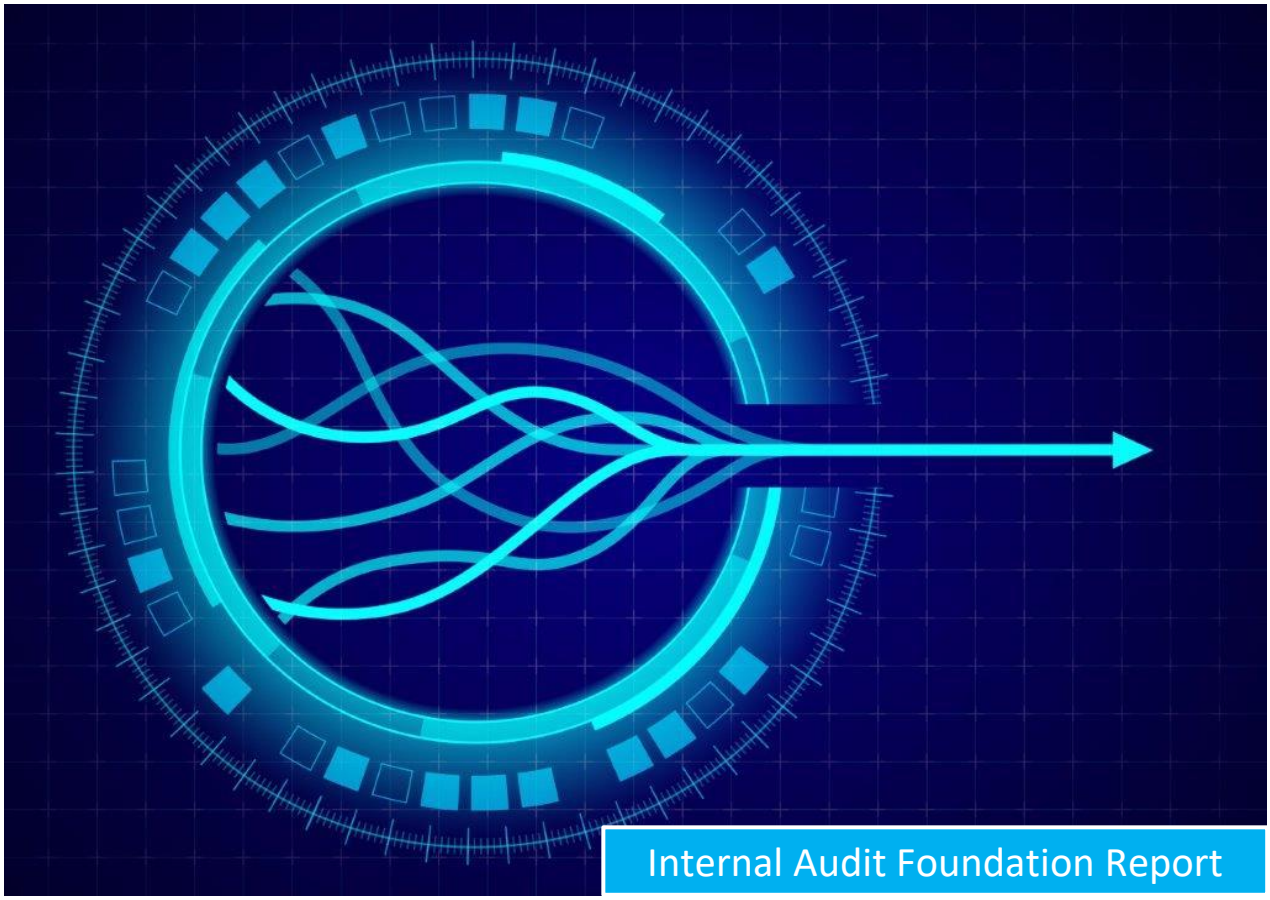


Internal Audit Foundation Report

USING EVOLVING TECHNOLOGIES TO IMPROVE COLLABORATION

How GRC Software Can Support Risk Management and Internal Audit

By Russell Stohr

INTERNAL AUDIT FOUNDATION™

REFINITIV™
DATA IS JUST THE BEGINNING

Published by the Internal Audit Foundation
1035 Greenwood Blvd., Suite 149
Lake Mary, Florida 32746, USA

The IIA’s International Professional Practices Framework (IPPF) comprises the full range of existing and developing practice guidance for the profession. The IPPF provides guidance to internal auditors globally and paves the way to world-class internal auditing.

