MetricStream

Integrating KRI frameworks into risk assessments

Key risk indicators (KRIs) are critical predictors of unfavourable events that can adversely impact organisations. They monitor changes in the levels of risk exposure and contribute to the early warning signs that enable organisations to report and accurately assess risks, prevent crises and mitigate them in time. In a webinar convened by *Operational Risk* and sponsored by MetricStream, our panel discusses how integration of KRI frameworks into risk assessments acts as a metric of change in an organisation's risk profile

To facilitate the review and assessment process of KRIs, one needs an in-depth understanding of risks that will enable proper identification, establish appropriate risk indicators and monitor performance consistently, while leveraging technology to assist this process. Given the advances made by technology today, it is imperative to leverage it to look at different indicators in the context of risk data being collated for an organisation. Technology enables the measurement of different risk categories, metrics and even occurrences.

Operational Risk: What are the most common mistakes that financial companies tend to make when they're selecting and using KRIs?

Ann Rodriguez: Financial services have been talking about KRIs for over a decade, really touting them as the future of predictive risk management.

So far they haven't lived up to expectations, but I think that is, in large part, due to the overall maturity of enterprise risk management (ERM). If you fast-forward to today – where we have definitely advanced enterprise risk and have a lot of the basic elements in place within financial services – some of the challenges we see are more implementation-oriented.

I think a couple of big ones would be, first, failing to align KRI selection to the big picture – business strategy, risk appetite and the key risks that could impact the organisation – and, second, the human element; there is a whole range of biases that human beings bring to the mix when they discuss and consider information.

Monica Quintela: When implementing a programme for indicators you need to ensure that you give it enough time for the indicators to mature and to be able to calibrate results. You need to have at least six months of calibration for the indicators to really tell you what is happening and for you to be able to take the right actions once you have the measure.

THE PANEL

Brenda Boultwood, Senior Vice President of Industry Solutions, MetricStream
Monica Quintela, Executive Vice President, Director of Operational Risk, BBVA USA
Ann Rodriguez, Head of Enterprise Risk Governance, GE Capital
Kenneth Wainwright, Senior Audit Manager, EMEA, Citi

Kenneth Wainwright: It's important that the KRIs that you have actually link to strategy, to appetite, and that they're broad enough to reflect all the key risks that you're actually running. A lot of the time it's a function of seeing a lot of quantity but not necessarily quality. So, it's really trying to pick out the risk indicators that are truly key and truly representative of the risks that you are running from a business-wide perspective.

Brenda Boultwood KRIs are just a form of metric. We've had metrics to measure operations and efficiency, to measure our progress and change management and to measure the degree of compliance, for example. Also, like in the IT world, we have metrics that measure production stability, the degree of security or the threats and vulnerabilities we face.

What we're talking about here are risk metrics, and it is relatively less mature; it's a newer 'flavour' of metric, if you will. I think it leads to the biggest misuse, which is really when the business unit doesn't agree or doesn't adopt the metric that the risk function is using to monitor the risk level. The metric – in this case the KRI – may be used by risk but not by the business unit.

Then I think you often have big differences that emerge in expectations and how risk tries to apply the metric – a KRI, for example, in measuring risk appetite, or a scorecard approach to operational risk capital, or even as we try to relate it to our risk assessment process. Those are two main issues I'd highlight around using risk metrics at this stage in our development of an ERM programme.

Operational Risk: What are the best ways to get buy-in – to get the KRIs that you're producing actually used by the people who should be using them?

Ann Rodriguez: I think the concept of getting buy-in is really critical for the implementation of the KRI programme; it's foundational. You have to begin the process by getting the support and engagement throughout the organisation. It begins with a top-down mandate on the programme and the effort itself, the vision for that, but it has to be something that can permeate the organisation.

It's time-consuming; it takes a lot in terms of education on the value proposition, what folks can expect to see in terms of the collection and usage. This is just a very time-consuming but very critical first step in the implementation process.

Kenneth Wainwright: There is a lot of quantification, so a lot of metrics are produced, but sometimes we forget about the communication that sits behind that. It's about communicating what is key, as opposed to communicating what is everything, ensuring that what we are communicating is aligned to what are genuinely the key risks of the organisation. Also that it is meaningful in terms of strategic business direction and risk appetite, and ensuring that the data that is presented provides more information and is succinct enough to be impactful. You can use dashboards; you can use graphical representations to convey the message. More work needs to go into the presentation of the message than into developing more and more metrics.

