IDC

SPOTLIGHT

Sponsored by: PwC

The automation and orchestration of risk management processes is fast becoming a reality that organizations can take full advantage of to accurately understand the current state of risk.

The Value of Automating and Orchestrating Risk Management Processes

August 2023

Written by: Philip D. Harris, CISSP, CCSK, Research Director, Governance, Risk, and Compliance Services

AT A GLANCE

KEY TAKEAWAY

IDC believes the risk management platform market will continue to grow and evolve in the next two to five years as more companies adopt these solutions. This evolution will include risk quantification, simplified control baselines, and financial views and reporting that speak to executives and board members more effectively.

Introduction

For most — if not all — organizations, managing risks has always been a challenge. Increasing and ever-evolving threats, from cybersecurity weaknesses to financial crimes like money laundering and insurance fraud, coupled with digital transformations that seem to be occurring at a record pace, are only adding to this challenge. And poor management of risks can be costly to an organization's reputation as well as its bottom line. Inadequate risk management can result in assessments that take too long to produce, are riddled with inconsistencies and inaccuracies, yield improper recommendations that only partially treat risks, and allow some risks to go untreated. This, in turn, can lead to IT and business dissatisfaction. Poor risk management also can lead to ineffective reporting of an organization's risk posture to senior management and the board of directors, impacting governance and their ability to address potential threats.

An important first step in an organization's risk management is to confirm that effective processes are in place to orchestrate ongoing risk mitigation. Using cybersecurity risk management automation with organized data storage, an intelligent risk register, and standardized control frameworks — in addition to orchestrating risk management processes — can help. These elements are all essential components of an effective risk management program.

Manual Risk Assessment Methodology

Many organizations continue to utilize a manual risk assessment methodology. This often includes some form of questionnaires, standardized checklists, spreadsheets, cobbled-together management reporting, and point-in-time snapshots of their risk posture state. For some companies, their risk management program may only capture application risks versus infrastructure risks or third-party risks — or a combination. These programs might also apply methodologies either developed in-house or from outside consulting firms or vendors specializing in business, financial, operational, and fraud risk. And these methodologies might work in tandem with other relevant internal business and/or finance policies combined with a standard framework.

The number of staff needed for executing manual risk assessments using this model will vary depending upon the volume of work required. Operating a risk management program across an organization can require multiple risk professionals. However, finding and hiring employees with the necessary technical, interpersonal, and risk management skills can potentially be a heavy lift. Professionals with these skills — and who have at least five years of experience — can be difficult to find and recruit. Companies need risk management professionals who can carry on a conversation with the necessary IT and developer teams. They need people who can dig under the policy requirements and "ask the questions behind the questions" to get at the real risks. In addition, these individuals need to possess "thinking outside-the-box" skills that enable them to identify compensating controls where a direct mitigating control might not be feasible.

Another concern with manual assessments is that risk reporting can be cumbersome and unwieldy. When cybersecurity risks are identified in a formal document format, cataloging and understanding all the issues can be difficult. For example, the assessee might lose track of the risks requiring treatment, and the report could become shelfware. Other types of reporting might not answer the questions that interest senior management and/or the board. In many organizations, the risk management team might also catalog these risks either in a central spreadsheet or in multiple spreadsheets. This would then act as a quasi-risk register where follow-up may be needed to address risks in a timely manner.

In addition, organizations might — or might not — have various risk treatment protocols such as risk acceptance or risk avoidance that are captured and cataloged, and ultimately approved by senior management. However, this type of information can be captured in spreadsheets. In some cases, the CISO may be the one accepting the risks or determining the other risk treatment protocols.

The goal of an organization's risk management process is to satisfactorily complete and close the risks to provide an ongoing view of its risk posture. Problems can arise, however, if these in-house manual risk management processes lack a closed loop in the methodology where there is follow up to determine whether risks were remediated.

Another potential issue could occur if the business owner and/or assessee perceives manual risk management as laborious at best and a bottleneck at worst. This could result in making risk management a process that the organization tries very hard to avoid. And this attitude could lead to risks being introduced into the environment unbeknownst to the team, senior management, and the board. In the event of a cyberattack or breach, this lack of awareness could prove disastrous to the organization.

