KRM22

Digitize Your Risk Register

KRM22 Whitepaper

Document Type: Thought Leadership
Prepared by: Andrew Smart
Date: 21 August 2020

CONTENTS

INTRODUCTION

Capital Markets and other financial services firms have spent many years talking about, and in some cases, implementing 'digital transformation' initiatives.

These initiatives are the result of the convergence of several trends;

- Increased speed and penetration of the Internet
- Increased in capability and penetration of powerful connected smart devices
- Changes in customer and employee expectations
- Technology innovation, mainly related to Big Data and Analytics, enabling more to be done for less, faster.
- Meet regulatory expectations, who want to see fewer manual processes and greater transparency and accountability within firms

Digital transformations promise to drive increase efficiencies, greater operational agility and cut operating costs.

While these initiatives have impacted many areas across firms, risk management often lags in terms of digitisation and automation is. This is particularly true of non-financial risk disciplines such as operational, technology and enterprise risk management.

Within these risk disciplines, one of the most widely used risk tools is risk registers. A risk register is a repository for all Firm's risks; documenting the nature, ownership and type of risk. Typically, risk registers contain related internal controls, other risk mitigations and a RAG status for each risk. The colour-coded RAG status is generally based on risk severity, calculated on the impact and probability of the risk occurring.

Maintaining and updating the RAG status is typically done via the Risk and Control Self-assessment (RCSA) process, often undertaken on a monthly or quarterly basis.

During the RCSA process, 'risk owners' review their risks and controls to determine if the RAG status reflects the current level of risk and control effectiveness.

The RCSA process is a key input into regularly monthly risk reporting to a risk committee, executive management meeting or similar. Often the central document within this type of risk reporting pack is a risk heatmap, typically showing the top 10 or top 20 risks.

Alongside the risk register, over time, some firms extend their risk framework to include

- capturing risk events (also known as risk incidents),
- tracking key risk indicators (KRIs), key control indicators (KCIs),
- tracking projects and tasks to mitigate risks and improving effectiveness.

These three core aspects of risk management,

1) Maintaining a single repository of risks and controls
2) Managing the Risk and Control Self-assessment process (RCSA)
3) Risk reporting

are ripe for a digital transformation as they are typically supported by an array of ad hoc, spreadsheet-based tools or previous generation compliance-driven risk tools.

As spreadsheets are available to everyone, easy to use and appear to be 'free', using them to support risk management activities is understandable; however, it is far from the best way forward.

Taking a spreadsheet-based approach adds cost and complex without promoting the right culture around risk management. It does not generate the information and insights to enable better risk-based decision making and hence drive better business results.

PROBLEM

Whether it is creating risk registers, delivering the RCSA process or generating risk reports, within many firms, spreadsheets are the 'go-to' tool accompanied by email and lots of chaser phone calls. All this manual work is done to ensure risks and controls are assessed on time, events are captured and consolidated, and reports prepared in time for the next risk committee meeting, executive or board risk report.

> *"I waste a lot of time in outlook, digging through 100's of emails trying to understand what events we are currently dealing with and the status of each event. I wake up every day, open outlook and wait to be punched in the face by the next risk event"* ***Managing Director, Front Office/Trading***

This widespread use of spreadsheets is problematic for four key reasons;

1. Spreadsheets are error-prone and can increase operational risk
2. Too manual, too slow and too unresponsive to support strategic and operational decision-making
3. Does not encourage the right risk culture or establish clear accountabilities for risk
4. Adds 20% - 30% to the operating cost of the risk team.

Spreadsheets are error-prone and can increase operational risk

Using a spreadsheet to capture and hold your Firm's risk register and enable risk assessments to be undertaken within the business, may deliver, or appear to deliver, short-term value; however, it comes with several costs and constraints.

The main costs are often those hidden costs that come with manual, cumbersome systems which are time-consuming to support and use. They build in inefficiencies which can be difficult to remove once embedded and ironically, spreadsheet systems re high-risk tools.

Through their research, the European Spreadsheet Risks Interest Group (http://www.eusprig.org/) found that 50% of spreadsheet models used operationally in large firms contain material defects.

