Risk and control self-assessment: What's next?

How technology can evolve the RCSA process for better risk-based decisions

KPMG International | kpmg.com/risk

Contents

01 Introduction

Enhancing the way **Risk and Control Self-Assessment** (RCSA) is conducted presents many opportunities for companies — to protect their business, employees and customers; to support growth; to reduce cost and to build and protect brand reputation. The RCSA process has long been the 'bread and butter' of the risk practitioner and as risk management embeds and matures within companies, employees without risk in their title have also come to appreciate the important role they play in the risk management lifecycle. The RCSA involves the identification and assessment of a company's risks and controls. Ideally, it should be an efficient and systematic approach used by organizations to confidently manage their risk profile and support senior managers to make timely, informed, risk-based decisions, by:

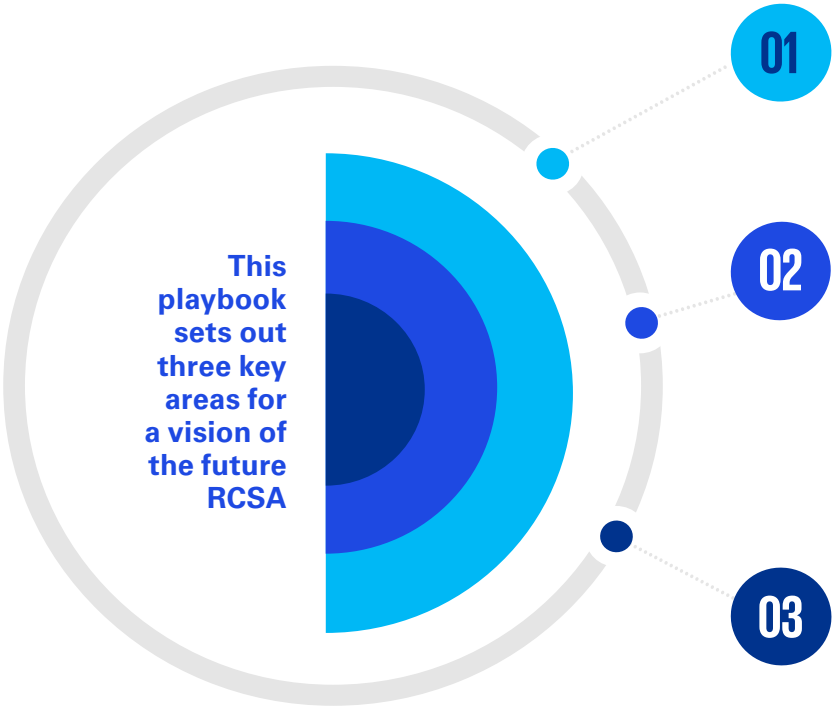
- Highlighting the most material risks impacting the company's strategic goals.
- Assessing the risk outlook of the business, considering changes in the business profile and external events.
- Identifying specific, material weaknesses in the control environment that threaten controls performance and improvement.
- Supporting the implementation and monitoring of risk mitigation plans.
- Driving and embedding risk awareness and a strong risk culture across the company.

However, effectively operationalizing the RCSA is often challenging and is seldom considered to be the value adding exercise that it has the potential to be. There are several drivers for this that include: a reliance on inefficient and manual processes, a lack of buy-in against the backdrop of competing risk management priorities in a time constrained environment, the process being seen as a regulatory compliance exercise rather than a mechanism for continuous improvement, and difficulties in tracing risk and control accountability and ownership. This is compounded by challenges sourcing and validating accurate risk data, poor data quality and inconsistency which limits the ability to deploy data analytics to deliver insights and inform actions.

But take a step back and imagine a world where real-time risk and control information drives business decisions without these issues, where there is no need for the current levels of process, resourcing and effort. For RCSAs to drive the desired level of value, there should be a shift from a 'point in time' assessment to a more dynamic, rapidly evolving view of risk, adept at keeping pace with the company. Technology and data are the linchpins that enable the effective utilization of analytics and serve as the conduit for artificial intelligence (AI) and machine learning (ML) to be harnessed. As many companies are at different stages of their digital transformation journey, leveraging tools and platforms will likely be fundamental when executing the RCSA to help businesses make better informed, risk-based decisions.

