Digitization of Risk Management

Equipping the business to make informed risk decisions

In today's dynamic world full of opportunity and risk, business transformations and increasing regulatory pressure, organizations need to become more agile while still managing their risk.

Despite investments in GRC tools, risk and compliance processes in organizations today remain largely manual and siloed, and risk data remains fragmented. Significant improvements in risk management can be obtained when learning from digital business transformations. This article aims to outline the authors' vision on how to digitize risk management, in-control, and assurance practices.

M.C. Bautista CIA CISA
is a Director at KPMG in the Netherlands.
bautista.maria@kpmg.nl

B. Krutzen PhD
is a Partner at KPMG in the Netherlands.
krutzen.ben@kpmg.nl

INTRODUCTION

Opportunity Statement

Despite guidance provided by professional bodies, available academic research, and significant investments in GRC tools, risk management practices at most companies remain largely manual and siloed. At the same time, the business environment is becoming more disruptive and demanding:

- Digital transformations undertaken by many organizations rapidly evolve their IT environment and operating models;
- Boards and Management are expected to be more transparent on their risk appetite, and how risk appetite is operationalized across the organization;
- Regulatory pressure is increasing, while the cost and value of compliance activities are being challenged by the C-suite.

In this context, there is a clear opportunity for risk managers to contribute to business agility, quality risk decision making, and to underpin the public trust in their companies.

Our Vision: Integration across five risk dimensions

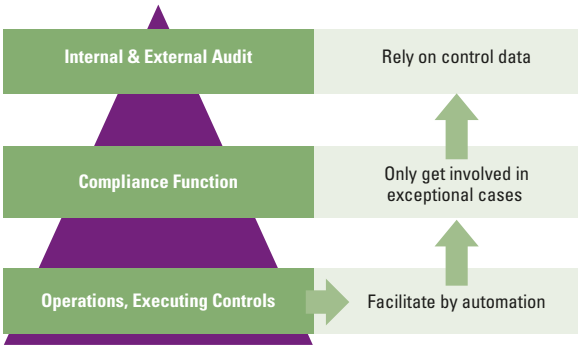
A value adding (enterprise) risk management function orchestrates integration across the following five dimensions.

1. Integrated workflow across the lines of defense (LOD)
Equipping the business (LOD-1) to effectively own their risks and controls, increasing transparency and efficiency for the risk and compliance function (LOD-2), and enabling continuous assurance for internal and external audits (LOD-3/4).

Most analytics efforts related to controls are today executed as part of assurance activities. As a result, the business is often confronted with insights from compliance or internal audit, and is forced to find reasons for what actually happened months ago. Unnecessary surprises from controls testing in Q3 can be avoided by providing the business with the right analytics insights to be continuously aware and in control of their own processes, and the associated risks and control effectiveness.