EUSPRIG has identified several key areas of risks related to the use of spreadsheets. These include;

1. Human Error – To err is human; hence the majority, greater than 90% of spreadsheets contain errors, with approximately 50% of spreadsheet models used operationally in large firms, contain material defects. Because of the ad hoc development approach to spreadsheet 'tools' and the lack of systematic testing, such tools are error pone, and those error often remain, unnoticed.
2. Fraud – Because spreadsheet tool development is often outside of accepted development processes and mix 'code' and data, they create an environment for perpetrating fraud. The $600m fraud perpetrated by John Rusnak at AIB/Allfirst was spreadsheet related, as have many others since.
3. Overconfidence in decision-making – People tend to simply accept numbers shown within a spreadsheet without rigorously challenging either the numbers, how they were generated or the support data (if that is even available in the spreadsheet). This can "lead to a position where decision makers may act in the belief that decisions can be made with confidence on the output from the spreadsheet despite evidence to the contrary" [Banks & Monday, 2002].
4. Spreadsheet tools add to operational risk – Widespread use of spreadsheet tools, often described as 'grey IT' or as End-User Computing (EUC) tools can actually increase your operational risk… they very thing you are trying to manage! "The case of failed Jamaican commercial banks demonstrates how poor archiving can lead to weaknesses in spreadsheet control that contribute to operational risk" [Lemieux, 2005].

Too manual, too slow and too unresponsive to support strategic and operational decision-making

Today, business operates in real-time, leveraging data and analytics to generate meaningful information and insights to support strategic and operational decision-making. Unfortunately, because of the widespread use of spreadsheets, many risk management teams are not in a position to meaningfully contribute to and support decision-making.

Consider this real-world example from within a global IT function within a mid-sized, highly rated investment bank.

The Global IT leadership team would meet during the second week of each month.During this meeting, they would review the risk report, which included a 'Top 20 Risk Report' and other supporting risk reports.

The Global IT function was managing approximately 230 key risks which were assessed quarterly as part of their RCSA process. Nearly 120 people were directly or indirectly involved in this process. The risk register and RCSA process were all managed using a combination of a cumbersome spreadsheet 'system' and a lot of email and phone communications.

All risk mitigation tasks, and internal controls were captured and managed via spreadsheets, as were risk events. Task and event status updates were a daily and weekly ritual which generated a high level of email conversation and confusion about which were the latest reports and the right email conversation/thread.

Risk measurement was via a suite of metric; including both Risk and Control Indicators (KRIs and KCIs). The metrics were monthly and all updated manually via 40 different spreadsheets globally which were manually consolidated at a regional and global level.

As a result of this heavily manual process, when the Global IT team meet in the 2nd week of the month, the information within their risk reports was between 4-6 weeks old. Additionally, there was no ability to 'drill-down' to underlying data or understand underlying drivers of risk therefore if a member of the leadership team challenged the information reported or asked probing questions, the answers often had to wait until the following meeting.

IT is a fast-moving, fast-changing environment, therefore, it is not surprising to find that the Global IT leadership team did not value or respect the monthly risk reports. These reports simply didn't help the team decision-making or enable them to deliver a better IT environment to the bank.

In an environment where a business or technology change or incident could occur and alter the risk profile within minutes or hours, a spreadsheet-based system built around a monthly or quarterly risk cycle simply is not fit for purpose.

Does not encourage the right risk culture or establish clear accountabilities for risk

Creating and sustaining the right culture, a 'risk-based culture', is critical for the effective management of risk within firms.

Culture can be a difficult thing to define precisely. One formal definition is: culture comprises the Firm's people, shared values, symbols, behaviours and assumptions. Another more pragmatic interpretation of culture is "the way we do things around here".

Systems and automated processes can signal to staff the importance that the firm places on certain activities therefore shaping the culture around those activities. Accepting the use of an ad hoc spreadsheet system, throwing people at the problem and requiring a significant amount of manual work/rework signals that the Firm doesn't take risk management seriously and will lead to a poor risk culture.

Part of a good 'risk-based culture' is embedding clear accountabilities for risk management and embedding those accountabilities at the individual risk level. Typically, firms using a spreadsheet-based risk tool will have a column for 'risk owner' however, precisely what is meant by risk owner is often left undefined. Is this the person who is accountable for the risk? Is this the person who is undertaking the activities to manage the risk, is the person who provides the data related to the risk or is it the business function where the risk resides? This lack of clarity around the risk owner role does not encourage or enable a risk-based culture.

