MILLIMAN BRIEFING NOTE

Design, Calibration & Reporting of Effective Key Risk Indicators

Eamonn Phelan, FSAI, CERA
Fred Vosvenieks, FIA, CERA
Cormac Gleeson, BAFS
Eóin Stack, BAFS
Gavin Maher, BAFS

Key Risk Indicators ("**KRIs**") form an essential part of the risk management toolkit. In this note, we discuss approaches to developing a robust suite of KRIs, and wider considerations for risk reporting.

The purpose of KRIs is to act as an early warning indicator that a company's risk profile may potentially deviate from its risk tolerance or risk limits in the future. KRIs should not be designed based on what is easily monitored, but rather on what is most useful and most meaningful. The primary purpose of a KRI is to inform stakeholders if there is a need for action to be taken.

In a "three-lines-of-defence" world, all three lines have a role to play from design of KRIs through to reporting and communication of results. When all three lines work together, organisations should be able to achieve a focussed and effective KRI framework, covering the key risk exposures and providing accurate and timely information to help maintain the risk profile in line with risk appetite. There is a particular need for good collaboration between the first and second lines in order to arrive at a shared view that the KRI framework can be a useful guide to the risk exposure, to get alignment on how the KRIs should be interpreted, to promote awareness of the circumstances in which a given KRI might cease to be a good risk indicator, and so on.

There are many considerations to bear in mind when developing KRIs. A higher-level, risk-focussed approach can help ensure the development of a robust suite of KRIs which can be communicated effectively, enabling proactive risk mitigation actions to be taken. By designing KRIs which focus on the underlying drivers of risk, rather than simply summarising the risks themselves, the risk monitoring framework will be forward-looking. This provides useful information about potential changes in risk exposures and enables management to take effective action in the light of early warning signs, rather than just providing a retrospective view.

Depending on the risk in question, a good suite of KRIs should be capable of signalling:

- the onset of a short-term / temporary spike in risk exposure;
- raised risk exposure or uncertainty over a specific period, e.g. market cycle, business planning period, etc.;
- permanent, long-term changes in risk profile.

This should then feed a discussion on frequency of reporting and the time period in question (e.g. daily/weekly/monthly movements), in order to arrive at a reporting framework which helps to identify changes in risk and any potential trends of interest.

The COVID-19 pandemic provides a unique case study in crisis monitoring and risk reporting. To date, developing and maintaining a suite of KRIs with relatively static metrics and associated limits has been common practice in the market. KRIs should remain aligned with the risk profile and risk appetite of an organisation; for some insurers, the COVID-19 pandemic may have materially impacted these, but have firms revisited the appropriateness of their KRIs?

In this paper we consider best practices around the development of a KRI suite, looking at considerations for design, calibration, and reporting

KRI Design

There are a number of potential methodologies to adopt when designing a suite of KRIs. In general, these can be separated into "Bottom-Up" and "Top-Down" approaches. A Bottom-Up approach will focus on the existing processes in place, and the current information available. This may be suitable for certain types of business, however it could lead to a risk of anchoring bias[1] and building a risk monitoring system on what is readily available, rather than targeting information that would be more informative and more useful for decision-making. There is also a risk in a Bottom-Up approach of over-leveraging existing first-line processes and re-purposing them, instead of designing independent risk management processes.

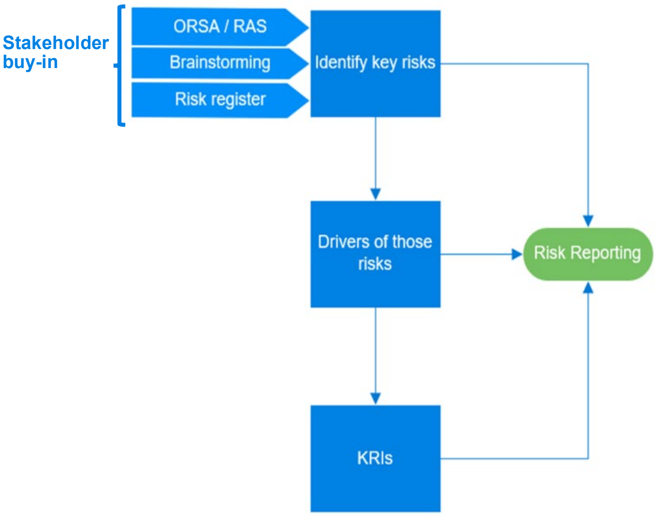
In contrast, a Top-Down approach (see Figure 1) focuses on risks at a high-level initially, and then drills down to better understand the underlying risk drivers. The practicalities of existing systems will still influence the design of the KRIs, but placing the emphasis on the core risks to the business at the