Automated Risk Assessment Methodology

Automating their risk management program is potentially one of the better investments an organization can make today. The automated solution, however, should be one that supports them systematically in the orchestration of their risk management and assessment methodologies. Moreover, it should be a solution that keeps the end customer (assessee) in mind. Its goal should include producing outcomes that encourage the assessee to focus on ways to reduce risks in their area. The assessee should also be educated regarding the reasons for and the importance of identifying and remediating risks — as well as the benefits of this to the organization.

There are many ways that automation and orchestration can assist with risk management. These include providing a platform where the industry methodologies, standards, and regulations are already loaded to enable a consistent application of the assessment process. In such a platform, control frameworks could be prepackaged, enabling selection and mapping of policies to controls and to findings. Organizations could also use these frameworks and policies to provide a common control framework if they need the ability to mix and match frameworks to satisfy global compliance requirements. Consider an ecommerce organization that requires compliance with the payment card industry data

security standard (PCI-DSS) and to the NIST CSF. Having a common control framework enables the company to create an effective baseline from which all risk assessment work is completed. In such a framework, the organization can further tailor cybersecurity risk questions to configure scoring and weightings that better reflect its risk impact.

Automation can help companies orchestrate painstaking activities such as the risk triage process. This, in turn, can help them shepherd the methodology through the entire life cycle of risk management. Automating this process can help them confirm that what they're assessing is properly categorized according to the perceived risk they identified at the assessment onset. It's then possible for them to set appropriate estimates of the timing needed to complete the assessment work. This can help enable the business, IT, or developers to move forward without delay.

Furthermore, the automated risk management solution could enable the organization to then load the risks captured from the assessment into a centralized repository. This repository could automatically create and add the appropriate entries into the risk register. This risk register can act not only as a repository but also as a workbench where the project management, tracking, and closure of risks is organized and communicated to the proper business owners. Doing this can help these stakeholders confirm that risk treatment activities are built into project plans and task lists. The centralized collection of risks will also help the organization analyze and identify risk drivers and controls. This activity could surface ongoing risk themes that could result in approval and budgeting for larger projects to address these potential threats. The risk register could become an intelligent source of work efforts that are sent to the appropriate owners for remediation and are tracked for progress. Once remediated, risks can then undergo reevaluation and be officially closed. Risk acceptances and risk avoidances can be documented, stored, and approved by the appropriate level of executive management and further tagged within the completed assessment.

Having a risk management platform can also help organizations establish consistent reporting so that risk scoring and trends are further visualized in dashboards. This will help security teams provide their senior management and their boards with a consistent reporting mechanism that's clear, unambiguous, and devoid of jargon. Management would now be aware of actions taken such as risk acceptances, risk closures, and risk reduction/remediation trending. Armed with this information, senior management and the board could now ask relevant questions and make more informed risk decisions. This would also empower security teams to create distinct types of reporting for business and technical stakeholders.

Other aspects of risk management outcomes include activities such as defining current state and desired state analysis, creating prioritized road maps, and estimating budget requirements.

Benefits

There are several advantages of an organization automating and orchestrating its risk management processes:

- Both risk staff and business staff could partner more effectively to produce better results instead of being at odds. What creates this effectiveness is certainty. There would now be a platform that helps organizations confirm that the risk criteria they're using is consistent over time. The business could, therefore, be more aggressive in determining if there are other controls or processes that it may need to implement to help confirm that future risk assessments are more complete.
- Bringing clarity to the assessment results can empower the business to implement controls and processes more readily.

- Risk trackability becomes a project management effort that can result in more efficient risk closure. This process could potentially be turned over to a project management office to manage completion and closure of findings across business and technology.
- Scoring, trend analysis, and executive management reporting can be visualized to inform executives about the risks and engage them in more proactive discussions. In today's environment, it's critical that executives and board members are more educated about risks. Enabling this group to make effective risk decisions based upon a complete view of the risk posture can result in laser-focused spending in the right places.
- Freeing risk staff from cumbersome manual processes can allow them to be more productive and spend more time identifying and analyzing risk.

Trends

More service providers are creating risk management platforms that seek to automate and orchestrate risk management programs. Understanding the importance of continuous improvement to the risk management process can enable risk teams to align quickly with the business and develop creative risk mitigation strategies.