Monica Quintela: How to present is very important. Also, buy-in is very important, mostly because if the business does not buy into the concept, into the metrics, into what you're trying to see from the risk perspective, then they're going to fail to take actions. If they haven't bought into the risk measures, they will probably not buy in to the action that they need to take.

Brenda Boultwood: I'd add that, in an area like market risk – and I'll pick on this area just because that was my background – you have a relatively simple set of metrics. It might be about your net positions, your sensitivities or maybe a value-at-risk measure, but there might be three or four metrics that you regularly use to tell the story when you're communicating to the board or senior management. But, when we're talking about ERM or particularly focused on operational risk management, the key to communication is really picking the story you're trying to tell. With operational risk, we know it's everything outside of market and credit risk, so it is big. It might be about an external event; it could be about a large loss that has been registered either by a peer or at the company. The metrics that you use need to be related to the story you're telling, and it needs to be convincing.

And the other part of it would be repetition – the board or management gets more comfortable the more they see the metrics being used. In operational risk we're still trying to refine things, and so there's experimentation and metrics can change – more so than in market or credit risk – where a steady set of metrics are used. That works against us, but I think we can be successful if we're clear about the story we're telling and we have buy-in from our peers on the management group.

Brenda Boultwood

Operational Risk: Are there any good ways to build up this kind of authority that you're going to need to engender that kind of trust?

Brenda Boultwood: One of the interesting practices I've seen a few financial institutions use is what some people call a 'sandbox'. It's creating a safe place where experimentation can occur and where businesspeople and other functional groups can see the value of the metric that is, for example, being proposed for measuring a certain people, process or system risk. In a sandbox environment, that metric might be part of an internal discussion but doesn't get reported to senior management or the board until it has been in the sandbox for a certain amount of time and there's a certain degree of acceptance through your governance forums.

That's one example of something that helps in the socialisation process – gaining that acceptance so we do have agreement when we're telling our story, after a loss event or when we're trying to explain something that has happened to our enterprise risk profile.

Ann Rodriguez: I think having an enterprise team to provide the co-ordination and ensure all of the voices are heard across the various stakeholders within the organisation. That goes for not only defining the KRI but resetting thresholds and, ultimately, how the ultimate message appears at the various levels at which we report KRI information.

There is a whole lot of process and governance that has to go into that. It also has to go at a quick pace and with the recognition that there needs to be an authority that says "this is what is going to the board" or "this is what is going to senior management."

Kenneth Wainwright: From an audit perspective it's quite an interesting one, because one of the things I would look for is that senior management – when they're engaging in the debate, and are debating the impact and the risk rather than the data itself, when they're debating the risk and that the metrics you are using are more meaningful. When you see debate of the metric itself, then it challenges the overall credibility of that KRI process.

Operational Risk: One of the big traps about the modern op risk and enterprise risk environment is that you have a huge technological advantage. You can collect vast amounts of management information but, equally, that presents the temptation to measure 350 different KRIs at once and becoming swamped with the results. Alongside that, you can also measure them in real time, or much closer to real time than would have been possible even a few years ago. How serious are these problems, and how can you address them?

Kenneth Wainwright: It goes back to the statistical concept of parsimony. You're trying to identify the metrics that move the dial. What you don't want to do is generate a lot of metrics just for the sake of generating those metrics.

A key test for me would be to say "you have this suite of KRIs", be they 60, 100 or 300, "show me how those KRIs would have identified previous losses or previous breaches of compliance or would have helped previous risk incidents be escalated more quickly. Show me in reality how the suite of KRIs on which you are focusing is actually explaining your risk profile and prompting management action". It's a back-test view of the world you can use to make sure you're not just generating metrics for the sake of generating metrics.

It's an imperfect science but, if you look at it through that lens, it does help you drive a more succinct set of metrics. It also then helps you position the message that you're trying to convey to senior management.

Ann Rodriguez

Monica Quintela: Yes, one important point here in order to avoid drowning in data is that we focus on the most important things, on the critical ones. Every institution should know where the critical risks are that they want to monitor on an ongoing basis. If you don't have that vision, then you're going to be drowning in data today because the data access is incredible like never before.

Then, obviously, you can put data together very fast. If you lose sight of the main critical risks that you want to focus on, then you're going to have a problem.