[1] Anchoring bias occurs when people rely too much on pre-existing information or the first information they find when making decisions. (https://corporatefinanceinstitute.com/resources/knowledge/trading-investing/anchoring-bias/)

outset of the design process should lead to a more effective set of KRIs.

The key risks can be identified using the Own Risk and Solvency Assessment ("**ORSA**"), with reference to the risk appetite statement ("**RAS**"). (The RAS typically comprises high level risk tolerances that are Board approved and hence gives some insight as to what is of most importance to the corporation from a risk perspective). The process can be conducted periodically to confirm if the KRIs that had been designed are still fit for purpose or if they need to be updated to reflect changes to the business or external environment.

FIGURE 1: TOP-DOWN DESIGN PROCESS



Stakeholder buy-in at this early stage is important as engaging with the various departments at each step in the design process will enhance the robustness of KRIs. Senior management and the risk function should be involved in the original determination of the risk appetite of the company, and any future revisions thereof. KRIs will then be linked to the risks included in this risk appetite. Senior management involvement will also ensure that KRIs are suitably aligned with the wider business strategy.

Understanding the risks

Once the core risks have been identified, the next step is to drill down and further understand the drivers of these risks. The purpose of the KRIs will be to monitor these risk drivers.

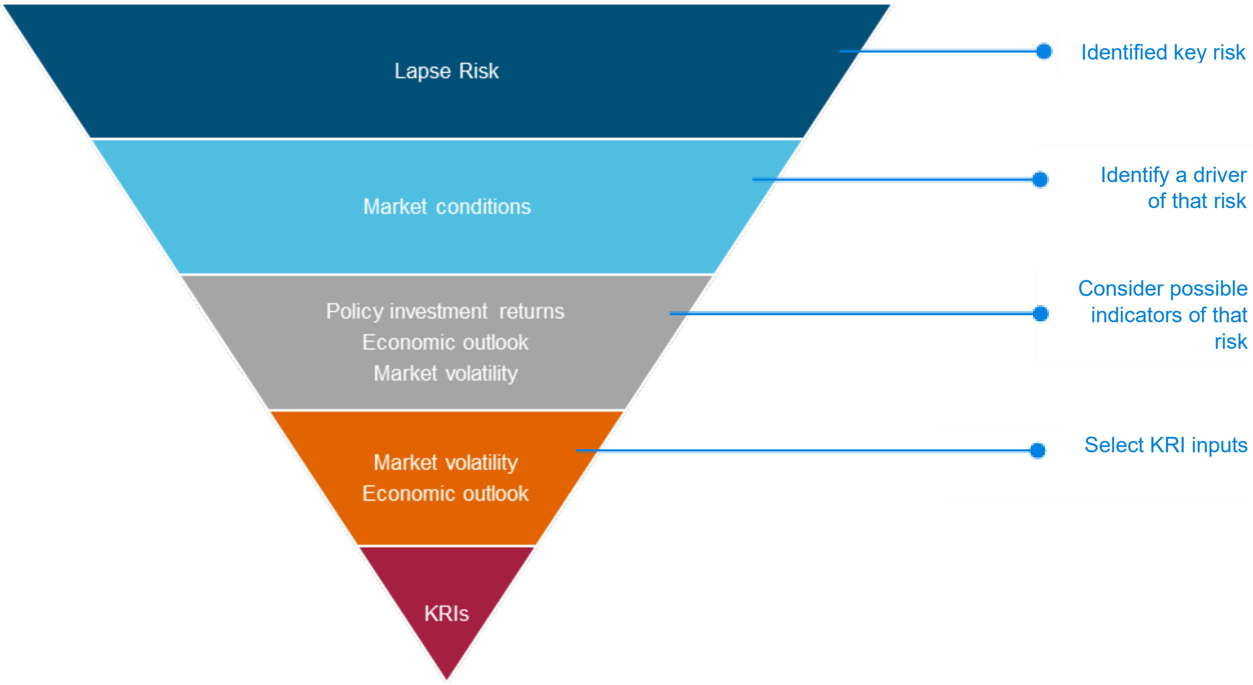
There can be many drivers for any one risk, and often these will vary by company. It is not practical to include a KRI for every underlying driver, nor is it effective as too many KRIs can lead to an onerous risk reporting process and ineffective communication. A "step-through" of each risk is an effective tool to prioritise risk drivers. An example for lapse risk on unit-linked business is shown in Figure 2:

- Identify the causal drivers associated with the risk, in terms of either increased likelihood and / or increased severity (e.g. market conditions);
- Shortlist the most material causal drivers from the full list of those identified;
- In turn, determine the specific feature or aspect of each causal driver that will be indicative of a potential change in risk exposure (e.g. market volatility, economic outlook, etc.);
- Choose the metric that will be used to monitor the risk driver (e.g. for relative competitor performance: fund return vs. average competitor fund return, ranking in top 10 performing funds, etc.).

The insight gained through drilling down and focussing on the key drivers which materially impact the ability of an organisation to achieve its business plan can be applied to other areas of the risk management framework. For example, quantifying the impact that these drivers have on performance could be used in a framework to continuously monitor solvency.

Additionally, the same information monitored by KRIs could inform the recovery indicators that are included as part of a Recovery and Resolution Plan.

FIGURE 2: LAPSE RISK STEP-THROUGH



Data sources

Traditional sources of data, such as internal operational data or market data should be easily accessible. However, more advanced techniques of data extraction can now be utilised to design KRIs around unstructured data, such as social media trends, counts of news articles on certain topics, or clicks on company websites. These techniques can also be used to develop softer, qualitative KRIs to complement quantitative metrics. For example, a KRI that is able to pick up information from news reports that mention, say, difficulties around the renewal of an OPEC deal on oil production levels, could trigger a proactive action to reduce exposure to assets sensitive to oil price movements, rather than only reacting once asset values have already become more volatile, as illustrated in Figure 3 below.

KRI Calibration

Individual risk levels

A red/amber/yellow/green (RAYG) system can be used to calibrate the risk limits of the KRIs. This ‘traffic-light’ system acts as a means of distinguishing the status of KRIs, for example:

- Green – Associated risk is in line with objectives and no action is required.
- Yellow – Warning that there is a chance of not meeting planned targets. Increased monitoring is required, as well as consideration of actions to mitigate risk.
- Amber – Execute actions to return to risk appetite or avoid a potential future breach in risk appetite, escalation of breach should be made to executive management and the risk committee.
- Red – Execute actions to return to risk appetite or avoid a potential future breach in risk appetite, escalation of breach to the Board.

This system of calibrating individual trigger levels can be connected to the risk appetite statement of the company if it also uses a similar scale. However, a status red KRI should not necessarily indicate a breach of risk appetite; instead it can indicate the need to take action promptly to avoid breaching the thresholds set in the risk appetite. It depends on the purpose of the KRI in question. In any case, alignment with risk appetite is critical.

The amber and/or red thresholds for each KRI should be set at a level that would trigger the company and its management to take action and consider changes to operations.

Some limits may also be “soft” in so much as they would act as a trigger for management discussion rather than specific management action as would be the case where limits are “hard”.

Companies regulated under Solvency II will need to provide a forward-looking view of solvency needs as part of their ORSA. Work related to forecasting capital requirement calculations can be used to help calibrate trigger levels indicating movements that result in solvency issues.

The calibrated thresholds could be of a quantitative nature, where warnings for further action are triggered if metrics fall either side of a certain numerical level. For example, numerical triggers for reputational risk, as in Figure 4.

