprise. This document, a companion piece to RMA Community Bank Risk Management: Key Elements of Board Reporting, will guide risk practitioners to create and enhance their risk monitoring program through insightful considerations of KRIs.

Advance your world.

Contents

CHAPTER 1

Overview of Good KRIs

KPIs vs. KRIs

Programs may use multiple indicators to track various outcomes. The two most common are key performance indicators (KPIs) and key risk indicators (KRIs). The terms are sometimes (incorrectly) used interchangeably; both have an important and distinct purpose.

While **KPIs** help organizations understand how well they are doing in relation to their strategic plans, **KRIs** help them understand the risks involved and the likelihood of not delivering good outcomes in the future. This means KRIs can be the reverse of KPIs.

KRIs are unwarranted predictors of unfavorable events that can adversely impact the bank. KRIs monitor changes in the levels of risk exposure and contribute to the early warning signs that enable organizations to report risks, prevent crises, and mitigate them in time.

Using a simple example of a call center, "the average time to answer a customer's call" may indicate the performance of the agents (KPI). Whereas "the total downtime," or the amount of time the call center is unable to answer calls during business hours, may indicate, among other risks, an increasing risk of poor customer service (KRI).

Leading vs. Lagging Metrics

Indicators can be **lagging**, which indicates how the business historically performed, or **leading**, which predicts future conditions. Where possible, practitioners should strive to find leading metrics, but leading indicators are harder to develop and measure because they are more abstract.

In the example of cybersecurity, "the average cost per security incident" is a lagging indicator because of its historical nature and may not comprehensively predict the likelihood or impact (cost) of a future security incident. Whereas the use of multiple metrics such as 1) "number of phishing emails," 2) "number of vulnerabilities with or without patch availabilities," and 3) "trends of cyberattacks at similar banks" may be combined to predict the likelihood and success of a future cyberattack at the bank.

In another example, exceeding the designed capacity of a process or technology may indicate if reputation and costly compliance issues will arise in the future. For instance, a loan review process is staffed to thoroughly review 50 new loans in a week, but a new low rate change results in 100 new loans. If the

expectation is to double capacity within the same period, then it is reasonable to surmise that elements could be overlooked, resulting in mistakes and errors. The impact may have regulatory compliance and customer experience issues in the following weeks, or even years.

'Smart' KRIs

To borrow Peter Drucker's management by objectives concept[1], risk practitioners should use the SMART methodology in KRI development to ensure their organizations can measure and monitor progress in mitigating risk. SMART KRIs are specific, measurable, actionable, relevant, and timely targets that provide a useful framework for evaluating the effectiveness of KRIs. Additionally, using SMART goals helps to ensure that the KRIs chosen are the most appropriate for achieving the desired outcomes. It also helps to ensure the KRIs are evaluated accurately and without bias or subjectivity. Furthermore, by setting goals according to SMART criteria, risk managers can measure both qualitative and quantitative aspects of their performance; this allows them to identify patterns and discrepancies more clearly over time within their KPIs, providing valuable insight into organizational risks. Finally, using SMART goals with KRIs encourages practicality as well as accountability—both help keep organizations aligned with their objectives when it comes to managing risk and achieving business goals.

- **S: Specific** – Linked to key activities, risks, or regulations (called "drivers") and enable monitoring and measurement of those drivers on a recurring basis.
- **M: Measurable** – Can ideally be quantified but should be reasonably measurable.
- **A: Actionable** – Should help management in making decisions and taking actions.
- **R: Relevant** – Associated to high-level, strategic goals or risks.
- **T: Timely** – Should provide early warning signals of approaching risks or gaps in preparedness.