The IIA and the Foundation work in partnership with researchers from around the globe who conduct valuable studies on critical issues affecting today’s business world. Much of the content presented in their final reports is a result of Foundation-funded research and prepared as a service to the Foundation and the internal audit profession. Expressed opinions, interpretations, or points of view represent a consensus of the researchers and do not necessarily reflect or represent the official position or policies of The IIA or the Foundation.

ISBN-13: 978-1-63454-122-0
25 24 23 22 21 1 2 3 4 5 6

Contents

INTRODUCTION

Internal audit's ability to innovate is critical to success in today's business environment. In November 2020, the Internal Audit Foundation helped conduct a survey to understand the use and planned future use of technology in internal audit. The survey was distributed in North America to chief audit executives (CAEs), directors, and managers working in the internal audit profession; 134 responses were received. Respondents reported that 50% of their internal audit functions are still using manual technologies (spreadsheets, SharePoint, etc.) to complete internal audit management activities, potentially not taking full advantage of the benefits that evolving technologies offer. It is important for internal audit functions to continue to develop an innovative mindset and update existing methods of performing audit engagements. Governance, risk, and control (GRC) is one type of technology that has recently evolved and functions may find useful.

GRC has traveled a long journey since 1995 when the first software to support audit management was released. GRC technology moved to the forefront in the early 2000s, after the U.S. Sarbanes-Oxley Act of 2002 was enacted. Soon after, organizations struggled to organize information related to their processes, risks, and controls.

Over time, the early applications expanded to other areas of practice within assurance, including operational risk management, IT governance, and vendor risk management. Many ended up with different, disconnected technologies (for example, an audit program from one vendor, a third-party risk program from another vendor, and a risk management program from yet a different vendor). As organizations labored to gain an aggregate view, they experienced extensive redundancy and a lack of value from investments in these technologies.

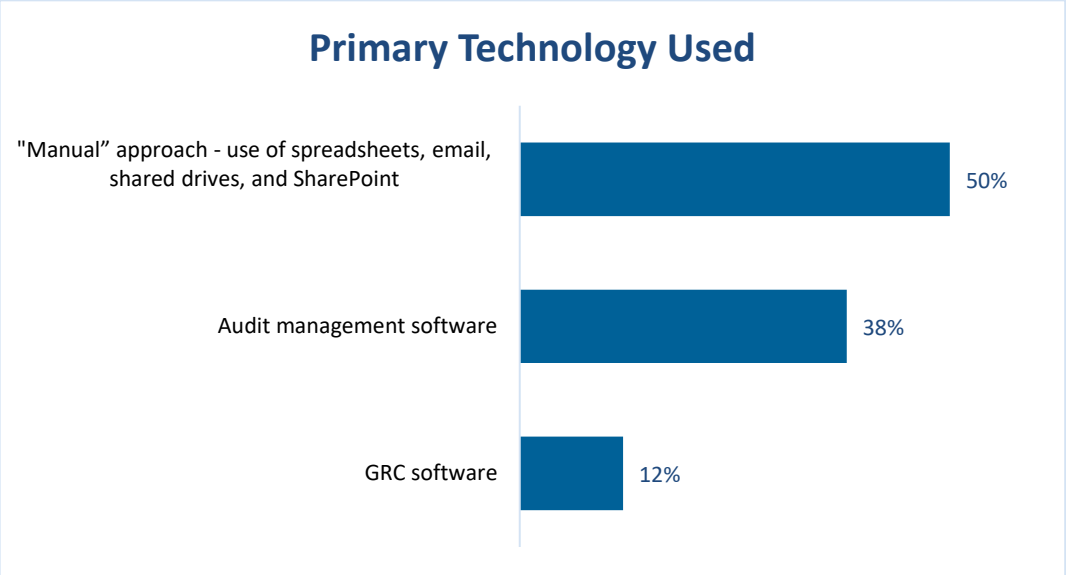
Technology and advisory service providers then started to emphasize the importance of an integrated technology platform. Most of the assurance applications were on a single platform provided by a single vendor, and it was assumed that this would accomplish the integrated requirements from the business perspective.