FIGURE 3: RISK TIMELINE

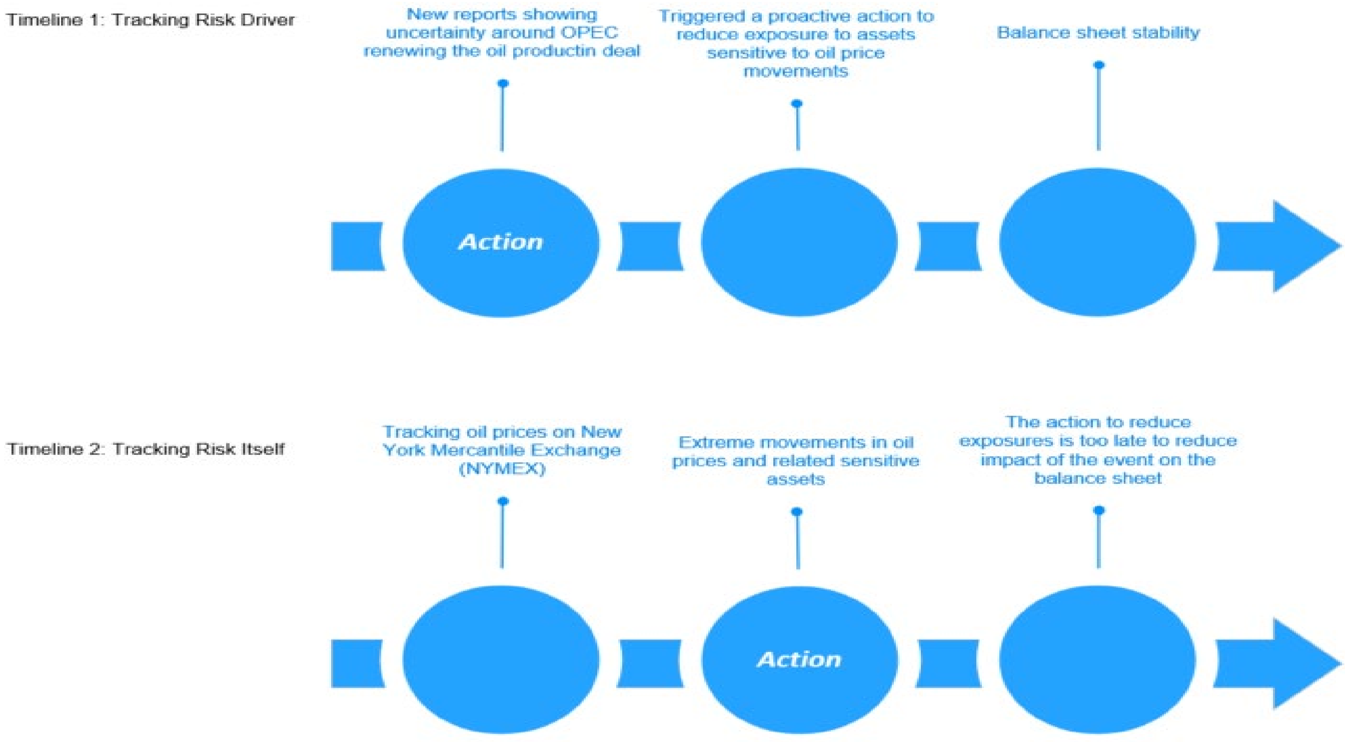

Timeline 1: Tracking Risk Driver
New reports showing uncertainty around OPEC renewing the oil productin deal
Triggered a proactive action to reduce exposure to assets sensitive to oil price movements
Balance sheet stability
Action
Timeline 2: Tracking Risk Itself
Tracking oil prices on New York Mercantile Exchange (NYMEX)
Extreme movements in oil prices and related sensitive assets
The action to reduce exposures is too late to reduce impact of the event on the balance sheet
Action

FIGURE 4: KRI TRIGGER POINTS

Number of negative coverage events during quarter	Red: > 2
	Amber: 2
	Yellow: 1
	Green: 0

Classification of these triggers may not be as clear if they are qualitative (see Figure 5). Calibrating threshold points in this way is more open to interpretation. For example, defining the status of a high loss event based on potential losses.