“But take a step back and imagine a world where real-time risk and control information drives business decisions.”

A better vision for the future?



Connected and dynamic RCSA

The RCSA of the future is expected to be characterized by dynamic and real-time assessment based on universally accessible and timely information. The ability to unify and exchange objective data consistently from multiple information sources will likely form the backbone of the future RCSA.

Consistent and efficient RCSA

Driven by standardized and systematic processes, risk and control information should be interconnected. This enables management to be alerted where changes are needed to the risk profile. It can signal where risk rating adjustment or even initiation of correct control action is required, which in turn, can enable the organization to realign itself with its defined risk appetite. Streamlined risk processes and a methodical approach to controls testing can support an accurate view on risk and controls performance as a key feed into the RCSA. A comprehensive and up to date risk and control taxonomy can also enable consistency in the way risk is identified and reported across the organization.

Informative and value adding RCSA

The future RCSA should support a positive risk culture by supporting management to make informed risk-based decisions using insightful reports. Management remains vigilant to changes in the risk environment, ready to act where re-assessment of the risk environment is necessary, and actively considering when risks should be identified and modelled. At all times, the risk profile should reflect the reality of both the current and emerging risks to which the company is exposed. Ultimately, the RCSA of the future should be more efficient and can reduce subjectivity in the 'self' assessment, delivering a more objective result.

The following sections explore each component of the vision in turn, considering the current challenges and the response required to support the achievement of this vision.

02

Connected and dynamic RCSA

The challenge:

RCSAs are performed at pre-defined intervals and in an isolated manner, resulting in the information being frequently out-of-touch and out-of-date.

Currently, RCSAs are undertaken at rigidly scheduled intervals throughout the year. This assessment is often accompanied by huge levels of manual effort to collate and analyze significant volumes of risk information. The timetabling of risk assessments creates a delay between capturing and reviewing information, making it difficult to achieve an accurate picture of the risk exposure faced by the organization. Consequently, outdated RSCAs are prone to gaps arising, such as evolving strategies and products or changing processes, projects, and regulations.

RCSAs also tend to be undertaken in a siloed manner, often guided by how organizational hierarchy is captured within risk tooling systems, or how risk management is embedded within the first line. The process of analyzing data across multiple business areas presents challenges in aggregating data sets across functions and establishing a comprehensive perspective. This complexity can be further compounded when RCSA data is collected through methods such as questionnaires, which may not effectively convey the purpose and significance of the task, nor instill the necessary understanding of how the results influence the organization. Consequently, this can lead to missed opportunities for cross-functional analysis, such as understanding how risks identified in the RCSA of a procurement function may impact the risk landscape of technology or cybersecurity, particularly in cases where IT solutions have been outsourced.

The response:

'Real time' RCSA, which is dynamic, leverages effective triggers and considers the interconnectedness of risk and controls.

The nature, size and velocity of risks are evolving, and companies must adapt to keep pace. A shift in focus is needed from performing RCSAs at predefined intervals with time-based backstops, to a more dynamic approach. The ongoing monitoring of the risk environment is crucial to identify new risks or when an existing risk requires re-assessment. Therefore, it is beneficial to define a suite of trigger events: a series of potential scenarios that require organizations to re-review the risk environment to identify and assess risk. These could be external, such as competitive, industry and regulatory events, or internal, such as audit and regulatory findings or significant changes in strategy or transaction volumes.

Once triggers are identified they can be underpinned by key risk indicators (KRIs) and monitored to identify any changes that might elevate or help reduce risk exposure. But this represents a challenging task: it is one thing to identify a range of triggers and design a balanced suite of leading and lagging indicators in support of these, but quite another to join-up such data points to drive routine risk assessments and re-assessments. This is where technology can add significant value.

