MetricStream

PERFORM WITH INTEGRITY™

The Future of Integrated Risk Management

Position Paper

The scale and scope of risks faced by organizations today are expanding and changing faster than ever before. Driving this trend are disruptions and rapid innovations in business models and technologies. Meanwhile, as markets and organizations grow more interconnected, the points of intersection among risks are increasing. The result is that organizations now need to not only understand risks in isolation, but also recognize the interconnectedness between traditional risks (e.g., credit and market risks) and emerging risks (e.g., cyber and data privacy risks).

Traditional risks are known risks where the unknown aspect is really the measure of the risk. Therefore, in theory at least, these risks can be defined and mitigated. On the other hand, emerging risks, as well as how they intersect with traditional risks, are relatively unknown. Since they cannot be identified or defined, they also cannot be measured. These "unknown-unknown" risks—which expose organizations to uncertainties and losses that they cannot even perceive, let alone prepare for or predict—are commonly called black swan events.

Against this backdrop, the following pages of this paper explore a forward-looking framework for integrated risk management – one that brings together diverse and dispersed risks, providing a means to understand the intersection between these risks, and thus, identify unknown-unknowns. The paper also looks at how to build an adaptive program for risk prediction and proactive response, keeping in mind the rapid pace of change in operating markets. It then delves into the organizational challenges involved in managing "unknown-unknown" risks, as well as the strategic direction of the industry as it prepares for these risks and their domino effect.

Current State

Siloed Risk Programs Designed to Address Point-in-Time Challenges

Risk management programs, especially those dealing with non-financial risks, have evolved independently over time to address specific regulatory requirements in specific jurisdictions. Most of these programs have been largely reactive in nature, looking to address "known unknown" risks which materialize primarily as regulatory actions. While some of these programs have developed the maturity to monitor and manage individual risks, they are hardly ever integrated with other frameworks across the enterprise.

As risks become more interconnected, it is no longer enough to evaluate their impact merely within individual risk categories. Recently, at a large bank, a multi-million dollar risk event materialized as a credit loss, but it actually crept in many years ago when repeated control failures occurred in the operational risk program due to a lack of validation between the loan approval and loan disbursement process in core banking systems.

Risk programs today tend to monitor and manage risks in silos, making it impossible for stakeholders to track how their mitigation actions impact the realization of other risks.

Hyper-Connectivity Leading to Unknown-Unknown Risks

With the rise of the "sharing economy[1]", organizations and their operating markets have become dependent on infrastructure and capabilities outside their enterprise boundaries, sometimes even for mission critical services. As a result, both the types of risk and their interconnectedness are increasing. Today, the size of a loss associated with a risk event isn't just determined by risk frequency and impact, but also by the velocity with which that impact spreads through other interconnected risks.

In a risk program that does not transcend risk types or departments, it becomes very difficult to understand and measure risk interconnectivity and velocity because risk relationships are not well-defined and hence not monitored. Yet, it is within this intersection of disparate risk programs and infrastructure that unknown-unknown risk events with catastrophic losses originate and spread.

Today, banks and financial institutions are adopting conversational AI or chatbots for a plethora of use cases. However, the primary use of these tools has been to automate customer interactions – for example, robo-advisors providing assistance on wealth management services. While these chatbots are usually assessed against direct risks such as information security, data privacy, and model risks, what is often ignored is their strong correlative impact on credit risks -- especially if the self-learning AI models used to provide investment advice develop biases towards a certain class of financial products. Worse still are the conduct risks that could arise, should the chatbots become racially biased, as we saw with Microsoft's Twitter chatbot, "Tay".

Currently, organizations with siloed risk programs are unlikely to be able to identify and monitor the interconnectedness between various risks associated with new technologies like conversational AI chatbots. The unknown-unknown risks that originate from the intersections between traditional and emerging risks can grow to catastrophic proportions, coming to the organization's notice only when a massive loss event occurs.

[1]An economic model that allows people to exchange tangible and intangible resources with each other on demand and at scale, reducing transactional friction and the need for middlemen (e.g., coworking spaces, ridesharing, crowdfunding)

Industry Contagion Arising from the Intersection of Traditional and Emerging Risks

The interconnectedness of operating markets, coupled with emerging risks and their relationships with other risks, have given rise to a contagion effect that extends beyond the boundaries of the enterprise. Today, the risk posture of a given business line can be impacted by risks originating from multiple other parts of the organization, or even other enterprises. If these risks aren't looked at from a broader perspective, they could continue to grow within their silos, emerging as a systemic, industry-wide failure at some point in time.