Ann Rodriguez: I would add that there are multiple layers of KRIs within an organisation, or just metrics within an organisation. They have varying degrees of importance, depending on your perspective.

We need a way of scorecarding the relative attributes of each of our KRIs, to make sure that we have a defendable way of showing why we have chosen to represent as key the final sets that are appearing on a management report. The attributes can be anything from "does it relate to a strategic objective?" to "is it something we collect in real time? Can we measure it now? Is the primary usage for risk?" There is a whole suite of those that we can grade out to say: "this is a metric that is very important to our organisation".

Operational Risk: How good are the users of KRIs? How good are operational risk managers and enterprise managers in general at moving beyond a kind of threshold approach, where a KRI is either green or it's red, and moving to a more gradated approach where you get a lot more insight from each KRI into what the actual state of play is?

Brenda Boultwood: I've seen this vary quite a bit by organisation. For example, in the IT organisation there is a pretty clear understanding, typically, of the critical or primary metrics and KRIs that are used. For example, if you're trying to measure vulnerability of your network or security access control violations, there are pretty clear metrics that are employed that actually can trigger the response time requirement – "this issue needs to be closed out in four seconds", or "we have a day to resolve this" – and also can be used to trigger the type of action plan that has to occur as a result of threshold violation.

While IT can report a lot of their metrics as red, yellow or green when they're communicating to senior management – for example, the production stability issues they have had or the vulnerability threats that they have experienced and perhaps mitigated – they also go beyond that in terms of using the metric and the degree of how far it's over a threshold, or just the fact that it's over a threshold, to trigger actions or trigger a timeline for resolution.

Kenneth Wainwright

That is based on their understanding the appetite around criticality and how exposed the network can be or how many data access control errors they are willing to tolerate. This has been practised and refined over many years. I think other areas like people metrics and the ability "what are we going to do if someone hasn't completed the required training?" or "what are we going to do if we have more than X per cent of our employees that are new hires within the last three months working on some business process?"

The required actions or the criticality of the response, such as, "how much time do we have to respond?" is less defined and is maybe less consistent because we're dealing with human beings. We'll never be as calibrated, if you will, as some of the IT metrics I was just talking about. Perhaps we have to accept that the degree of calibration in our ability to move beyond red, yellow, green, for example, perhaps depends on the type of metric and how much we are going to invest in our responses.

Ann Rodriguez: From a calibration perspective, the thresholds do have an implicit notion of risk tolerance. That is something that is fluid over time as well. It is often supported by the back-testing process so that, as you see things change or go wrong within your environment – either from a tolerance or from an actual event – those things form a feedback loop and help provide more insight as to how these thresholds should be set and what actions should be taken associated with those thresholds.

Kenneth Wainwright: Coming at it from a review perspective, key questions for me are: how does it link to risk appetite? How do you know when it's too much risk? And the fundamental question: when does it start to matter?

I don't think you can get away from the judgement issue completely. That's the sort of thing that I would focus on when I'm looking at how well constructed these KRIs are. Are you able to look at all that data and really determine when it starts to matter?

Operational Risk: Ann, you said that one of the biggest sources of error that you had seen was the human element, specifically bias. Can you expand on that?

Ann Rodriguez: Human beings are generally programmed to feel overconfident. That's a bias. People would rather leave things as they are, so they have a bias to be averse to loss or they may be less concerned about the prospect of gain. All of these things factor in, and there's a whole suite of these types of biases that can have an impact when you're considering both the threshold-setting process and the actual interpretation. There's anchoring, where the first time you see a bit of information you tend to rely heavily on it so advises all future decisions and perspectives. Confirmation bias is where we tend to favour information that aligns with our own preconceptions. That's a big one when we're trying to tell a risk story. I call them 'social challenges'. They can also come into play when you're also starting up a programme, because it will change the way people put forward KRIs to begin with. If they have a blind spot, it permeates the entire programme.

Operational Risk: There is going to be an unconscious tendency for people to suggest KRIs that will show that they're doing things well.

Ann Rodriguez: Exactly.

Brenda Boultwood: Those social challenges aggregate and lead to a culture within a company. It's interesting seeing different cultures at work around how they're going to use risk metrics. For example, there are companies that really want to quantify everything. So, when we're talking about a risk assessment they want to have metrics linked to each of their risk factors so they could automate scoring of their inherent risks. They would like to have key control indicators (KCIs) linked to each of their controls so they could take the results of control-testing results and the control metrics, KCIs, and use them to automate the scoring of, for example, the control effectiveness – operational as well as design effectiveness – to automate the whole process of getting to a residual risk level.