FIGURE 5: QUALITATIVE KRIs

Occurrence of high loss event reported in line with internal materiality	Red: Event escalated
	Amber: Event identified
	Yellow: Potential event
	Green: No event

For new KRIs, back testing is an important exercise to test the appropriateness of calibrated trigger levels. Walking through either historical or theoretical scenarios of adverse performance can help companies understand at what point the KRI thresholds would have been triggered. This is particularly pertinent with the outbreak of the COVID-19 pandemic. The company can use these scenarios to evaluate if the suite of KRIs would have provided a timely enough warning to trigger a risk mitigation strategy and may identify gaps in the KRI suite where threshold calibration may have been inappropriate. The exercise may also identify new indicators that would have alerted the company to the issue earlier.

In addition to the metrics themselves, there is benefit to running the KRIs through various "lenses" to reveal trends that are hard to spot. The data extraction referenced above can provide information metrics, which are adept at revealing:

- Whether the performance of a metric makes sense in the context of past behaviour;
- Whether a new metric adds new information that existing metrics do not contain already;
- Which metrics are informing others and therefore potentially indicating a causal relationship; and
- The proximity to a tipping point (i.e. a threshold which if passed would significantly change the company's operations and risk profile).

These additional lenses help to "make sense" of all the data that has been collected and help the user put the information into a meaningful context and enhance understanding of the related risk.

Risk aggregation calibration

Grouping KRIs by risk type or category can help develop an aggregated warning signal. This involves capturing the status of several related KRIs in a single combined metric. A higher-level view of the main risk categories could have linked calibrated triggers using a similar system to individual risks.

For instance, a small number of "yellow" triggers in isolation may not seem like a point of concern but if they are all within the same risk category, it should be flagged. For example, consider a company with four KRIs grouped under a category for liquidity risk as in Figure 6.

FIGURE 6: LIQUIDITY RISK KRIs

Liquidity Risk KRIs
1. % Assets Duration > 5 years
2. Tax assets as a % of own funds
3. Liquid shareholder assets
4. Liquidity ratio

An aggregated calibration could be driven by the status of each individual risk, as shown below in Figure 7.

FIGURE 7: AGGREGATIVE KRI TRIGGER POINTS

Aggregate view of Liquidity risk	Red: 4 Yellow KRIs
	Amber: 3 Yellow KRIs
	Yellow: 2 Yellow KRIs
	Green: 0 or 1 Yellow KRIs

Other combinations of individual KRI statuses could be used to calibrate aggregate triggers e.g. one red and two amber KRIs could give an aggregate red status. A further consideration could be to weight the contribution of each risk towards its overall KRI trigger given some may be more important contributors to the company's overall view of the risk.

A similar approach can be used to calibrate KRIs when aggregating by time horizon, rather than risk group (see Figure 8).

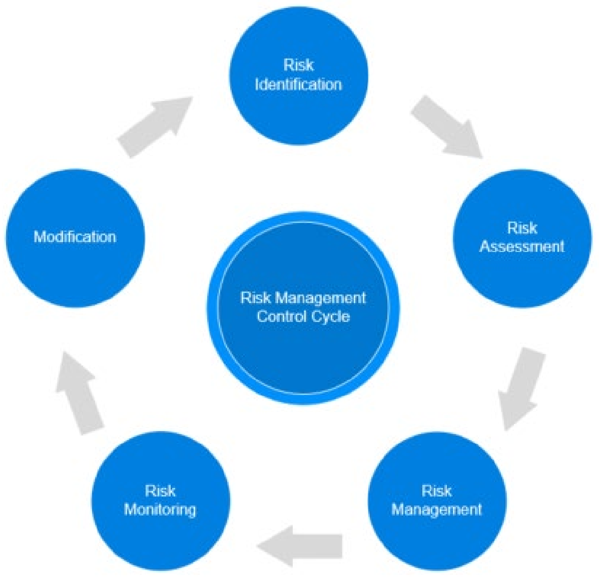
FIGURE 8: AGGREGATE KRI BY TIME HORIZON

Aggregate view of risks with short-term time horizons	Red: > 7 Yellow KRIs
	Amber: 3 – 6 Yellow KRIs
	Yellow: 2 or 3 Yellow KRIs
	Green: < 2 Amber KRIs