While many CEOs and other senior management will stress the importance of managing risk and taking a systematic approach, if they then support this message with spreadsheet tools, this is often seen as a 'talking the talk but not walking the walk'.

Reduce your cost of risk by 20% - 30%

Using spreadsheet-based tools for your risk register, driving the RCSA process and generating risk reports is, as stated, a highly manual, people-intensive approach which is inherently inefficient and ineffective. Costly and talent risk professional spend their time and energy chasing data and updating spreadsheets rather than getting out in the business and enabling risks to be managed.

It is also inherently costly. Based on our experience, we estimate this approach can add at least 25% to the Firm's cost of risk. This is in line with industry leaders such as Bain & Co and Mckinsey, who consistently use 20% - 30% as an estimate of the costs firms could save through better use of systems and technology within risk management.

In a paper published in February 2017, Digital risk: Transforming risk management for the 2020s, Mckinsey stated that "Our experience suggests that by improving the efficiency and effectiveness of current risk- management approaches, digital risk initiatives can reduce operating costs for risk activities by 20 to 30 percent". Further, they point out that "current processes are resource-intensive and insufficiently effective."

Building on this theme, in another paper published in April 2019, Transforming risk efficiency and effectiveness, Mckinsey found that "a well-executed, end-to-end risk function transformation can decrease costs by up to 20% while improving transparency, accountabilities and employee and customer experience".

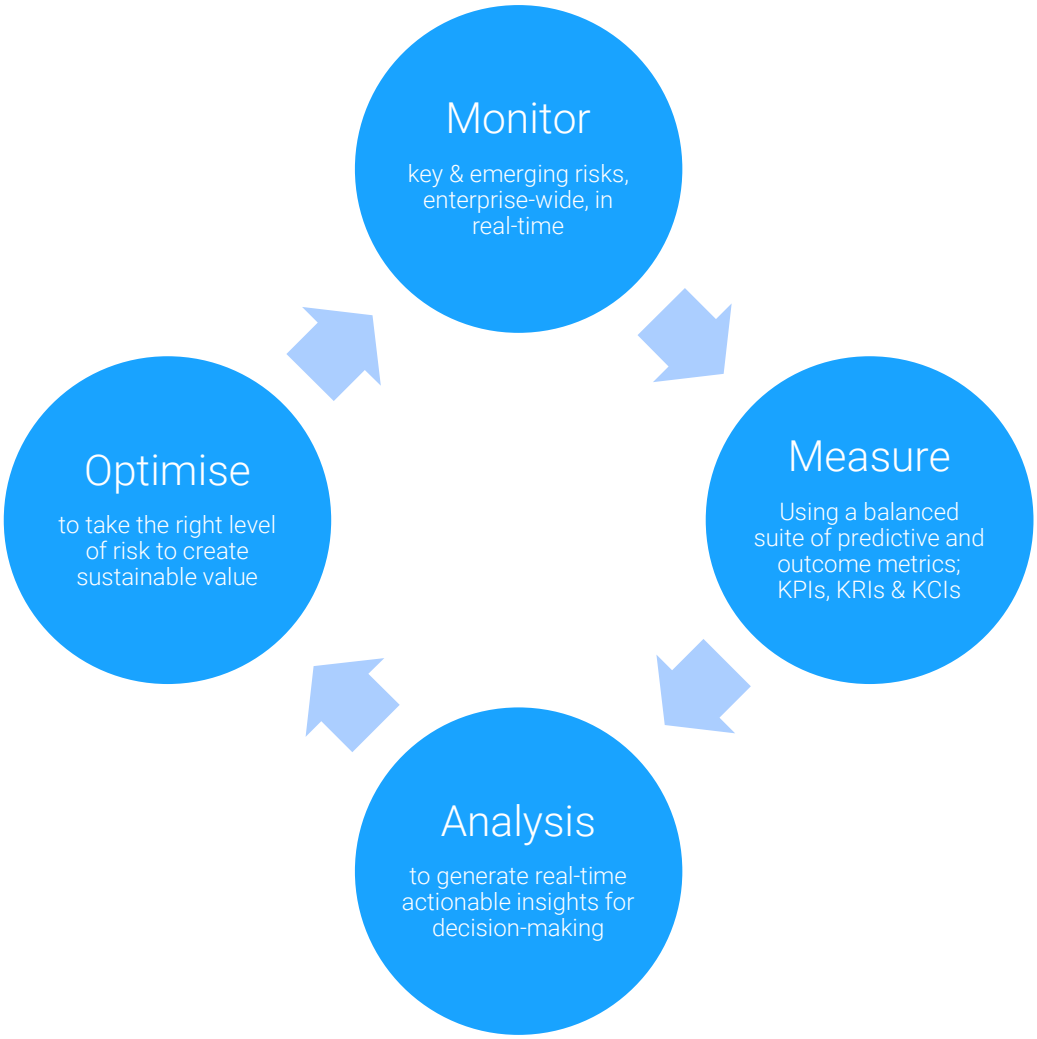
Bain & Co go a little further, stating that "we estimate that governance, risk and compliance (GRC) (ERP by another name) costs account for 15% to 20% of the total "run the bank" cost base of most major banks. And GRC demand drives roughly 40% of costs for "change the bank" projects underway".