Regulators and market participants are becoming increasingly aware of such risks. In their discussion paper on operational resilience, the Bank of England, Prudential Regulation Authority (PRA), and Financial Conduct Authority (FCA), argue that operational disruptions within an organization can cause "harm to consumers and market participants" and "instability in the financial system". This represents a significant shift in perspective from a time when risk management was looked at in silos not just within organizations, but in operating markets at large.

Future State

Over the years, organizations have invested resources and effort in building their risk management program infrastructure and maturity. The problem is that many of these programs have concentrated on measuring and managing risks in isolation. They have not been designed to respond to fast changing risks, or to understand risk interconnectivity in an environment where the contagion effect of risk spans multiple degrees of separation.

The proposed strategic objective of integrating risk programs is not to replace everything that has gone before, but rather to understand the relationship between various risk profiles, so that new risks can be proactively identified. The integrated risk program of the future looks to leverage the existing ecosystem of risk monitoring and management infrastructure, maintaining their federation and independence as required. However, the program also seeks to build an overarching integrative layer that establishes the relationships between different risks—including their impact and correlated issues—by tying them back to business objectives. It then focuses on building an adaptive, unified, coordinated, and real-time risk mitigation plan across business functions and risk groups through an integrated issue and action management strategy. Through this approach, risk information is available instantly, in digestible and understandable pieces, enabling the board of directors and senior leaders to make effective risk-based decisions.

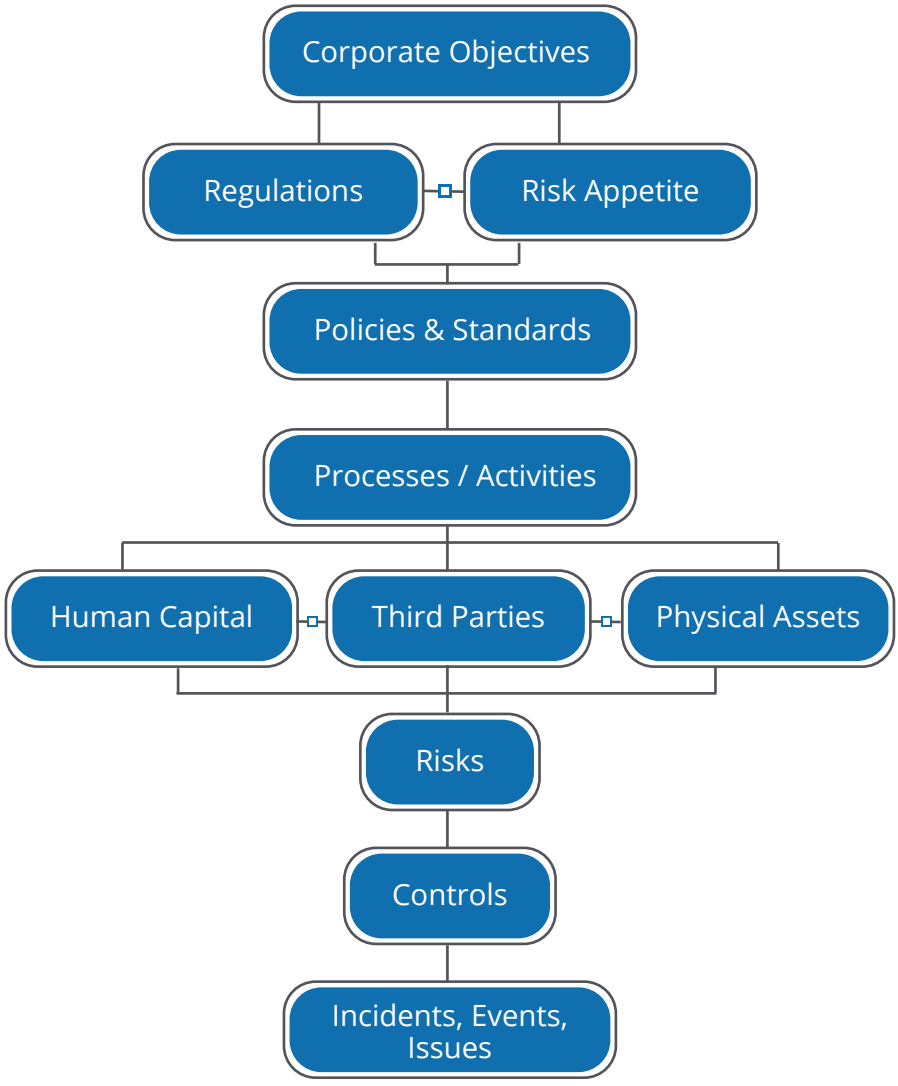
Here are some of the key best practices that organizations should consider while building a future-ready integrated risk management program:

Establishing an Integrated Risk Framework Aligned to Business Objectives

The first step in an integrated risk program is to establish a common understanding of the program's outcomes across various risk functions. That is done by defining corporate objectives, and then contextualizing them within the market constraints defined by regulatory requirements, as well as the risk appetite defined by the organization.

The constraints and objectives together are translated into a set of policies and standards which then become the guardrails for the organization to operate within. The policies and standards also serve as the bedrock for risk related processes and activities that enable the achievement of corporate objectives.

The processes and activities, in turn, flow down to the various functions and groups spread across the three lines of defense. These processes help measure and manage risks through appropriate controls and issue remediation efforts.



- What you are trying to achieve...
- Your constraints...
- Rules you need to follow...
- What you do in pursuit of your objectives...
- Instruments to execute your activities...
- What may impede progress...
- How you respond to impediments...
- What actually occurs that may need addressing...

Linking the Ecosystem of Risk Monitoring Tools with the Integrated Risk Framework

By establishing the framework illustrated in the previous section, organizations can effectively integrate information—both risk and business transaction related—from the ecosystem of tools used to monitor and manage risk. Various risk tracking and measurement programs for both financial and non-financial risks can now communicate with each other through a common point of contextualization i.e., business objectives.

The integrated risk framework leverages the ecosystem of risk monitoring tools through an integrated issue and action management capability where identified risks and their treatment plans are captured and aggregated. This capability is then linked to the risk universe (primarily the risk data model) to uncover commonalities between the issues identified in the various risk measurement and management tools. The integration and alignment of issues and actions with the common risk universe can be used to define a risk treatment plan with coordinated effort from various risk groups (spread across risk functions, regional entities, legal entities, and business functions).

Continuous Risk and Control Monitoring Providing Real-Time Information and Reducing Risk Response Time

The efficacy of an integrated issue and action management capability lies in an organization's ability to identify risk events in real time, perhaps even preemptively. For example, a leading financial exchange is tracking "rumors" on "pump and dump" schemes for certain stocks through a real-time social media risk monitoring tool. These rumors, once identified by the tool, are flagged as issues within the integrated risk program. Based on the relationships defined within this program, accountability is assigned to risk officers and market surveillance teams. Immediately, risk mitigation actions are coordinated by consumer protection teams. The perpetrators of the rumors are informed, and compliance teams take action to prevent these market participants from participating in the trade of the aforementioned stock.

Moving Risk Identification to the First Line of Defense

Since the first line of defense often becomes aware of emerging risks before others, they play a critical role in an integrated risk management program. The integrated issue and action management capability must be extended to them so that all issues identified at the first line are aggregated and consolidated with the issues identified by the ecosystem of risk monitoring tools. The result is a single repository of all risk related issues from the three lines of defense. This data enables the first line to allocate resources for issue remediation based on the areas of highest strategic importance or contribution to corporate objectives.

Enabling the First Line of Defense with Chatbots and Robotic Process Automation (RPA)

The process of capturing and aggregating issues and risk events from the first line of defense can be quite time-consuming and resource-intensive due to the large number of participants involved. However, technologies like robotic process automation and chatbots have exponentially increased the ability of risk functions to gather information from the first line of defense, while actually reducing the effort required. For example, at a the leading mortgage financing company, chatbots enabled on mobile devices, offer a simple and jargon-free way for first-line participants across the organization to report issues and risk events.

Cyber Emerging as a Key Risk with the Fastest Pace of Change

The rise of the digital enterprise has transformed IT and cyber risks into significant threats. As digital organizations look to adopt the cloud, and increase process automation, the risks associated with both internal and external IT assets are increasing. These IT and cyber risks have a compounding effect when considered in terms of their intersection with other, more traditional risks.