01

Qualifying triggers and KRIs will need to be continually reviewed to remain relevant. For example, the cessation of a particular type of investment account sold to clients will render all triggers related to that account-type obsolete. However, above all, trigger events should prompt the review of a risk-assessment as soon as possible. As such, organizations are turning to monitoring systems that can track KRIs and trigger criteria, notifying senior management when set thresholds are breached. Specialized software applications and tools record and assess risks based on this information, as well as provide proactive monitoring to continually rank risks, mitigate actions and re-calculate risk scores.

02

Accurate and accessible data is needed to perform a dynamic RCSA. Any technology used to enhance the RCSA process is only as good as the data that feeds it. In addition, the RCSA process needs to be conducted on a broad basis across key business activities to help ensure the interconnectedness of risk and controls is appropriately captured. Ensuring software applications or tooling are digitally connected to a suite of relevant data sources can help reduce the burden on risk practitioners, many of whom currently operate human augmented approaches to data collation and enable linkages to be more easily identified and captured. Automated data collection enables organizations to gather large amounts of information from various sources and to aggregate data points to provide holistic outputs. Advanced analytics tools can then analyze the data for comparability, patterns, and trends. For example, controls testing data can be seamlessly interconnected to the risks they mitigate and loss event data can be captured against specific risk categories, including key risks where they may have been 'tagged'. Identifying these areas of data interconnectivity can significantly enrich RCSAs.

03

Some more forward-thinking organizations are already starting to further push the boundaries of technology enablement, for example, there is the concept of 'Digital Twin' technology, which has found popularity in the hazard risk management focused industries such as outer space and motor racing. 'Digital Twins' are virtual simulations of a physical product, process or system that span the digital and real-world environment. 'Digital Twins' can be applied to risk management by collecting real-time data from the live production IT environments across the organization and creating a duplicate. The digital duplicate can then be manipulated and analyzed to test different scenarios in a safe, risk-free environment. In the context of the RCSA, it can enable a convergence of risk appetite and residual risk assessments using a combined view of indicators to derive a real-time or periodic calculation of residual risk. This allows RCSA processes to focus on objectively analyzing forward-looking information and causal factors, identifying a range of potential outcomes from different scenarios.

Ultimately, the business case for moving towards performing dynamic, real-time RCSAs must include reducing the burden on stakeholders to manually collate and process information. Integrating technology within existing systems enables data exchange, can help reduce duplication of effort and supports a holistic approach to risk management.

03

Consistent and efficient RCSA

The challenge:

RCSAs are highly inefficient and lack objective inputs.

When there is a lack of accessible risk and control information and other objective data sources, companies are required to take a more judgement-based approach to risk assessments. However, this subjectivity means RCSAs become prone to cognitive bias and inaccuracies, particularly availability bias.

This is compounded by a lack of evidence of objective controls performance. While controls are often quality assured locally, companies can invest vast amounts of time and effort to test and assure their control environments. Consequently, the exercise to gather and analyze the information for an annual risk assessment, let alone on a more frequent basis, can be time-consuming, particularly when it is not coordinated by a formal control testing program.

The RCSA can sometimes be de-prioritized compared to other risk-related activity, for example, tasks that are perceived as more high profile and without sufficient maintenance of the risk and control environment, this can become neglected over time. This can lead to controls which are poorly designed, incomplete or duplicative and risks may become redundant or outdated.

The response:

RCSAs are driven by streamlined processes and measurable and objective data.

In driving consistency, the RCSA process should be applied uniformly across the organization, including the methodology used, the level and style of reporting required and how control testing results and other key trigger data is applied. This facilitates swift cross-analysis of issues within one area with similar processes in other parts of the organization, enabling the calibration of RCSAs to identify significant trends and overarching themes. Importantly, this method permits the intersection of enterprise-wide oversight on critical topics with a vertical, RCSA-specific perspective. The outcome is a robust control framework that effectively addresses the most substantial risks faced by the organization.