In many ways, the current environment is still in a similar state. The surviving providers are consolidating around platforms where there are various modules that coexist on a single application and are able to talk to each other. From a user perspective, this is a good move forward. However, the integrations have become more complex and there is a greater need for customization. Not only is it difficult to keep current on these technology stacks, but organizations are also realizing that the ability for those applications to interact with the information and data available in the outside world is limited.

It is time for the next evolution of GRC technology.

GRC TECHNOLOGY: TODAY AND TOMORROW

The market is now at a crossroads where many organizations are looking at platform investments and thinking that it is time to re-architect their GRC technology. The November 2020 Foundation survey found that only 12% of respondents currently leverage GRC software in their audit management processes. Changing conditions since January 1, 2020 led 21% of internal audit functions to increase their use of these technologies to collaborate, communicate, and increase productivity, while more than 40% of functions now have plans to implement GRC technologies post 2020 to help address internal audit challenges.



Organizations are looking at an integrated ecosystem of technologies driving toward two outcomes:

1. Enable the organization to better leverage the vast amount of data that it is capturing across internal and external (third party) sources to inform decision-making and move to a "connected platform." A goal is to bring more information to end users so they are better prepared to provide a good viewpoint on risk and the effectiveness of controls.
2. Allow the organization to support collaboration between second- and third-line roles. Strong GRC can strengthen second-line functions so third-line roles can rely on them and move toward combined assurance. GRC now enables a more collaborative enterprise risk management (ERM) program, while combined assurance gives a broader view of risk and management.

Understanding that there is a tremendous world of emerging technologies, including machine learning, artificial intelligence (AI), and natural language processing, organizations do not always know the best way to implement them. New GRC architectures need to be scalable so users can plug in new technologies as they become available to gain direct value.

A good example is using emerging technologies to embed regulatory risk data in a change management process. In addition to seeing enacted law and pending changes, the organization can receive reports on where regulators are issuing enforcement actions and what topics they are focusing on in their speeches.

AI and other innovations are uniquely suited to help organizations surface, visualize, and act on regulatory issues for optimal benefit.

Organizations are now focusing on GRC technologies that facilitate a flexible ecosystem of systems and data. This will enable teams to access more data and ultimately get to a world where they can embed more cognitive capabilities into the GRC ecosystem to drive decision-making and automate processes.

Emerging Technologies and the Three Lines Model

The Three Lines Model from The Institute of Internal Auditors (IIA) helps organizations identify structures and processes that best help to achieve objectives and facilitate strong governance and risk management.

First-line functions lead and direct actions, as well as apply resources to achieve the organization's objectives. First-line roles communicate with the governing body, maintain processes for managing operations and risk, and ensure compliance.

Second-line functions provide risk management practices and objectives, such as compliance with laws, regulations, and acceptable ethical behavior; internal control; information and technology security; sustainability; and quality assurance.

The third line is internal audit. Third-line roles communicate independent and objective assurance and advice to management and the governing body on the adequacy and effectiveness of governance and risk management to support organizational objectives and continuous improvement.

Very few organizations today have platforms that do more than manage task assignments, collect information on processes being performed, and issue reports. These platforms are not at a point where they are making the business smarter or putting the business in a better position to anticipate and react to things that may cause harm.

GRC Technology Evolution

Early 2000s
Early roots of GRC focused on applications designed to support a single area (for example, internal audit, a Sarbanes-Oxley process, or an IT governance process), but were not usually integrated.

Mid 2000s to Current Time
Next-generation technologies began focusing on integrated GRC platforms, where vendors expanded services by adding more modules to their platforms. Organizations tended to use a sole vendor.

Transitioning Now
Realizing that the previous architectures will not serve their future needs, organizations are transitioning to an open model where they can plug in the best-in-breed applications from multiple vendors to meet specific needs and gain new benefits.

Many GRC platforms were developed from workflow or form-based platforms to capture information. The embedded data models are fairly rigid, hard-coded, and begin to suffer performance degradation around millions of records. These technologies simply won't scale to manage the volumes of data available in today's enterprises.