SOLUTION

The KRM22 Risk Cockpit is a real-time, Integrated Risk Management application designed to support various risk management disciplines including Enterprise Risk Management, Operational Risk Management and Technology Risk Management.

Built on the foundations of a conceptually sound risk framework, a flexible organisational mapping capability, an embedded accountabilities model and robust data management and analytics, the solution automates an end-to-end risk management process.

Figure 1 - KRM22 Risk Management Process



Monitor

The starting point for the risk management process is identifying and regularly assessing key and emerging risks that will prevent the successful delivery of strategic and operational performance. Alongside the risks, mitigations such as key controls should be identified. Risk and controls should be regularly monitored and assessed. One widely used, quantitative approach to assessment is the Risk and Control self-assessment (RCSA) process.

This is a systematic approach for gathering an assessment of the impact and likelihood of a risk occurring, generating a risk severity rating. The second component of an RCSA is the control effectiveness assessment, which involves assessing the design and operational performance of controls to generate a control effectiveness rating. The results of the RCSA process are often presented using RAG style dashboards and heatmaps.

Alongside the RCSA process, a systematic approach to capture, track and manage risk events (sometimes known as incidents) is often implemented. This enables events to be linked to risks that have crystallised and controls that have either failed or whose effectiveness will be impacted by the event. Risk events data can also help firms to identify gaps in their risk and controls framework and drive improvement initiatives and other proactive risk mitigations.

Measure

To build a more complete, real-time risk profile, and to compliment the risk and control self-assessment process, a balanced suite of metrics should be deployed to track changes and results against thresholds.

Metrics can be classified as either a Measure or an Indicator. Measures are used to capture business facts which are either used as a direct input into decision-making or used as part of a calculation to generate indictors. As an example, a measure might be the Number of Cleared Trades Yesterday. Whereas Indicators are typically derived; ratio, percentage or similar, from other metric data for example, an indicator (for risk of failure to clear all trades) might be Ratio of Trades Cleared vs Trades Cleared over the last 10 days at the same time.

There are three different types of indicators that firms should consider including within their risk framework;

- Key Performance Indicators (KPIs) - indicate performance against a target value and are typically RAG rated based on thresholds of acceptable and unacceptable levels of performance. Within a risk framework, these should be linked to business outcomes; objectives, processes, initiatives and systems.
- Key Risk Indicator (KRIs) –indicate the level and changes related to risk severity. Again, KRIs are RAG rated based on a target value and thresholds of acceptable and unacceptable levels of deviation from target. Within a risk framework, KRIs link directly to risks.
- Key Control Indicator (KCIs) –indicate the level and changes related to control effectiveness. Again, KCIs are RAG rated based on a target value and thresholds of acceptable and unacceptable levels of deviation from target. They are linked directly to controls.

Both measures and indicators can be further categorised as;

- Predictive – a predictive metric is designed to provide a 'predictive indication' of an outcome been realised; for example, Number of Uncleared Trades 60 minutes prior to market close.
- Outcome – an outcome metric is designed to measure if an outcome has been delivered or realised, for example, Number of Uncleared Trades post-market close.
- Informational – an informational metric is designed to provide a measurement of a metric which is of interest to key stakeholders, for example, Firm Share price.