The rationalization and standardization of control libraries can help test the level of completeness, relevance and necessity of controls. This helps companies to develop or refresh, and in some cases eliminate, redundant controls, so that organizations can systematically test the design and operating effectiveness of only those controls that are deemed critical, with the added benefit of driving down operational costs. Process management and the mapping of key processes to controls has gained traction recently, in response to regulatory breaches arising through control gaps within end-to-end processes. Using technologies such as AI and Natural Language Processing (NLP) can help with establishing and maintaining these libraries by rapidly analyzing large amounts of existing risk and control data to show ongoing opportunities for controls optimization and automation.

Leveraging RPA to drive efficiency

By using RPA, when a control failure occurs, a series of next steps can be automatically triggered based on pre-defined criteria.

Control Failure

RPA Analysis

Automated decisions (examples below)

Examples of automated decisions that could trigger a response:

1. **Prompt Human Intervention**
   e.g. a client's account is flagged as needing inspection due to fraudulent activity.
2. **Remedial action triggers automatically**
   e.g. an investment is automatically sold due to a drop in fund performance.
3. **Automated control adjustment**
   e.g. a payment transaction is blocked as fraud activity is detected.

Robotic Process Automation (RPA) can support the efficacy of the risk assessment itself. For example, by performing 'in the moment' validation checks on the way controls are articulated and highlighting any anomalies or errors in controls assessment ratings. RPA can retrieve and extract data from multiple internal systems, databases and spreadsheets, and use the information to apply automatic adjustments to risk ratings, based on pre-programmed parameters set by trigger events and risk and control indicators. Conversely, the implementation of corrective controls can detect and remediate errors or irregularities before they manifest within the risk assessment itself. Even where human intervention is needed, this approach can significantly reduce the potential for inconsistency, ambiguity or subjectivity, and can help companies prioritize where remedial action is required.

Not only can risk assessments be re-adjusted automatically, but in some cases the required remedial action can be automatically activated to bring risks back into appetite, particularly for financial risk-related metrics. In the case of stop-loss orders within the investment banking sector, the holding can be automatically sold should the share price fall below a pre-defined threshold, which limits potential losses. This requires no intervention by the trader and instead can be monitored through effective risk reporting.

Non-Financial Risk (NFR) data has similar potential, with many examples of automated action being taken requiring limited or no human intervention. For example, monitoring the value and frequency of customer payment transactions to identify fraudulent activity or where a customer may have a vulnerability. Similarly, anomalies can be detected through algorithms that utilize historical data and statistical models to identify unusual patterns or deviations. Where set thresholds are exceeded, systems can automatically place temporary restrictions on accounts, block specific transactions or place red flags on customer records, alerting staff to investigate files or contact the customer. Such examples demonstrate the added value not only to the organization but also their customers. By leveraging technology, the 'self' component of the RCSA becomes significantly evolved, replacing human judgement with a fully objective assessment, or at least pseudo-assessment, where employees may still be required to apply judgement in terms of action plan decision making or to review the outputs of insightful reporting.

04

Informative and value adding RCSA

The challenge:

RCSAs are not viewed as a priority or relevant to organizational strategic aims and objectives.

By nature of their title, RCSAs are labeled as 'self-assessments' and their execution can at times be labor-intensive. This level of effort may, on occasion, lead to a automatic 'check-the-box' mindset among staff. Companies become pre-occupied with producing an inventory of risks and controls to report to key committees, rather than focusing on the insight and relevance to their strategic aims and value-driven outcomes. Subsequently the RCSA and strategic planning processes can become misaligned, where the RCSA is seen as a disjointed activity unrelated to the strategic goals of the company.

This results in a disproportionate focus on delivering the RCSA process rather than establishing meaningful insight. Consequently, staff find themselves embroiled in 'firefighting' a series of loss events and breaches, which can take the business 'by surprise', rather than proactively managing and mitigating risk that might otherwise impact the achievement of the company's goals. Without buy-in from the top, the RCSA methodology, accountability, ownership, and application of it will likely vary across the organization. This inhibits an enterprise-wide view of key risk themes and creates difficulties in aggregating risks. It can also create issues in consolidating insights and themes to support strategic decision making for the organization.

The response:

A positive risk culture underpins the RCSA process with strong ownership and accountability by employees.