With the siloed model, there were problems with repetition and the ability to share data among teams. This usually had the greatest impact on the first-line roles. For example, IT may have asked the first line about a control, the Sarbanes-Oxley team might have asked about the same control, and then internal audit might have asked for evidence of the same control. Teams were not able to rely on the work already performed, creating a lot of overhead without much benefit to the business. Asking about controls did not help the first line improve processes or controls, nor to better understand how the business was running.

When the architecture transitioned to multiple modules from one vendor on one platform, there was a weakness in that the developers were deciding how the interactions would work, even though each

organization's assurance function had its own unique needs and processes. This forced extra customization, which proved expensive and difficult to keep updated, both from a vendor and a business standpoint. Although better than the previous ad hoc model, it was still not as efficient as possible.

Another challenge facing businesses today is shrinking budgets. Organizations need to get more out of the technology and staff they already have, while expanding deliverables and refocusing on business value. For example, they may want to increase coverage into new regulatory areas such as data privacy and operational resilience. Therefore, they are asking questions such as: "How do we make our technology better?", "How do we add more value?", and "How do we gain more insights in an intuitive and intelligent way?"

Solutions for the Future

To address current challenges, organizations need to think about expanding or adopting GRC architecture and consider multiple applications/technologies that better suit business and assurance needs. By integrating applications, teams can share information from both internal and external sources, which improves decision-making. It also creates efficiencies, such as second- and third-line roles being able to avoid asking first-line roles about a control, instead having direct sightline into details to find out how many times a control was executed and if there were discrepancies. All three lines would benefit from seeing where a process might be impacting the business, enabling the organization to identify where it may need to make changes.

The Art of the Possible

An important disruptive innovation is fueling the next generation of GRC platforms—zero-code and low-code applications. These require little to no programming, which enables organizations to quickly build and deploy dynamic custom applications and remove barriers to embedding new data into processes to improve decision-making. The organization can then change the application without modifying the underlying source code.

For example, the internal audit team and the risk team look at the organization in different ways. With a traditional approach, these groups would have to adapt to the other's view, making each function less effective. Zero code removes these constraints. It allows each assurance function to define the way they think about the business, the metadata, and taxonomies, while still being able to consolidate data for analysis and reporting.

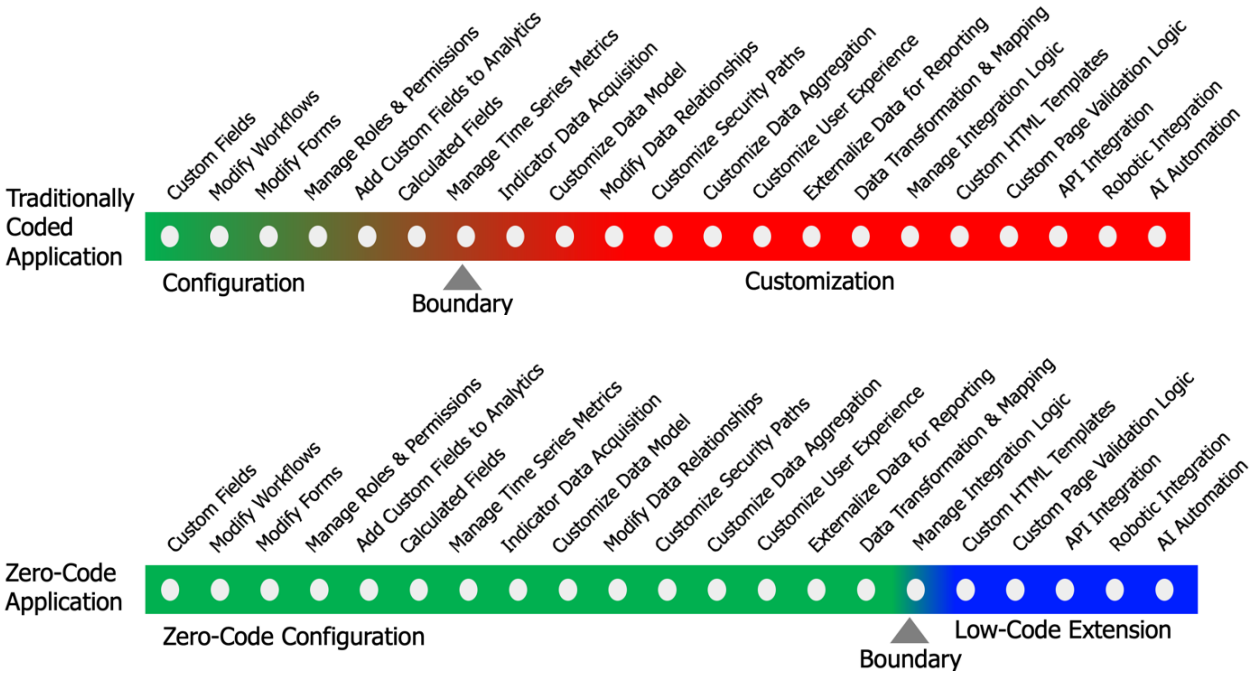
Another advantage of zero code is the business now has control over the application, data model, and user experience. If a team wants to bring in transactional data from the accounting system, sales data from a customer relationship management (CRM) system, and combine with a data feed from a third-party risk provider that looks at incidents in the market, they can integrate that information into a single view to inform a first-line business user on the risk assessment process. They can also see how processes are performing from a transactional basis, how the business is doing financially related to its goals, and what similar businesses are experiencing that may impact this business.