1 Drucker, Peter, The Practice of Management, Harper, New York, 1954; Heinemann, London, 1955; revised edn, Butterworth-Heinemann, 2007

CHAPTER 2

Developing KRIs

Having KRIs is best practice, but it is not about having KRIs for the sake of having them. Practitioners should evaluate the best areas to invest their limited resources to get the best return, or in this case, the best insight. Beyond required regulatory compliance, which is out of scope in this document, there are several areas to consider and review to create a leading KRI program. They include:

1. Aligning **strategic objectives** and risks to identify underlying metrics;
2. Seeking recommendations from **stakeholders** such as risk owners to identify existing and potential metrics;
3. Conducting a **root-cause analysis** to broaden the perspectives of metrics, and then evaluating each;
4. Consulting **external data sources** to benchmark your list of metrics against leading practices; and
5. Developing **thresholds** to ensure action.

Strategic Corporate Objectives

Risk practitioners play an essential role in helping financial institutions achieve their corporate objectives. To do this, they must understand what those objectives are and how to measure and manage any potential risks associated with them. By creating KRIs, risk practitioners can help banking organizations identify and monitor critical risks that could affect the attainment of their objectives. KRIs should be tailored to specific organizational goals, considering both qualitative and quantitative factors, such as credit exposure and economic trends. Risk practitioners can also use KRIs to determine the potential severity of each risk and develop appropriate strategies for minimizing or eliminating them. Furthermore, these indicators can also be used to track performance over time, helping banking organizations continually review, adjust, and optimize their risk management practices. With the right amount of knowledge and expertise, risk practitioners can provide invaluable insight into corporate objectives for banks and other financial firms — making them more prepared for uncertain times ahead.

If using a system to track KRIs, consider tagging KRIs to a register of corporate objectives and key or critical processes for better reporting.

Stakeholders

Stakeholders in KRIs are individuals or groups who have an interest or action in the risks associated with a company's operations. These stakeholders can include board members, managers, employees, customers/community, regulators, and even third parties. They all have responsibilities related to KRIs as well as a vested interest in the success of the bank in managing its risks.

Overall, stakeholders involved with KRIs need to collaborate to assess any potential risks and ensure appropriate measures are taken to mitigate them. This could include implementing new policies or procedures, creating new systems for collecting data more efficiently, improving existing processes, or training employees on new technologies that can help detect risks earlier on. By involving all parties involved with KRIs, companies can better protect themselves against potential losses due to financial mismanagement or other unforeseen events.

If using a tool to collect KRI data submissions, consider these roles in the system. By identifying individuals instead of groups, practitioners may find better accountability.

- **Accountable Executive Leader.** Use divisional leaders to drive accountability of their teams and bring visibility to the risks within the division.
- **Business Owner.** Use the business unit leader to drive accountability of their team and bring visibility to the risks within the business unit or department.
- **Business Analyst.** Depending on the bank's resources, the business owner may not have the availability to submit multiple indicators. Instead, consider utilizing a subordinate to gather and submit data.
- **Risk/Compliance Analyst.** Consider tagging individuals within an assurance function who can track and trend KRIs and who can further consult in required actions.
- **Watcher(s).** There may be additional individuals who need to be informed of the trending KRIs.

Root-Cause Analysis

To narrow the focus, it is suggested to conduct a root-cause analysis of major risks or recent risk events to determine the best metrics to monitor. The most common approach is the "five whys" methodology. This is where a problem statement is agreed upon and a practitioner asks at least five "why" questions to gauge the likelihood of a particular risk.

For example, if the problem statement is, "there is a high likelihood of a cyberattack," perhaps the conversation goes like this:

Q1: Why is there is a high likelihood of a cyberattack?

A1: Because we lack significant information security.

Q2: Why do we lack significant information security?

A2: We have high turnover in the information security team.

Q3: Why do we have high turnover in that team?

A3: Reason A

Q4: Why does [reason A] occur?

A4: Reason B

Q5: Why does [reason B] occur?

A5: Response C

This exercise often will yield numerous answers throughout the various levels. Whereas A1 (above) is one response, perhaps an additional reason is because cyberattacks are increasing in frequency and complexity. This would lead the conversation in a different path. Practitioners should encourage these various paths and probe several root causes that can result in the risk being materialized.