Monica Quintela

Other companies are saying this is something they can't fully automate or that they may be able to partially automate, but would never replace human judgement. A big misuse of KRIs, in my view, is not finding the appropriate balance between full automation and judgement, and how important that is if you're completing a risk assessment or if you're trying to explain a large risk event that has happened.

Those social challenges can lead to, ultimately, cultural biases that can really impact the whole set of goals you're trying to achieve for your ERM programme, and the metrics in particular.

Monica Quintela: This is another illustration of the importance of having an independent group looking into the metrics that we want to relay to management and how, because that will take away the bias of the business in trying to not show what is happening.

Ann Rodriguez: There are ways around this. A lot of it is process and awareness. It's just having enough thoughtfulness about what you're doing to avoid quick, impulsive interpretations of the information. To leverage the data wherever possible in a repeatable way, to have that independence and that independent function that challenges the ongoing interpretation of the information, but all the while supporting that broad engagement of people around an outside of the process or situation that you're trying to look at.

The other thing I would say is just trying to make sure that, as you're engaging with folks in the organisation, you avoid that 'star status' and 'groupthink' when collecting those different perspectives.

Kenneth Wainwright: I would say this is a common theme in all institutions. It's a very difficult one to deal with because, fundamentally, it comes down to people, it comes down to culture. It comes down to whether people are comfortable shining the light on themselves, and not that many are.

Having some sort of independent oversight of these different KRIs and how they are used is quite valuable – not in the sense of policing it as much as ensuring that they are, let's say, objective and that they're fairly reported and things aren't hidden. When things start to get hidden, then your risk profile automatically increases and you're in a bad place.

Operational Risk: How do KRIs mesh with other sources of management information when you're trying to paint this overall enterprise-level picture for the benefit of senior management?

Brenda Boultwood: In terms of an operational risk programme, you think about four major data components. These would be: your loss events or, more broadly, your risk events; your risk assessments; the KRIs or control indicators, other metrics that you're collecting. The fourth component is the scenario analysis and being able to go beyond, having confidence, business buy-in in all four components of the data that forms an operational risk management programme so that you can go beyond just a loss distribution approach to capital modelling or risk appetite statements that is solely based on metrics. Maybe risk appetite based on a combination of metrics.

You also need to consider loss events or loss tolerances, and levels of residual risk so that you can get a variety of ways of expressing that risk appetite. Then going back to capital modelling, then having confidence in the more subjective business environment and internal control factors that have more of a scorecard approach, so that individuals within the company – within the risk function, the business, and management – can be reassured that there is a statistically driven capital level that you're comfortable with. Also, there might be subjective environmental and internal control factors that you are also using to calibrate that level of capital.

It's a dangerous thing to try to do with regulators as they watch how you're doing this, but it's something that can only be done if the people within the company – within risk, the business and management –have confidence in all four components of the operational risk data that has been collected.

It is important to think about KRIs as just one of several categories of information. Management and the business have to have the same degree of confidence in the quality of this information as they would in a risk assessment or in the quality of the loss events that are captured, internal and external to the company.

Ann Rodriguez: That the KRIs provide input into all the other elements, particularly risk assessment and risk appetite. They provide perspective as you go through processes to look at all of those things, but they also take input from those things. If there are changes in the risk assessment, if there are changes in the business environment and you have to look again at your KRIs based on those things to see whether or not you've got the right KRIs still, if you need new [thresholds], if you need to modify or change the thresholds, I think it all works together, to the point where KRIs might appear on a report. Then all of the other aspects of risk assessment, changes in the business environment, changes in strategy or changes in the appetite all provide an additional context to the messaging that appears.

Kenneth Wainwright: I would say it is essential to have everything linked up and nothing in isolation. So, you have to show how KRIs go back to your risk appetite, even through to scenario analysis, back to risk assessment and how you use that integrated risk management framework to manage a risk profile.

Monica Quintela: The four components are very important, but I think KRIs add value by allowing us to have a more dynamic risk assessment, because usually what happens is that the risk assessments are very static. They're done, maybe, on a quarterly basis. KRIs give us the opportunity to have a really live risk assessment.

>> Listen to the full proceedings of the webinar *Integrating KRI frameworks into risk assessments* at *www.risk.net/2438672*