Modern GRC architecture should feature a zero-code platform as the centerpiece of the ecosystem architecture. Technologies are typically very strong enablers of integration, allowing organizations to still leverage best-of-breed applications. Zero-code platforms are often available with a wide range of prebuild solutions with contemporary best practices built in, enabling faster time to value and fewer implementation barriers. Zero-code applications are also remarkably good at filling application gaps (i.e., all the nagging micro processes the organization still has that are enabled in spreadsheets and email).

Frequently replacing these processes with commercial off-the-shelf applications, if available, or custom internal IT development is not a commercially viable option. In contrast, a zero-code platform can often convert spreadsheet and other desktop application-enabled processes into fully enabled applications in a few hours or days while enhancing security, auditability, and integration. Zero code is a remarkable step

forward in application development paradigms, drastically reducing internal IT costs and enabling IT teams to better service the GRC functions, while retaining critical IT development skillsets to focus on core business priorities.

Figure 1: Traditionally Coded Application vs Zero-Code Application



EMERGING GRC TECHNOLOGY USE CASES

With the breadth and fast-paced development of emerging technologies, it is more important than ever that end users have the ability to easily see information, visualize broader boundaries, and conceptualize them to enhance business preparedness and decision-making. The following cases demonstrate the use of GRC technology.

Case One: Emerging Regulatory Risk in a Global Bank

A European-based global bank had a decentralized regulatory compliance management approach. Each region in which it operated had its own compliance office, which was responsible for identifying and mapping the legal and regulatory obligations for the specific jurisdictions in the region. While each compliance office had reasonably good processes, the disparity in the processes and technologies used made it difficult to create and monitor a global view of the bank's obligations and regulatory change management. This led to a wide range of issues, but most significantly the bank missed some important requirements, was fined, and was issued a matter requiring attention (MRA).

To rectify this, the bank decided to centralize the regulatory library and change management processes while still retaining the added jurisdiction-specific expertise and focus of the regional compliance offices. This hybrid approach would ensure global visibility and cross-regional coverage assurance. Further, a single global regulatory event feed would be implemented, covering all regions and augmented by additional jurisdiction-specific feeds where further state/local/provincial coverage would be required. The bank wanted to augment its regulatory change management processes with an additional source to focus specifically on emerging regulatory risk analytics. This enabled each of the regional offices to adopt a more risk-aware prioritization in their processing while improving overall management reporting value from the solution.

The bank selected a leading zero-code GRC platform and regulatory compliance solution package as the foundation of the new solution. The platform featured a zero-code architecture that would enable the bank's specific hybrid model objectives without customization. Critically, the solution supported the multifeed requirement and was pre-integrated with many of the leading content providers, including regional-specific providers.

For the central data feed, one of the key objectives was to receive the regulatory requirements in a granular, machine-readable, and tagged format. This would allow the bank to adjust the granularity of mapping specific to each rulebook. In some cases, specific sections would be mapped directly to the organization's taxonomy and obligations; in other cases, it would be done at the subsection or rulebook level. This flexibility would ensure optimization of the workload generated by the change management feeds—a critical consideration.