Then, stakeholders should review the various root causes to determine the best metric(s) that meets the previously forementioned SMART methodology.

External Data Sources

External sources may provide the KRI/metrics program with more reliable metrics to track risks, but they can be hard to locate and may change methodology or stop updating or reporting without warning. There are vast free and paid services that can provide metrics such as credit ratings, environmental and carbon emissions reports, cybersecurity ratings, and many more. Practitioners should consider what data is more valuable to the program and stakeholders.

The most well-known and recent example of external data occurred during the beginning and height of the pandemic, where almost every company in the United States likely utilized Johns Hopkins University's COVID-19 Dashboard[2], the CDC's COVID Data Tracker[3], and state-level case rate statistics to determine the risk of an employee contracting and spreading COVID-19. While these reporting programs continue to be active as of this publication, programs that relied on the data likely saw changes in reporting methodology several times throughout the response, which is a cautionary tale of how external data may change abruptly.

2 COVID-19 Dashboard by the Center for Systems Science and Engineering (CSSE) at Johns Hopkins University (JHU): https://www.arcgis.com/apps/dashboards/bda7594740fd40299423467b48e9ecf6

3 Centers for Disease Control and Prevention COVID Data Tracker: https://covid.cdc.gov/covid-data-tracker/#datatracker-home

Creating Thresholds

Thresholds are an important part of KRIs, since they act as benchmarks that measure performance over time. They provide a clear and precise indicator of when a risk has reached an unacceptable level, thus allowing the business to take proactive steps to address and mitigate it. Preset actions are also important to be clear what is expected of leaders—just as a storm watch brings awareness of potential hazards and a storm warning encourages everyone to seek shelter.

Practitioners should not think of thresholds as a binary "good vs. bad" metric—although that approach may be acceptable to new or less mature programs. Instead, it is recommended to use a tiered approach to indicate, within tolerance, the ability to warn of any concerns, and when a concern exceeds the threshold and may require formal action. See Figure 1 as an example. The most common reporting structure is the "RAG" or Red/Amber/Green method, where green is nominal/expected, yellow is warning, and red is undesirable.