The importance of securing board level and senior management buy-in for the success of RCSAs cannot be overemphasized, effective buy-in from the top propels business leaders to take full ownership for the RCSA process. Having a positive risk culture promotes greater risk awareness across the organization, which encourages everyone to be responsible for the risks associated with their processes and to put in place effective controls to mitigate those risks. It can also focus managerial attention and budget on investing in the tools required to support effective assessment, as well as driving consistent use of these across the organization. A formalized RCSA framework, with associated standards and guidance, that details roles and responsibilities, risk assessment methodology and a process toolkit to support staff in owning the RCSA and utilizing its outputs are key practical enablers.

The core principle of risk management involves understanding, analyzing and addressing risk to help the company achieve its strategic objectives. RCSA adds value to this process by bringing together the RCSA framework with 'on the ground' employee involvement. Companies must continually develop and build the risk capability of their employees. Key to empowerment and accountability for RCSA is that staff must not only understand the processes they operate, but also how and when to apply the risk assessment methodology and determine any resulting corrective action needed.

Technology becomes a valuable tool to empower key stakeholders to monitor areas of increased risk or control weaknesses with a clear call to action:

01

At senior management meetings and local risk forums, the focus should be on reviewing risk reports and discussing emerging risk themes within business units, escalating issues as needed. Risk committees, on the other hand, should take a cross-functional view of emerging risks and utilize technology-driven management information to enhance analysis, freeing skilled staff from raw data interpretation.

02

RPA technology offers the capacity to streamline reporting by automating manual and repetitive tasks. It can also consolidate diverse information sources via risk management platforms, resulting in the production of real-time, interactive, user-friendly reports, tailored visualizations, and dashboards, along with aggregated risk heat maps. This approach provides valuable insights, allowing users to delve into the specifics of risks and controls, pinpointing the interdependencies between controls and processes and offering a comprehensive, one-stop view of the risk landscape.

03

A collaborative culture is a key enabler to supporting a cross-functional view of themes and insights from the analysis of RCSA. The use of cloud-based platforms and collaboration tools allows risk knowledge and information to be shared in real-time, for example, security or data risk assessments. Communication has evolved and post-pandemic working environments make greater use of instant messaging and video conferencing capabilities which can be harnessed in the RCSA process to boost collaboration, alongside in-person workshops.