Recalibration of KRIs

Once a suite of KRIs has been designed and calibrated, if they are not revisited then initial KRI limits may become less relevant over time. Continuous monitoring and regular review can allow companies to recalibrate KRI thresholds and have a more dynamic view of risk (see Figure 9). Feedback loops are an essential part of the KRI design process. The review of KRIs should involve the first and second lines, and members of the executive team and possibly the Board, as various stakeholders will have different perspectives. This review would not only cover the risk profile of the company and the suite of KRIs in place, but also the calibration levels of these KRIs and whether the trigger levels are appropriately set for risk mitigation actions to be put in place.

FIGURE 9: RISK MANAGEMENT CONTROL CYCLE



In the event of a crisis or major change, it would be important to re-evaluate the effectiveness of current limits and be proactive in altering levels of tolerance before and after significant events. The recent increased market volatility arising as a result of COVID-19 provides a useful illustrative example. If a KRI has been set to be triggered by, for example, a 20% volatility increase, how could a company consider changing this level if it has already been breached when last evaluated? One possible approach would be to use a pre-defined "second level" of KRIs which had been prepared for crisis management. These would likely have lower thresholds in order to more effectively manage a crisis.

Other factors to consider when recalibrating KRIs over time or after an extreme event could include:

- Has policyholder behaviour changed?
- Has the nature of the risks the company is exposed to changed?
- Has the business mix of the company changed?
- Has the company operating model changed?
- Has the wider business environment changed?

Emerging risk KRIs

Although the potential impact from emerging risks are difficult to quantify, it is important to design tools for monitoring these risks as they can have a major impact on the company. KRIs should be brought into consideration when building a framework for the management of emerging risk.

Most of the considerations discussed above are also applicable when designing KRIs in respect of emerging risks. Additionally, two key points should be emphasised for emerging risk monitoring:

- Whether or not the risk will actually emerge (becoming a current risk) over a defined time period; and
- The organisation's exposure to that risk if it did emerge.

Designing indicators to quantitatively assess the impact of emerging risks to the business may prove difficult given the inherent uncertainty around these events. Qualitative KRIs can be a useful tool to assess and communicate the change in these emerging risks over time and help determine when an emerging risk should be integrated into the standard risk register. An example, of a KRI to track the status of a relevant emerging risk in the legislative process is highlighted in in Figure 10 below.

FIGURE 10: CLIMATE CHANGE LEGISLATION KRI

Status of climate change legislation	Legislation passed
	Legislation being drafted
	Lobbying stages

KRIs can also help reframe certain aspects of emerging risks. It is difficult to quantitatively report the likelihood of an emerging risk materialising, such as climate change or extreme weather events. Instead, KRIs can effectively communicate the impact to the business if these events were to occur. This may help address possible ambiguities or gaps in understanding of stakeholders.

Practical applications are discussed further in the paper "The cyber risk spend: How do you quantify the cost of cyber risk – and your return on investment?" by our colleagues Neil Cantle, Chris Harner, and Lisa Henderson. Here, KRIs and simulation techniques are used to evaluate distribution of loss outcomes to quantify financial costs of plausible cyber risk events.

KRI Reporting

As with any reporting, it is important to consider the potential audience of the final report. Therefore, different KRI reports may be created for different stakeholders depending on their needs. However, these reports should remain internally consistent; separate reports should not communicate different overall messages or be framed such that the KRIs are not interpreted consistently. The level of supporting commentary will also depend on the audience and their level of technical understanding. Communicating risk appropriately to various stakeholders is a key component of a risk management framework.

Specific reports should focus on communicating this information to first-line functions who will best understand the need for change and the practicalities of implementing any action plans. Technical understanding from senior management and the Board of Directors will not be needed to the same extent but it should be clear to them how the KRIs reported impact the company's view of risk at a high level, and the impact to the strategic objectives. Separate reports may also be prepared for different functions depending on their needs.