The technology selected used a combination of neural network models and natural language processing to automate the consumption, conversion, and tagging of global laws and regulatory requirements that were automatically fed into the zero-code platform through a prebuild integration. The quality of the tagging greatly facilitated mapping to the organizational taxonomy, significantly reducing the time and effort to establish the centralized regulatory library. The regional feeds came from an additional four vendors with specialization in content for the four largest regions by risk. Each feed arrived in the system through different interfaces, but the central platform supported the harmonization of the content, checking each source against the centralized feed and managing redundancy.

Last, the bank used an additional feed focused on emerging risk analytics. This vendor had developed specific AI algorithms to monitor law and regulatory body sources for the occurrence of thematic references and enforcement actions, highlighting areas of specific and heightened focus for each body. This source was cross referenced through a common taxonomy of obligations to the bank's regulatory library. The combined solution provided management and each compliance office with an enhanced view into what regulators were focused on going forward, enabling better preparation for the future.

By leveraging an ecosystem-based approach, the bank was able to identify the best-of-breed providers for each of the core requirements. The zero-code application platform enabled it to merge the technologies and data into one seamless solution that was fine-tuned to the bank's specific hybrid operating model. The combined state-of-the-art solution significantly improved the consistency, quality, and efficiency of the bank's regulatory compliance processes while providing senior management with global visibility and heightened confidence in their coverage.

Case Two: Operational Resilience and Crisis Monitoring in a Large Global Technology Service Provider

As with many businesses, the days and weeks following the March 2020 COVID-19 shutdowns strained every aspect of the organization's service provider infrastructure, customer service, and third-party management infrastructure. This global technology firm provided a broad range of application and data services to several corporate and financial services firms. In addition to the complex internal dependencies to maintain continuity of services, many of the products and services had complex third- and fourth-party dependencies. The business continuity planning for the internal dependencies held up well, and the organization had no challenges maintaining its own operations.

The organization quickly realized, however, that it was struggling to keep up with the daily/weekly requests for impact and continuity information from its customers, and it was simultaneously finding the same struggle getting timely responses to requests for impact and continuity analysis from its critical third-party providers. The problem was further exacerbated by a lack of integration among its third-party risk management, procurement, and contract systems; service inventory; and CRM systems. This lack of integration caused difficulty in identifying where third-party dependencies intersected with products and services, and ultimately customers' portfolios. This made it extremely cumbersome and time-consuming to assess the potential continuity impact for any one individual customer, given the specific mix of products, services, and service-level agreement (SLA) commitments for that particular customer.

With no near-term relief from the growing pandemic in sight, management, with support of the second- and third-line functions, began a detailed assessment of the impacts and knowledge gained from the first few months of the outbreak. It determined immediate action would be taken to develop a fully integrated operational resilience capability. The solution would enable the organization to directly connect each product and service it offered with its third-party dependencies and risks, contractual SLAs and performance, CRM systems, and ultimately with its human resource (HR) system for critical employee information. The primary objective would be to enable the organization to provide a near real-time continuity analysis for any specific customer or service. The system would be extended to enable critical third-party service providers to offer the organization more dynamic updates on their own continuity assessments. Last, the system would enable the organization to monitor global events, beginning with global monitoring of COVID-19 impacts, in the context of its product and service offering to better anticipate events that could be leading indicators of potential service disruptions in the future.

The second line, with support from IT, was charged with defining the architecture and supporting solutions. At the time, no commercially available solutions for the specific approach to operational resilience appeared to be available on the market. Wanting to avoid a costly custom development project, the team reached out to the solution provider for its operational risk management product. The technology was based on a true zero-code technology, and the hope was that its OpRisk solution could be extended with the necessary data structures and functionality. They quickly discovered the provider was already working on a new solution template for operational resilience, and while not a complete match for the firm's specific

requirements, the template would provide a substantial head start and some additional functionality the firm had not considered. With the platform already installed, the group was able to implement and configure the template to its foundation requirements and begin to provide management reporting through the new application.

In addition to modeling the complicated data relationships, workflows, and reporting in the new operational resilience solution, the technology needed to be tightly integrated with other applications already in its ecosystem, beginning with the third-party risk management system, CRM system, and customer support ticket systems. These integrations were iteratively layered into the application to enhance the users' access to critical decision support data. Additional integrations are planned for the future.