Risk quantification is also being introduced to provide more financially relevant information about risks and their impact on the organization. With risk quantification, risk teams can now empower the CISO to interact with executives and board members on a level that's more understandable to the business.

Considering PwC

Designed to provide more insight into how financial risk threats connect to each other and back to the business, Ready Assess is a PwC product that offers organizations a holistic view of evolving risks and helps empower better compliance decisions. This digital platform centralizes the disparate parts of an assessment with visually oriented reporting, intuitive data interaction, and tracking of an organization's activities.

A major Ready Assess differentiator is the knowledge that supports the tool internally. PwC professionals have developed repositories for assessments across disciplines —from risk assessments to transformation readiness assessments — and they've built this into the application. They've developed these repositories over the past several years, and these have been leveraged by organizations around the globe. This platform can be used by other risk functions within an organization such as fraud, finance, and business operations. Enabling multiple functions within the organization to feed risk data into a single platform helps create a powerful risk reporting mechanism that provides a singular view of risk for the entire organization — and not just for cybersecurity.

Another Ready Assess differentiator is the customization that it supports. Ready Assess is a platform baseline that can be easily customized. While an organization is required to conduct risk assessments of distinct types, each can employ its own methodology. PwC's solution was built in a way that effectively balances the flexibility needed to accommodate multiple approaches with the necessary guardrails for a self-service application. This affords organizations the ability to port their methodologies into Ready Assess and augment them further with curated content within the application.

Ready Assess was also built to help streamline and automate certain aspects of the risk assessment process. Among other features, the platform provides a host of capabilities including automated reporting, scoring model maintenance, an integrated audit trail, an ever-expanding library of assessment questions, seamless data integration, and rapid

methodology updates. Ultimately, Ready Assess is designed to empower organizations to think faster and act quicker to stay on top of the ever-changing world of risk management.

Challenges

Platforms that specifically address the need to automate and orchestrate risk management programs and methodologies are a nascent market, and organizations will seek to continuously make enhancements and customizations that suit their own needs.

Ready Assess provides a risk management platform that offers many advantages for all risk management teams across an organization. The challenge will be to have a process in place to confirm that the current elegance of the user interface (UI) does not turn into a deepening series of click-throughs that analysts will have to go through to get their jobs done. Monitoring user interface changes over time — and including real-world practitioners to test these changes — will be necessary to avoid this from occurring.

Conclusion

IDC believes the risk management platform market will continue to grow and evolve in the next two to five years as more companies adopt these solutions. This evolution will include risk quantification, simplified control baselines, and financial views and reporting that speak to executives and board members more effectively.

Slowly but surely, organizations will cease to manage risk via spreadsheets and manual processes. No longer will they be subject to ineffective risk closure and risk teams that produce inconsistent results. Risk management will become a more effective and well-functioning set of processes and activities that will be able to produce the state of risk posture at any time throughout the year or business cycle. And it will do this in a way that is easily understood by all members of an organization with a need to know.

About the Analyst

Philip D. Harris, CISSP, CCSK, *Research Director, Governance, Risk, and Compliance Services*

Phil Harris is the research director for GRCS. He is responsible for developing and socializing IDC's point of view on governance, risk, and compliance across people and processes focused on creating a foundation of privacy and trust with enterprises, IT suppliers, and service providers.

MESSAGE FROM THE SPONSOR

Reimagine Risk, Unlock Opportunity: Risk Management Products from PwC

With decades of industry experience and regulatory knowledge, PwC provides strategic guidance and robust solutions that help organizations solve complex business challenges. Our products are developed in collaboration with PwC practitioners at the leading edge of risk, regulation, controls, compliance and more, to help you navigate one — or all — of the phases you will encounter throughout the risk lifecycle. To learn more about our suite of risk management products or request more information, please visit our website.

IDC Custom Solutions

The content in this paper was adapted from existing IDC research published on www.idc.com.

IDC Research, Inc.
140 Kendrick Street
Building B
Needham, MA 02494, USA
T 508.872.8200
F 508.935.4015
Twitter @IDC
idc-insights-community.com
www.idc.com