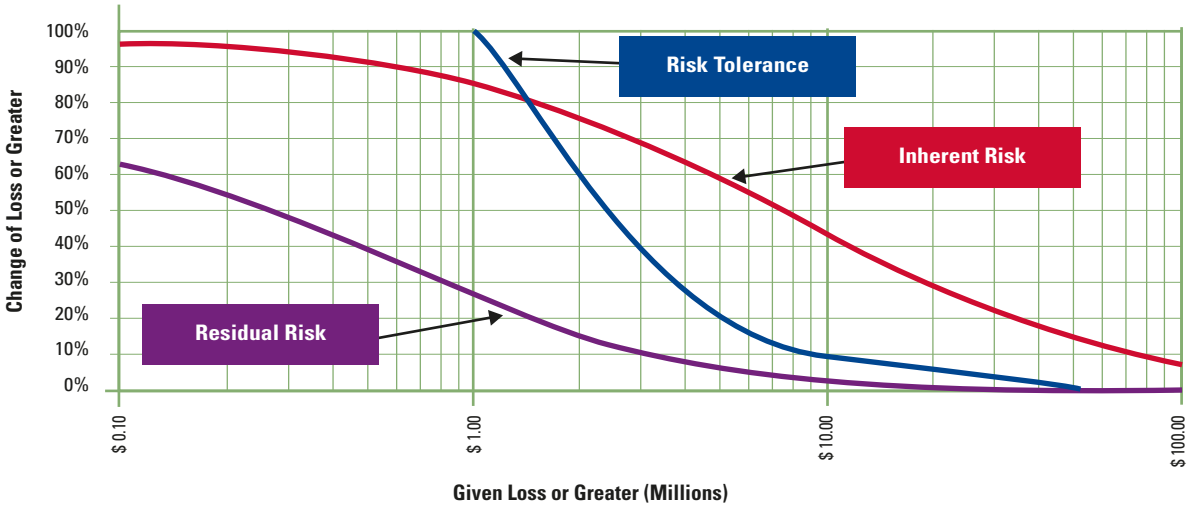
By providing the business with analytics of their processes in the form of *Continuous Control Monitoring* (CCM), their ownership naturally increases, and they will more effectively mitigate their risks in a timely fashion. The data generated in these processes will provide LOD-2 with valuable ongoing and comprehensive transparency, and if done well, LOD-3 can rely on the same data, and achieve a form of continuous assurance. This in turn, will reduce the effort and cost required in both LOD-2 and in LOD-3/4.

Figure 1. Workflow across lines of defence.



Digital transformations undertaken by many organizations rapidly evolve their IT environment and operating models

Figure 2. Loss Exceedance Curves.



There is a significant disconnect between the management of operational and enterprise level strategic risks

2. Integration of strategic, tactical and operational risks
Based on tangible risk scenarios and using sound statistical methods.

Today, in most organizations, there is a significant disconnect between the management of operational and enterprise level strategic risks. The enterprise risk management cycle is often an isolated process, largely detached from relevant operational issues and decisions. And risk appetite statements, if articulated at all, do not get effectively deployed in the day-to-day operations, turning these appetite statements into paper exercises.

Managing risks across the enterprise, according to an appetite, in a consistent manner, can provide critical insights for decision making at every level, and ensure that scarce resources are applied in the most impactful areas.

To integrate operational, tactical and strategic (enterprise) risks, a consistent risk hierarchy is required, as well as a mathematically correct aggregation and drill-down of these risks, based on tangible, end-to-end risk scenarios. Risks should be expressed in terms of the type of business impact, and potential business losses should be quantified to provide a solid foundation for a like-for-like comparison of enterprise risks from different risk domains.

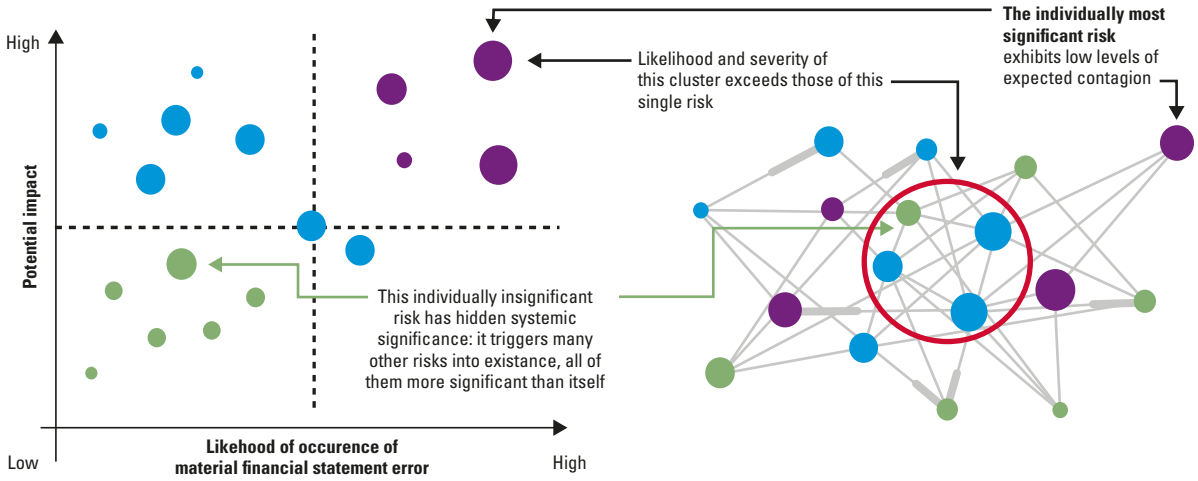
For complex, technical risks, such as cyber, these risk scenarios should be modeled, because manual or spreadsheet-based assessments cannot appropriately represent the critical components of the risk scenarios that determine the potential losses.