Established frameworks like FAIR, as well as enabling risk management technology, have made it easier for organizations to identify and quantify IT and cyber risks across information assets. The ability to aggregate these findings, and map them to other risk profiles, is key to a truly integrated risk program.

Ultimately, an integrated risk management program enables organizations to identify issues from multiple risk monitoring programs and tools that were previously managed in siloes. Using this data on issues, organizations can correlate different risks, and at their intersection, find previously “unknown-unknown” risks. Advancements in artificial intelligence (AI) and machine learning (ML) will make the process more efficient and effective.

Building an Ecosystem of Integrated Risk Methodologies and Taxonomies

With an integrated risk management program, organizations gain a single source of truth to aggregate risk events and issue related information from multiple risk monitoring tools, as well as the first line of defense. The next step in the evolution of this program is the development of a systemic, industry wide risk management dataset that could help organizations identify and prepare for risks that might not yet have materialized within their enterprises, but have done so in others with similar business interests, operating in similar markets.

Early efforts to build such systemic datasets have included the external operational loss databases created by ORX and GOLD. ORX is already embarking on phase 2 of "developing an industry operational risk taxonomy". In the future, we are likely to see industry-wide risk datasets being built not just for operational losses and risk taxonomies, but also for issue aggregation and risk treatment plans.

Finding Unknown-Unknown Risks with AI and ML Enabled Risk Intelligence

Integrated repositories of risk events and issues, coupled with organizational and industry-wide risk datasets, will offer organizations the ability to correlate issues and risk remediation actions. This golden source of information, when contextualized to a common risk universe, can be acted on by AI and ML related analytics to identify both unknown risks—in the cross-section of different risk profiles—as well as unknown relationships between issues. Based on the insights, organizations can formulate an integrated risk response strategy.

Preparing the Organization for an Integrated Risk Management Approach

Integrated risk management as a program will require significant changes in people, skills, and processes, as well as technology. Some of the core aspects of change will involve:

1. **Reallocation:** With risk monitoring and issue identification moving to the first line of defense, skills will have to be transferred from the first line to the second line. As the latter gains a deeper understanding of issues and risks realized by the first line, they can then design programs that will be owned and operated by the first line.

2. **Reskilling:** The reskilling of risk practitioners will be a twofold endeavor. The first aspect will be about building the ability to understand emerging risk categories and their behavioral patterns, while also strengthening risk monitoring capabilities. Take, for example, cyber risk. Not only is its velocity and interconnectedness with other risks far greater than that of traditional risks, but it also requires a level of monitoring that is far more real-time and data-intensive.

   The second aspect of reskilling will be about understanding the concurrence of risks, while also identifying the materiality in this interconnectivity. Essentially, risk practitioners will need to cultivate a multi-faceted understanding of risks. For example, today, the use of AI algorithms in business services has given rise to information security risks which, in turn, are closely associated with compliance risks linked to data privacy regulations like the General Data Protection Regulation (GDPR). Practitioners of compliance risk and data privacy management will need to be aware of the risk intersections and dependencies across both their disciplines. They cannot restrict themselves to measuring risks in silos.

Drive Business Results by Harnessing Uncertainty

By embedding risk management into business processes through the integrated risk program discussed in this paper, organizations will gain greater visibility into the health of their business, as well as better information to support strategic decisions. The integrated risk program, which highlights both upside and downside risks, will enable organizations to proactively assess and act on opportunities, rather than having them pass by simply because they were unknown or unmonitored.

Today, boards and executive management are expected to understand the nuances of risk, both from a governance perspective as well as from a business performance perspective. The C-suite is expected to be aware of the organization's risk appetite, while articulating its risk culture. They also need to be able to fully understand the integrated risk posture of their organization, so that they can provide stability and consistency in a highly uncertain operating environment.

With that in mind, the big questions for organizations today and beyond are:

- What value do we place on understanding and thus reducing uncertainty?
- What if we could increase the predictability of business outcomes?
- How can we capture more and more of the upside of uncertainty?

This is the new paradigm for risk management — moving from an information and compliance-focused approach, to a new method that directly links risk management to performance by harnessing uncertainty.

Contact us
visit: www.metricstream.com