With the basic operational resilience functionality and data mapping completed, the firm turned its attention to the global monitoring componentry. It selected an innovative AI-based technology that leverages a cutting-edge combination of AI and machine learning to scan, tag, and index millions of global sources in 42 languages. The technology provided user-defined channels, dashboards, and dynamic alerts to deliver highly relevant news, research, and market analytics in real time. The provider had already applied its technology to the development of a COVID-19 tracker and was pre-integrated with its operational resilience platform. Today, the firm is actively monitoring COVID-19 variant outbreaks in geographies where it has critical dependencies on third-party service providers, and it is also working on defining several additional trackers to surface other types of political, social, and economic news.

The use case illustrates how firms that have adopted an ecosystem architecture approach to their GRC infrastructure and use zero-code platforms as a core component of the architecture can quickly adapt to changing business dynamics. They can do so with a level of agility that significantly exceeds more traditional development approaches and outpaces the ability of traditional application providers to innovate and adapt to market requirements.

MOVING TO AN INTEGRATED ARCHITECTURE

Leading firms are evaluating their overall architectures and making critical realizations that their traditional GRC technologies are not well-suited to a forward-thinking integrated information environment. To address this, they are now shifting to an ecosystem of technologies where there is a fundamental underlying architecture that controls how information and data are shared across them, and then plugging in on top of that either a best practice solution that fits the specific need or a technology that the organization can build and grow internally.

This is again where zero-code and low-code applications serve an important role. The concepts behind them have been around for a few years, but they are now experiencing a surge of interest because they can help an organization meet its requirements today and put it in a capable place to address dynamic needs.

Underlying this is cost efficiency, which is a key consideration as budgets undergo greater scrutiny. Many firms are looking to enable the business side of the assurance functions to have more control over the assurance applications. This way, smaller changes, such as adjusting a workflow or changing an organizational structure, do not require as much of a heavy lift from IT development resources. Rather than having to code from scratch, IT can turn applications around in hours or days instead of months or years.

Three Ways Assurance Functions Can Harness Future Value

As business and assurance leaders look to gain value from next-generation architectures, three aspects stand out:

Flexibility and Speed

Many assurance functions are limited by the technology they are using. For some, their policies and processes have moved forward to meet the needs of the changing market and regulatory environment, but their existing technology makes it difficult to keep pace.

The first thing to look for in a new architecture is flexibility to redefine the application—from its most fundamental underpinnings, to the data model, and all the way through the user experience. By doing that, the second- and third-line functions are able to tailor their applications from a support standpoint to be more efficient, make better use of IT resources, and greatly reduce redundancy.

The Information Advantage

There is so much data available today, both internal and external, that any next-generation architecture needs to improve decision-making within all first-, second-, and third-line roles. Using information sources and assurance processes is where the next round of value will be generated. Leaders must ensure that this is done in a way that is contextually specific and attuned to each user's role.

Integrated, Usable, and Secure

To have real impacts on efficiencies, the efforts of the assurance functions should be closely integrated so they can share work performed. For example, a group that is focused on operational resiliency may uncover items that should inform decision-making in the group focused on third-party risk and the group working on business strategy. Being able to share information across applications increases control and usability.

Today's environment requires a security model that enables and tightly controls the integration among the applications. If enabled, the organization can reduce duplicate testing activities and, through one course of action, more efficiently remediate numerous issues across multiple assurance functions. This opens the door to additional cost savings and improved use of skilled resources.

MAINTAINING INDEPENDENCE

Independence, Not Isolation

Third-line functions (internal audit) should be able to view information produced by second-line functions and use it to inform their own planning processes while still maintaining independence and the ability to state their assessment of the health of the business. In many cases, this creates a conflicting view—the business thinks it has a level of risk exposure that is within its tolerance, but internal audit may have an opposite view. As a result, independence without isolation is critical to making information available while still maintaining clear security boundaries around that information.

The area of highly sensitive issues is a good example. Internal audit needs to have visibility into the issues, but some areas of the business should not. Legal may even specify that some issues are so sensitive that only the CAE has access. So, from an architecture standpoint, the business needs the capability to produce a level of granular security that enables sharing without exposing information that should not be shared.