It is good practice to use loss distributions, such as Loss Exceedance Curves (LEC: see diagram for example), to discuss risks, rather than using traditional risk heat-maps or risk visuals, because the latter cannot support reliable aggregation and drill-down of the risks.

3. Integrated insights from backward looking, present, and forward-looking data
By leveraging industry data, expert elicitation, and understanding risk interconnections.

The financial crisis has (once more) proven that forming decisions based only on historical data can be misleading. Especially in the current disruptive business environment, a lack of understanding of emerging risks, and how these correlate, can be a costly mistake.

Figure 3. Dynamic Risk Assessment.



Understanding company-relevant systemic risk correlations can improve strategic planning in dynamic operating environments. Risks that seem relatively unimportant on their own, can have a major potential impact when risk correlations are considered (see Figure 3 and section C. Dynamic Risk Assessments on page 79).

To derive these correlations, we will need to rely on estimations by experts. While a data-driven approach is generally preferred, research has shown that using elicitation of experts who have followed a calibration training, can provide robust results even if the available company and industry risk data are scarce.

Lessons learned from industry peers are also of value when it comes to risk forecasting. If risk data along the timeline is systematically captured and properly articulated, management can reflect on whether choices taken in the past are future-proof, and take better informed risk decisions.

4. Integrated in-control and compliance domains
Breaking through the functional silos and integrating control frameworks across the enterprise.

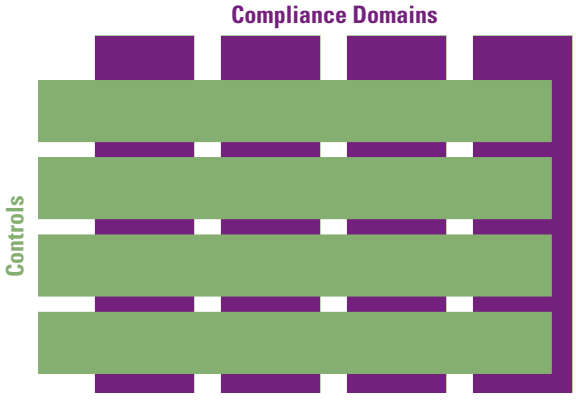
Companies often still approach in-control areas and compliance domains in an isolated manner. An example is the new GDPR European privacy regulation. Many companies are creating separate controls and compliance activities for this requirement. As a consequence, we see duplication of effort, misalignment and slow progress.

Organizations can greatly benefit from having a single center of excellence (CoE) risk and control function (LOD-2) for the entire organization, covering all in-control and compliance domains, and having a strong strategic and operational relationship with the legal function.

Such an LOD-2 organization oversees all controls across the risk and compliance domains, captured in a single integrated control framework (see diagram), and streamlines and orchestrates mitigating and testing efforts.

The Internal Audit function will value the insights provided through this integrated framework to better assess and decide on the level of assurance across the enterprise, rather than having a necessarily light-touch approach for each individual control domain.

Figure 4. Integrated Control Framework.