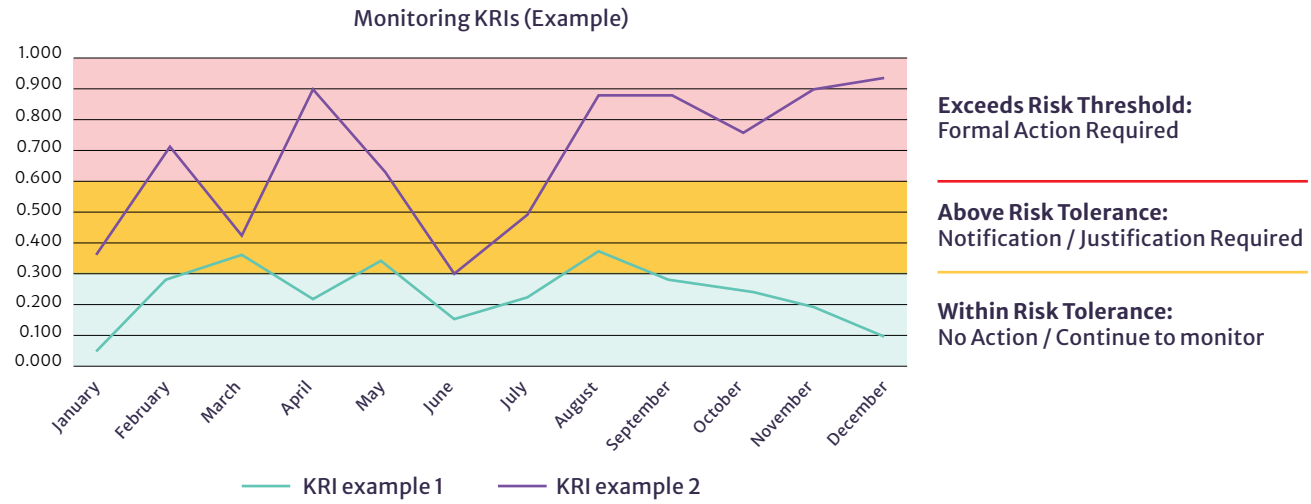

Figure 1

Creating the appropriate threshold and tolerance for KRIs is more art than science. It is up to each organization to determine its acceptance of the risk and when to involve and escalate other leaders. It is recommended to avoid using absolute values such as 0% or 100%. For example, for required compliance training, it is unlikely to get 100% of employees to take training due to factors like attrition or leaves of absence.

The creation of thresholds requires careful consideration regarding both the size and intensity of any given risk and the impact it may have on operations. Banks should also evaluate their industry sector to determine what is considered industry standard for thresholds in key risk indicators. Doing so will ensure risks can be effectively managed and opportunities seized to remain competitive in the current market climate.

Another consideration is the use of historical data to determine tolerances. Trend analysis of historical data can lead to better, more realistic threshold and tolerance levels. However, some risks have exponentially changed—a program wouldn't use cyberattacks from the 2000s to trend against attacks today. With climate change, inclement weather events of the past, both in frequency and impact, may not truly represent the occurrence and cost of future events. Additionally, society is seeing major shifts in the workforce and behaviors of individuals, which may impact future expectations.

CHAPTER 3

Evaluation and Optimization

As previously mentioned, KRIs are a valuable tool enabling organizations to identify, monitor, and respond to and anticipate current and future risk exposure levels. By regularly evaluating and optimizing these KRIs, banks can better understand their *current* risk profile in relation to their peers and the industry—and take steps toward mitigating the severity of those outcomes if they occur.

Identifying *Key* in KRIs

The challenge for most programs is usually not finding metrics or indicators—those are plentiful. The challenge is in determining the most succent, impactful, and reliable key risk indicators.

Developing key and leading KRIs can be a challenging and time-consuming endeavor, as ERM teams must interact with the business lines to identify existing metrics and construct an official process for capturing data. In addition, aggregating forward-looking risk indicators from multiple sources within the organization is necessary to develop enterprise level insights, making this activity even more complicated. Nevertheless, by dedicating resources toward careful analysis of these measures we can detect potential risk exposures before they occur, so your bank remains prepared for what may lie ahead.

A good practice to consider is combining multiple, non-key indicators at the department level into one or two key indicators that are shared at the leadership level.

Evaluation Factors

Evaluating KRIs should involve both qualitative and quantitative factors. Qualitatively, KRIs should be evaluated for relevance to the organization's current and future goals, whether they are timely and dependable enough to inform decision-making, and if any potential biases exist. Quantitatively, data collected through KRIs must be accurately captured and analyzed to provide meaningful insights. Practitioners should, among other things, consider the data's accuracy, precision, consistency, and validity when making decisions based on analytics derived from these indicators. Finally, all evaluations should be performed in alignment with existing industry standards or organizational policies and procedures.

Tactical questions to consider:

- **Drivers:** A driver is the reason a particular metric or KRI exists. Does the metric link to key activities, risks, or regulations? Is the driver still active and does the metric meet its requirements? If not, perhaps it should be updated or removed.
- **Impact and Influence:** Does the metric influence appropriate outcomes?
- **Metric Level:** While not all metrics need to reach every level in the organization, do the key metrics go to the appropriate audiences? Is too much or too little information being shared?
- **Cost:** What resources are required to continually track this metric? Is it a direct cost, such as paid access, or is it an indirect cost, such as staff time needed to gather, input, export, clean, or transmit the data? Is there a return on that investment?
- **Quantifiability:** What reliable data (internal or external) can this metric be benchmarked against? Are those sources still relevant and reliable?
- **Timing:** How delayed is the data, from the original source to the reporting, and how can that timeframe be shortened? Is there a more appropriate *leading* indicator instead of a *lagging* metric?