As the risk framework evolves and matures, it becomes clear which metrics add real value to decision-making and the number of metrics can be rationalised . Using the Risk Cockpit, also enables a metric to be more than one type of metric i.e.. a metric can be a KPI, a KRI and a KCI all at the same time.

Defining appropriate target values and thresholds can be a challenge for firms as they start their journey. To assist firms to better understand their metric data, and to improve target values and thresholds, the Risk Cockpit has the ability to dynamically and continuously calculate a target value

based on metric data. This enables firms to get started quickly and over time, set better targets and more meaningful thresholds.

Analysis

By its very nature, when making risk-based decisions, firms are doing so under conditions of uncertainty, less than perfect data and changing circumstances.

To make better decisions under these conditions, those making decisions need to have a range of input, from expert opinions (for example, qualitative risk assessments captured via the RSCA process) and quantitative data (for example, metrics data or risk events data). These different data inputs should be analysed to generate meaningful insights with which to make risk-based decisions.

In the initial stages, this analysis could take the form spreadsheet-like 'pivot tables' and business intelligence style 'slicing & dicing' of risk data. Over time more advanced analytical methods may be used, such as causal and probabilistic network models to discover and understand risk drivers and relationships which are not immediately apparent from less advanced analysis.

Optimise

Ultimately, the reason for undertaking risk management is not to reduce risk but to optimise the firms' risk-taking; balancing risk and reward. Research shows that firms who put in place the framework and tools to optimise risk-taking can generate a 20% increase in shareholder value compared to their peers. *See Milliman Risk Institute, August 2014 & Aon Risk Maturity Index, Insight Report, October 2017*

Implementing an integrated, enterprise risk management approach, build on the four pillars of strategy execution; risk appetite alignment, capital & liquidity efficiency and stress-testing using risk scenarios provides the management framework to optimise risk-taking. Key tools include;

- Business Model Canvas – Understand your business model and drivers of value.
- Strategy Map – Define your strategic objectives and understand the cause and effect relationships between objectives.
- Risk Appetite – Define clear risk appetite boundaries to determine the right level of risk based on your business model and strategic objectives.
- Probabilistic Capital and Liquidity models – Develop capital and liquidity models to ensure the Firm has the financial resources in the short and long term to fund itself, its trading activity and withstand reasonable shocks as and when they occur.
- Risk Scenarios – Develop a range of risk scenarios and stress-test your Firm's business model, strategy, risk appetite and financial resources to determine the Firm's sustainability and resilience under a broad range of operating environments.

BENEFITS

Eliminate spreadsheets

With powerful spreadsheet import capabilities and easy to configure 'Smart' register capabilities, the Risk Cockpit enables customers to get up and running in days and weeks, not months and years.

For firms who are just starting their risk journey, the solution includes Smart Registers to track risks, controls, risk events, and tasks.

For those customers looking to go beyond tracking risks and controls, the solution has Smart Registers for Objectives, Processes, Initiatives, Systems Information Assets and Metrics. Often a 'phase 2' activity, these Smart Registers enable firms to link risk management to strategic and operational performance and to complement and enhance the assessment process with real-time, data-driven metrics.

Enable automation of risk processes across organisation silos

Within the Risk Cockpit, there are powerful workflow, alerts, exception management and various visual tracking capabilities. These capabilities enable customers to automate their risk management processes and activities across the Firm. Features, such as the RCSA process, are triggered by date-driven, configurable frequencies and workflows to ensure risk assessments are completed on time. Those accountable for overdue risk assessments receive gentle reminders and automated follow-ups. The status of risks and risk management processes and activities is tracked via powerful colour-coded dashboards and visual tracking tools; timelines and Kanban boards.

Embed risk accountabilities

Embedded within the Risk Cockpit is the KRM22 ARCI accountability model (also known as RACI). ARCI is an easy to implement governance and decision-making model which clarifies an individual's role and authorities in relation to a process or activity where ambiguities and uncertainty exist. This results in greater decision-making transparency, faster decisions and a systematic streamlining of organisational decision-making processes.

The ARCI roles are;

Accountable (the buck stops here) – this is the individual who is ultimately accountable for the management of the risk, who has decision-making authority over the risk and makes the final decision about the management of the risk. There is only one per item within the risk framework, risk, control etc.