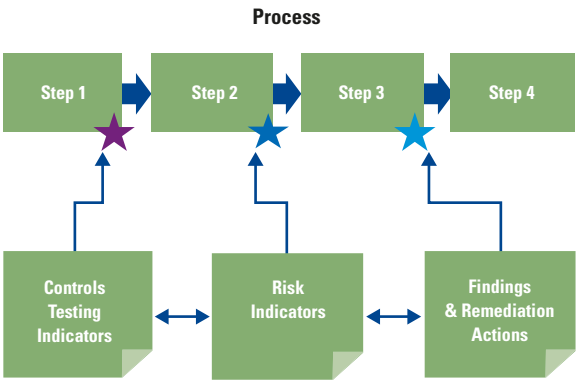
5. Integrated risk and control indicators and actions
Enabling the business to take quality and timely decisions based on operationalized risk appetite.

Many indicators are monitored daily in specific parts of the organization, and isolated decisions are being made to address issues. Often, these indicators are not clearly linked to risks and actions taken are unknown to the risk owners. At the same time, through external and internal assessments and audits, findings are produced, and actions defined to address them. Prioritization of actions is mainly based on who found the issue (audit actions generally taking precedence), while this might not be the best way to structurally reduce the risks of the organization.

Articulating an integrated view of process performance, risk and control indicators, assessment and audit findings, and the associated improvement actions, will not only enrich the quality of management decisions around the adequacy of indicator thresholds (link to risk appetite), pain points, short cuts and deviations, but will also enable an end-to-end view of process issues and allow management to strike the right balance between process agility, controls and early warnings to be embedded in the day-to-day operations.

From a risk perspective, the desired integration can be achieved through the mapping of indicators, issues and actions to process, assets, controls and through that ultimately to the end-end risk scenario's. Relatively simple changes to existing processes to structurally include such mapping, can enable this integration, and provide a powerful basis for management to more confidently set the appropriate indicator thresholds and priority of remediation activities.

Figure 5. Integrated Indicators and Actions.



HOW TO OPERATIONALIZE: DIGITIZATION OF RISK MANAGEMENT

KPMG has extensive, global experience with implementing traditional GRC tools from all key vendors ([Lamb17]). We have found that only a small portion of the desired integrations of risk management activities which we have specified in the previous section can be achieved with these tools, and even then, this often requires costly customizations with downstream consequences for the sustainability of the solution. In fact, these limitations hamper organizations in achieving the effective digitization of their risk management processes, which is a pre-requisite for the desired integration.

Given the strong pressure on organizations from their business transformations, with new threats and increasing regulatory pressures, and aligned with the industry analysts and with WEF views on the need for risk integration and quantification, we have pursued an alternative way to help organizations to deal with these challenges. We have partnered with Microsoft to develop our own enabling technology to our customers and provide managed risk services: **The KPMG Digital Risk Platform.**

This platform automates and integrates risk, in-control and assurance processes based on a consistent data flow. The diagram below shows the relevant components of the integrated risk management cycle.