An evaluation of KRIs should occur on a regular, ongoing basis to ensure the bank's risk profile stays up to date—perhaps annually or every two years. The frequency of this evaluation will depend on the type of data and the stakeholders' capacity to review the data. Additionally, it is suggested to review KRIs when there are significant changes within an organization (such as reorganizations, mergers, or acquisitions, which may impact the goals or risks; or technology updates or changes, which may create new opportunities to mine new data); when regulations are introduced or changed; or when there are changes in market trends. It is best practice to track when a KRI was reviewed and who approved it.

Utopian Green

For those looking to mature their program, consider if excessive caution is being applied and determine how to better optimize resources. Depending on the type of metric, having a metric that is *always within the green threshold*, some practitioners may call this "utopian green," may not be the best use of resources.

On one hand, if a metric is utopian green, does the risk no longer impact the organization and does it still need to be reported to leadership? If the risk remains unchanged, is there a better use of time for those individual(s) collecting and reporting that metric? Are there better metrics that should instead be considered?

On the other hand, as risk managers, practitioners should manage both the downside and upside of risks and consider any lost opportunities being forfeited. Take the illustration of a bank that only considers borrowers with an exceptional credit score (estimated to be 21% of all consumers[4]) for a loan and where the number of defaulted loans—the KRI in this example—is nearly zero. It is great to avoid the financial costs of recovering a troubled loan, but it also limits potential customers to only one in five people. If that bank allowed borrowers with a "very good" credit rating and higher (estimated to be 46% of consumers[4], the bank may have a higher default risk, but the revenue from a higher volume of loans could easily cover those costs. This would result in more customers—nearly one in two people, potentially—being served.

Note, this approach may not be appropriate for certain metrics, such as compliance, which do require normalized results and consistent reporting.

4 Experian: https://www.experian.com/blogs/ask-experian/credit-education/score-basics/what-is-a-good-credit-score/

CHAPTER 4

KRI Technology

This document has referenced technology in previous sections. In an informal poll of RMA Community Bank Council members, all are using some type of technology to manage their KRI/reporting program. However, the sophistication of those technologies range from a simple email and spreadsheet, to the use of a single-point solution (or a technology specific to managing KRIs), and up to complete Governance/Compliance/Risk ("GRC") or Integrated Risk Management ("IRM") tools.

A tool does make the KRI process much easier to manage and report, but the cost of implementation and maintaining such a tool may be too large for a community bank to absorb. In any case, it is recommended practitioners utilize whatever technology is available to: 1) remind KRI business analysts (the submitters) when to submit the metrics; 2) ensure the business owner has sufficient ability to review or approve the submission or provide commentary when a submission exceeds thresholds; 3) notify the risk analyst that the submission is ready for review; 4) document and track submissions (or flag missing submissions for follow up); and 5) compile and report submissions (such as a graph) to management and stakeholders.

CHAPTER 5

Conclusion

Monitoring and reporting risks is an essential element of risk management in community banking. Risk practitioners must understand principal elements of KRIs to inform decisions and inspire actions of leadership and stakeholders.

About Risk Management Association (RMA)

Founded in 1914, the Risk Management Association is a not-for-profit, member-driven professional association whose sole purpose is to advance the use of sound risk management principles in the financial services industry, including the farm credit sector. RMA promotes an enterprise approach to risk management that focuses on credit risk, market risk, and operational risk. Headquartered in Philadelphia, Pennsylvania, RMA has 1,600+ institutional members that include banks of all sizes as well as nonbank financial institutions. They are represented in the Association by 41,000 individuals located throughout North America, Europe, Australia, and Asia/Pacific.

Guided by RMA's mission of advancing sound risk management principles, RMA brings financial institutions high-quality, cost-effective model risk management services delivered by a team of industry practitioners with more than 25 advanced degrees.