04

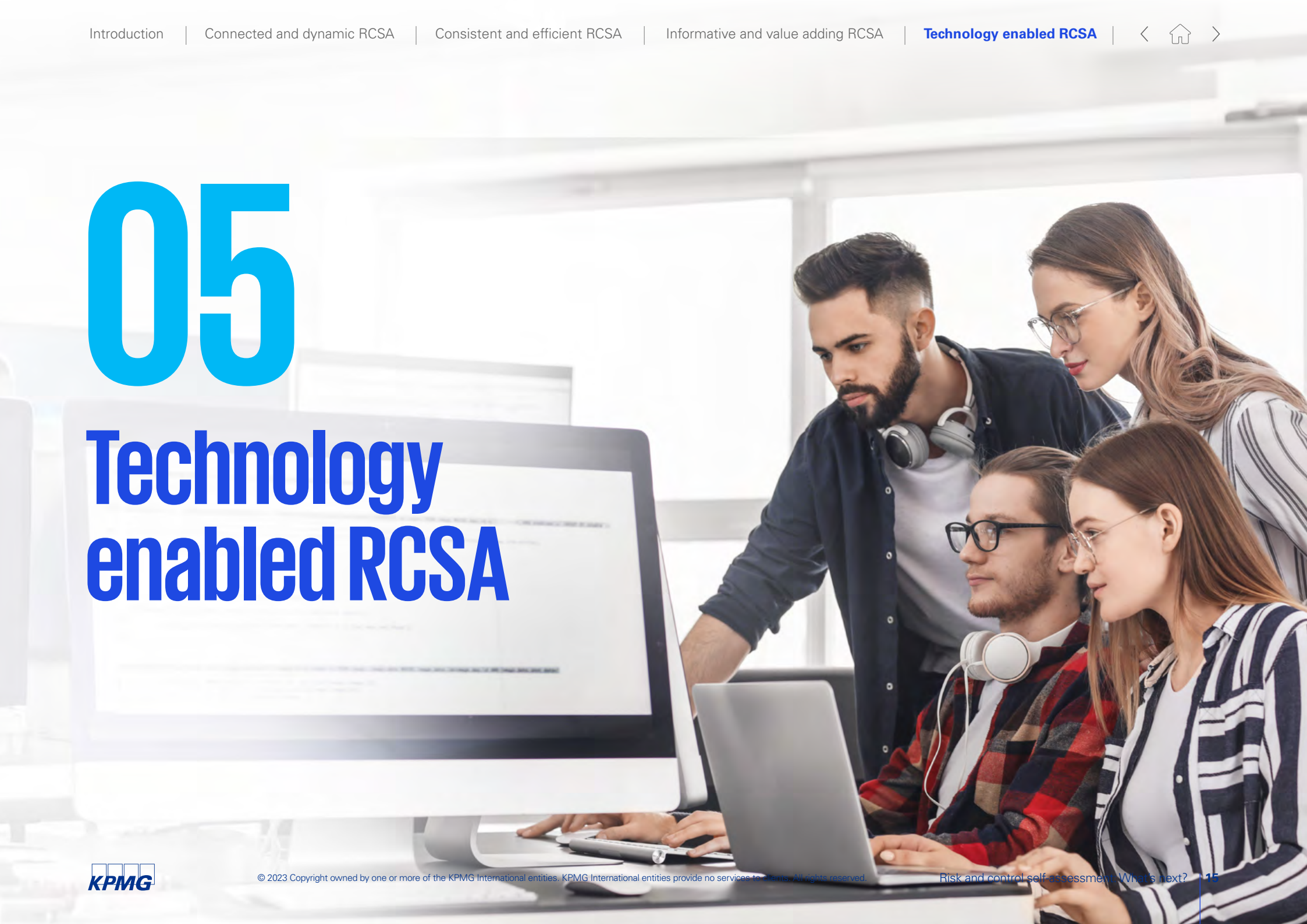
Automating workflows can streamline the steps required in conducting the RCSA and enable timely feedback loops without the need for manual effort. Workflow management software can record and automate the steps involved in delivering an RCSA. This could include assigning ownership of tasks so that actions can be tracked back to owners, setting deadlines and sending reminders and alerts.

05

Building on the benefits of automated reporting, the impact of stakeholder intervention can be tracked through dashboards and reports, which are personalized to different stakeholder groups. Real-time management information can be escalated to stakeholders via automated alerts or prompts, based on escalation ‘rules’ that are programmed into the reporting system, notifying or prompting them when management attention might be needed, for example at distinct stages of a new control or control improvement plan implementation.

05

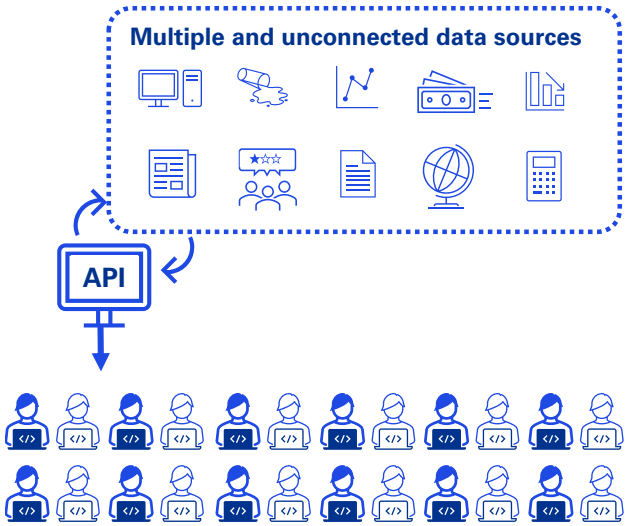
Technology enabled RCSA



Will embracing technology remove the need for RCSAs in future?

Using an API to drive simplification

By utilizing an Application Programming Interface (API), stakeholders can access a wide-range of data through a single API rather than multiple, disparate systems.