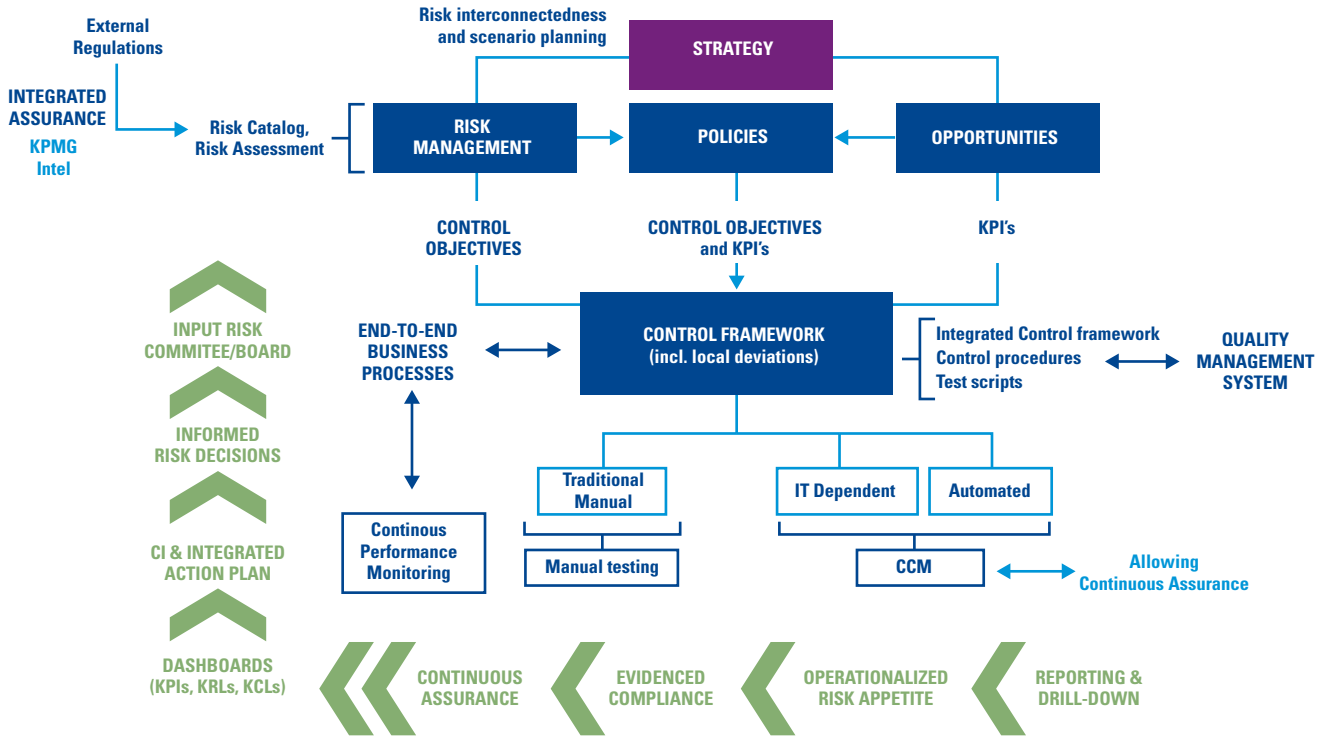
Key Enablers for Success

It is not sufficient to just provide a new technology platform to address the challenges which organizations face. It requires us to populate this platform in such a way, with configurations and data, that organizations can use it out-of-the-box with minimum effort on their part. We do this by leveraging our intellectual property, as we explain in the following sections.

A. Continuous Compliance Monitoring (CCM)
Through its audit and assurance activities, KPMG has assembled over the years a unique library of advanced control queries (called *Facts-to-Value*), which can be deployed by organizations to implement Continuous Control Monitoring with minimum effort and optimal results, using our Digital Risk Platform.

KPMG has a standard method to develop control-by-control business cases for the implementation of CCM, ensuring that effort is directed to achieve maximum value early on. A good understanding of how the use of CCM should be captured in the organization's control methodology and how the assurance processes have to updated to create a smooth transition are also important.

Figure 6. Our vision on Integrated Risk Management (as per Gartner's terminology) ([Kim18]).



B. Risk Modeling

For cyber risks, KPMG, together with Doug Hubbard of HDR [Hubb16], has created a quantitative model which is an integrated component of the Digital Risk Platform. KPMG is building up a library of risk scenarios for each industry, which enables benchmarking of risks with other organizations. The model is factored in a way that minimizes the amount of company-specific information required to run the model, and the model can easily be maintained over time. We call this offering *Quantification as a Service* to contrast its benefits with the isolated and labor intensive alternative solutions.

C. Dynamic Risk Assessments

Since a number of years, KPMG has a method (*Dynamic Risk Assessments*, DRA) to capture and calculate the implications of risk interconnections, which is being embedded in the Digital Risk Platform. Engagements with clients around the world have fine-tuned the model as well as the protocol to elicit the expert estimates, so that benefits can be obtained without unnecessary effort (see the specific article on Dynamic Risk Assessment starting on page 44 in this edition of Compact).

D. Control Framework Optimization

With our KPMG approach to map controls to processes it is possible to balance process control and agility from a business outcome perspective. What we have found in our client engagements is that organizations may not only have multiple frameworks, leading to a duplication of effort, but are more often than not also over-controlled, hindering the business, and spending too much money on compliance.