Responsible (the doers) – these are the individuals who undertake the work to manage the risk and implement the decisions taken by the accountable. There can be multiple responsible per item within the risk framework, risk, control etc.

Consult (keep in the loop) – these are the individuals who the accountable consults with prior to making decisions.

Informed (keep in the picture) – these are the individuals who the accountable informs post making decisions.

For regulated firms whose regulator will expect to see the three lines of defence implemented, the use of ARCI is highly complementary.

The three lines of defence is applied at the business function level; the first line of defence is 'the business', the second line is the risk management and compliance functions and the third line is the audit function. Whereas ARCI is applied to individuals, creating clarity, transparency and 'line of sight' accountability at the individual level.

This is an integral part of building a culture within which, the three lines of defence can be a useful management tool, and not just a regulatory, box-ticking exercise.

Empowered risk-based decision making

When firms move their risk management data and processes off ad hoc spreadsheets and onto the Risk Cockpit, they can transform the utility of their risk management processes. Rather than a monthly or quarterly process, revolving around management reporting cycles, firms can move to a real-time process. This enables them too

- create a single 'source of the truth' for all risk information which is always up to date rather than waiting for slow manual processes to be completed at the end of the month or quarter.
- spot potential issues early so they can take early action to either prevent the issue or minimise its impact
- get out of their inbox and manage risk events in real-time using visual timelines, Kanban boards and dashboards.
- Create clarity around firm structure and accountabilities and have this maintained in real-time for example a firm that uses the Risk Cockpit automatically 'hands off' accountability for key processes, risks and controls on a follow the sun basis.

This creates a dynamic risk management culture with the information and insights managers at all level need to quickly weigh the risk vs reward equation that is at the heart of so much strategic and operational decisions.

Reduce your Cost of Risk by at least 25%

Using spreadsheets to hold your risk register, support your risk and control self-assessment (RCSA) processes and generate regular risk reports is an inherently inefficient and ineffective approach.

The level of manual work required to make spreadsheet-based risk registers work creates a high, often hidden, cost on both the risk management team and those in the business who play a part in the risk management process.

Digitising the risk register and driving the automation of key risk management processes through automated data extraction, workflows and production of standard risk reporting dashboards significantly reduces the manual workload of risk management teams and the business.

Digitising the risk register has the potential to deliver a range of tangible and intangible benefits; however, from a financial perspective, the main driver is cost reduction. Based on our experience firms that digitise their 'risk registers'; moving their risk management processes off ad hoc spreadsheets and onto the KRM22 Enterprise Risk Cockpit can deliver a reduction of the operating cost of our risk management activities by a minimum of 25% within the first 90 – 180 days. We would expect those cost-saving to increase by a further 25% within the first 12- 18 months of using the Risk Cockpit.

CONCLUSION

Digital transformation initiatives have promised to drive increase efficiencies, greater operational agility and cut operating costs. Many of these initiatives have delivered on this promise; however, from a digitisation and automation perspective, risk management often lags other parts of the business.

With compelling tangible and intangible benefits, it is time to digitise your risk register and transform your entire risk management process and activities using the Risk Cockpit.

This service is designed to quickly move firms off their spreadsheet-based risk tool and onto the KRM22 Enterprise Risk Cockpit. Working in collaboration with risk specialist from KRM22, existing risk register, assessments and events data will be migrated and product knowledge transferred using an iterative, agile-based approach.

Taking this approach, firms can quickly, within ten days, eliminate their spreadsheet-based risk registers, cut their risk operating costs and start driving efficiencies and value from risk management.

References

Bain & Company. 2016. Banking Regtechs to the Rescue?. [ONLINE] Available at: https://www.bain.com/insights/banking-regtechs-to-the-rescue/

Mckinsey & Company. 2017. Digital risk: Transforming risk management for the 2020s. [ONLINE] Available at: https://www.mckinsey.com/business-functions/risk/our-insights/digital-risk-transforming-risk-management-for-the-2020s

Mckinsey & Company. 2019. Transforming risk efficiency and effectiveness. [ONLINE] Available at: https://www.mckinsey.com/business-functions/risk/our-insights/transforming-risk-efficiency-and-