RCSAs of the future will likely not only become a standardized decision-making tool used at all levels of management, but also a fully automated risk and control assessment process that interconnects and exchanges data from multiple sources. Some organizations, such as Fintech companies and other start-ups, will likely find the transition to using advanced technological solutions easier, without the heavy burden of legacy systems and platforms that other financial organizations may have.

More traditional organizations may need an incremental journey to move towards a fully digitized RCSA process due to their heritage IT estate, where a range of risk-related software (e.g. governance, risk and compliance tools and RegTech solutions) and other business systems, as well as tools such as End User Computing (EUC) solutions and databases are prevalent. Complex feeds of data further impact the pace at which organizations can streamline their RCSA process. As such, Application Programming Interfaces (API) become key in providing such organizations with the flexibility to simplify the design, administration and the use of existing applications by allowing the API to converse with existing information sources, negating the need to build costly and extensive systems infrastructure.

In the long term, technological enhancements may ultimately negate the need for RCSA altogether. The concept of RCSAs as we know it would cease to exist, as self-assessment becomes a fully automated, real-time process. Manual procedures become obsolete and are replaced by automated feeds into the re-assessment process through AI tools. As the role of risk continues to evolve, the respective roles and responsibility of the first and second line of defense will also transition. The second line should be able to focus on undertaking an oversight and challenge role, driven by insightful, trigger-based outputs. First line employees can take greater ownership of the risk identification and assessment.

Ultimately, it can allow organizations to focus on the pursuit of its strategic aims safe in the knowledge that the risk environment is as well understood as it can be. Technological advances should drive companies to take action to simplify the risk assessment process. The process can be simplified to a point where the inputs required much less attention and the outputs will be reviewed or drive their own action without human intervention. So, while we may one day see the need for an RCSA removed by technological advances, in the meantime embracing a technology enabled RCSA can help maximize value from this important process.

How this connects with what KPMG professionals do?

In the contemporary business landscape, the demand for transparency in risk and control management is on the rise. KPMG professionals recognize the paramount importance of solid risk management practices. The global organization of risk professionals bring a wealth of experience to the table, specializing in enhancing the efficiency and effectiveness of your RCSA processes while eliminating subjectivity.

KPMG professionals appreciate that an efficient RCSA process is the cornerstone of effective risk management. This approach leverages technology, enabling real-time data collection and analysis, empowering you to make well-informed, risk-based decisions. KPMG risk professionals are committed to standing alongside you, bolstering trust, mitigating risks, and unlocking new value, preparing you for the future.

Collaborating with KPMG firms can not only help enhance the effectiveness of your RCSA but also help ensure its alignment with your strategic business goals. KPMG professionals strategize closely with you to help ensure that your risk environment isn't just comprehended but actively and proactively managed by your teams. KPMG firms' adept team of risk professionals can help transform your RCSA into a robust and invaluable tool for risk management, ultimately working to strengthen your organization's resilience with trusted risk management practices.

Contacts

Fabiano Gobbo
Global Leader, Risk and Regulatory Advisory
KPMG International
fgobbo@kpmg.it

Holly O'Neill
Director, Banking Risk
KPMG in the UK
holly.oneill@kpmg.co.uk

Arvind Sarin
Partner
KPMG in Germany
arvindsarin@kpmg.com

Narinder Singh
Partner, Risk and Regulatory Advisory
KPMG in the UK
narinder.singh@kpmg.co.uk

Cameron Burke
Principal, Risk and Regulatory Advisory
KPMG in the US
cburke@kpmg.com

Matt Tottenham
Partner
KPMG Australia
mtottenham@kpmg.com.au

We'd like to acknowledge the contributions of Catherine Cox, Hannah Orisan, Mike Sumun and Alistair Wealthall.

Some or all of the services described herein may not be permissible for KPMG audit clients and their affiliates or related entities.

kpmg.com

Designed by Evalueserve.
Publication name: Risk and control self-assessment: What's next?
Publication number: 139046-G
Publication date: November 2023