We use *Quantification as a Service* to contrast its benefits with the isolated and labor intensive alternative solutions

It is especially important to simplify and streamline the controls before assessing the benefits of CCM, as otherwise, we may be automating controls that are actually not needed.

E. Integrated Reporting

KPMG has developed a model that structures reporting of risk data, whether these are findings, risk indicators, mitigation progress, quantified risks, maturity or benchmarking data. The model works consistently from the level of the board down to operations. This model, after Tricker [Tric15], enables the board to fulfill its fiduciary duties related to risk management, covering challenging domains such as cyber risk or privacy, in a manner that is defensible in court. This ensures that it addresses the increasing personal liabilities of board members.

As a final remark, it will come as no surprise that integrating and digitizing risk management processes is a journey that, in general, will take a several years for organizations of a significant size. However, this journey consists, if done well, of small, iterative steps, each of which provide immediate and demonstrable benefits. As long as these steps are taken with the end-goal in mind, the value for the organization along this journey will continuously keep increasing.

SUMMARY

There is an opportunity to increase the value of current risk management practices by integrating and automating risk management in organizations across a number of dimensions. This digitization of risk management brings more transparency, better risk decisions, while at the same time, reducing the effort and cost required.

We have learned from digital business transformations, and have set-out to put the power of automation and analytics in the hands of the business, who operate the processes and controls, who own the risks, and who are therefore best positioned to ensure risks are indeed mitigated.

We have a strong vision on how to digitize risk management, and, in the absence of strong alternatives in the market, we have partnered with Microsoft to develop an Azure cloud-based platform, the KPMG Digital Risk Platform, which it offers as a managed service.

Most importantly, this Digital Risk Platform harnesses many years of globally developed KPMG intellectual property on risk management, and makes this IP available for clients in way that requires minimal effort, while ensuring early and sustained benefits.

References

[Hubb16] Douglas W. Hubbard, Richard Seiersen, Daniel E. Geer Jr. and Stuart McClure, *How to measure anything in cybersecurity risk*, Hoboken, New Jersey: John Wiley & Sons, 2016.

[Kim18] Elizabeth Kim and John A. Wheeler, *Competitive Landscape: Integrated risk management solutions*, Gartner Report, 2018.

[Lamb17] G.J.L. Lamberiks, I.S. de Wit and S.J. Wouterse, *Trending topics in GRC Tooling*, Compact 2017/3, https://www.compact.nl/en/articles/trending-topics-in-grc-tooling/, 2017.

[Tric15] Bob Tricker, *Corporate Governance: Principles, Policies and Practices*, Oxford: Oxford University Press, 2015.

Masterclass DRM for Financials

Tilburg University and **KPMG** have taken the initiative to provide organizations and individuals with the necessary knowledge in the field of digital risks. Our program focuses on the three dimensions which are important in digital risk management: processes, data and organization. For more information and registering for the master class (in Dutch only), go to www.tilburguniversity.edu/drm.

About the authors

Maria Cruz Bautista Lucas CIA CISA is a Director in the KPMG Risk Consulting practice, based in the Netherlands. She is a certified auditor (CIA, CISA) with more than sixteen years of experience supporting management to improve risk insight and remain in-control during change and growth. Her current focus is on operationalizing Enterprise Risk Management, in-control activities and continuous assurance through digitization. Maria held senior risk management positions at Royal Dutch Shell Plc and at the A.P. Møller-Mærsk Group.

Ben Krutzen PhD is a Partner of the Dutch practice of KPMG IT Advisory. Ben holds a PhD in Theoretical Physics. Prior to joining KPMG, Ben was Deputy Group CISO at Royal Dutch Shell (RDS), accountable for the RDS Cyber Security Strategy (2010-2016). In this role, Ben has shaped the engagements on cyber with the board, and has defined and mobilized three successive multi-year company-wide improvement programs. Ben's current focus is to helping clients develop a risk based cyber security strategy and roadmap, and transforming their information risk management processes through integration and automation.