Risk dashboard

Preparation of a risk dashboard for risk reporting can be used to present KRIs and highlight changes from the previous periods.

Visual representation is important to convey appropriate messages and should be appropriate for all possible audiences. Using tables and graphs gives structure to the information while the coloured RAYG system can highlight points of concern. It is also particularly useful when showing changes in KRIs over time.

KRI monitoring and reporting may not be performed at the same frequency. For example, weekly evaluations could be carried out in line with other processes and then a more comprehensive report could be circulated quarterly. Those carrying out monitoring should be mindful of the need to produce ad-hoc reports for relevant stakeholders in the event of a severe breach in a KRI threshold, such as a red status.

"Everyday" risk reporting

One of the objectives of KRI reporting should be to aid the risk-owners in the first line. Reporting should identify KRIs as a starting point to encourage users to further investigate issues and drill-down into underlying operations.

Therefore, dynamic communication to the risk-owners is an important consideration in risk reporting. Being able to automate the production of key operational KRIs and to communicate them regularly, even daily, can greatly enhance the embedding of the risk management framework. Having engagement from the first line at the design stage will help ensure that KRIs are robust enough and fulfil the needs of the risk owners.

Reporting and monitoring should be coordinated between the first- and second-line functions. A synchronised approach should avoid, for example, the first and second line using different KRIs to monitor the same risk, or the second line function reporting on outdated KRIs in which actions have already been taken to resolve a breach in a threshold.

Action plan reporting

For KRI reports to add value, there is a need to communicate action points linked to the results. These actions should be required if a company believes a KRI will not return to a position within its risk appetite organically in a timely manner.

It would be beneficial to have a predetermined framework to evaluate how a company should react to changes in KRIs. For example:

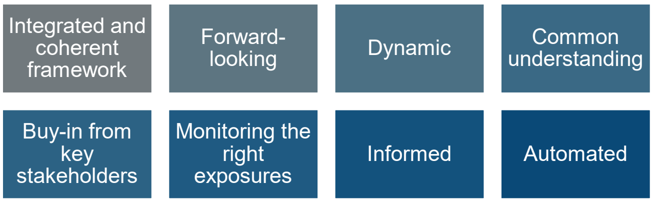
- What are the pre-defined actions for each trigger level?
- Are multiple actions needed to address a single KRI?
- Are there any considerations for aggregated KRI results?
- What are the costs and benefits of proposed actions?
- Is the change idiosyncratic or systemic? If the former is the case, what particular aspect of the organisation has led to this change in a KRI status? If the latter is the case, how are competitors and the wider industry likely to respond?

The KRI reports should provide an update on the status of any actions that had previously been taken as a result of a KRI breaching a threshold or showing a trend towards a threshold. This can then be used as part of the feedback loop.

Conclusion

The details in this note discuss important considerations for building and maintaining a suite of KRIs. The processes discussed for the design, calibration and reporting of KRIs can benefit a company's ability to monitor uncertainty and ultimately, better understand how to manage their risk profile. The characteristics of an effective KRI framework are summarised briefly in Figure 11 below.

FIGURE 11: CHARACTERISTICS OF AN EFFECTIVE KRI FRAMEWORK


Integrated and coherent framework
Forward-looking
Dynamic
Common understanding
Buy-in from key stakeholders
Monitoring the right exposures
Informed
Automated

How can Milliman help?

Milliman can assist you with all aspects of your risk management projects including advice on:

- Financial risk management
- Analytics
- CRO and outsourced risk support
- Cyber risk
- Enterprise risk management
- Operational risk management
- ORSA
- Recovery and resolution
- Reinsurance

For further information, please contact your usual Milliman consultant or those below.

Milliman

Milliman is among the world's largest providers of actuarial and related products and services. The firm has consulting practices in life insurance and financial services, property & casualty insurance, healthcare, and employee benefits. Founded in 1947, Milliman is an independent firm with offices in major cities around the globe.

milliman.com

CONTACT

Eamonn Phelan
eamonn.phelan@milliman.com

Fred Vosvenieks
fred.vosvenieks@milliman.com