As organizations explore new architectures, one key capability to enhance is collaboration across first-, second-, and third-line roles, while maintaining confidentiality and privacy. One way to do this in second- and third-line functions is to introduce the ability to stand up micro applications that uniquely and independently support each of the assurance functions in an optimal way. This allows the business to understand how the data shared among these applications should interact. Questions to ask at this point include: “What information should be shared, and at what point?”, “At what level of granularity should it be shared?”, and “Who should it be shared with?”

Emerging technologies and independence come to the forefront in enabling third-line roles to present a unique perspective of the business that is informed with data in a way that was not available in the past. This allows these roles to come to the table with an added value beyond identifying outstanding issues. Internal auditors can also present a case for how to help the business by addressing issues such as future hurdles to avoid, market perception of the business, emerging regulatory risks, pain points experienced by similar businesses, how to navigate through a global crisis such as a pandemic, and new perspectives on how the business thinks about its operation that might change its course for the better. Independence and collaboration, both in terms of access and visibility of data and information, bring value to the business.

SUMMARY

Harvesting New Value for the Future

Organizations that are on the forefront of innovation and driving the market from a thought leadership standpoint are clearly moving toward an architecture that is open, flexible, and focused on a connected ecosystem of technologies. They are also ramping up use of zero-code and low-code applications both in terms of enabling assurance functions to take more ownership and control of their applications and processes, and as a way to allow IT groups to respond more quickly to emerging business needs at a lower cost and lower resource impact.

These leading firms are taking inventory of the market, choosing the best-in-breed in emerging technologies that offer unique innovations, and plugging them into their systems to best inform decision-making now and as the market changes. This way, they access a value proposition to help the business achieve its goals and objectives while staying within the boundaries of internal policies and regulatory requirements.

As assurance leaders continue to evaluate their readiness to take advantage of these emerging innovations, there are several key questions to ask:

System-Focused Questions

Does today's technology still fit the purpose? Does it match internal policies and procedures when performing assurance processes today, or are teams working outside the system and entering data on the back end? Does the system need enhancements? Is there a long wait time, complexity, or a large cost associated with making changes? Are there barriers that prevent the system from keeping pace with the work that needs to be done?

Value-for-Use Questions

Is organizational leadership receiving value for use out of these applications? Are they getting more out of the application than they are putting in? Is an application simply a repository for tracking information and notifying team members when tasks are due and overdue? If it is the latter, then they are most likely not receiving appropriate value for use.

Insights Questions

Does the technology also support first-line function responsibilities? Does it help inform decision-making at any step of the process? Does the technology provide the ability to evidence what information was available at the time a decision was made? When looking at a dashboard, does it provide more than just an operational view? Is it giving insights into emerging risks? Is it showing areas of the business that might need additional focus? Does it highlight hot spots from a regulatory standpoint? Can the right people see areas where there should be greater concerns around incidents or loss?

Force Majeure Questions

Is the technology helping teams understand the impact of natural disasters, pandemics, and other force majeure causes of delay? Is it providing data that will help guide the organization to the best possible outcome in a challenging time?

Innovation Questions

Is the application ready to ingest future innovations? Is it ready for new plug-in capabilities? Does the application need a lot of customization? Is it difficult to keep it up to date? Is there a long lead time involved with requesting modifications, whether through internal IT support or the vendor?

Answering these questions will help determine whether or not today's technology platforms will continue to add value. If they do not allow the organization to efficiently incorporate new capabilities, the value for service is limited, as the aging of applications will only accelerate.

This is a good time and starting point for organizations to evaluate their underlying architecture and develop their go-forward strategy. It starts with evaluating where they are today, taking a realistic view of where they want their investment to be, and assessing if they are ready to take advantage of the full breadth of innovations now and in the future.

ABOUT REFINITIV

Refinitiv, an LSEG (London Stock Exchange Group) business, is one of the world's largest providers of financial markets data and infrastructure. Refinitiv provides information, insights, and technology that enables customers to execute critical investing, trading and risk decisions with confidence. By combining a unique open platform with best-in-class data and expertise, Refinitiv connects people to choice and opportunity – driving performance, innovation, and growth for our customers and partners. For more information, visit Refinitiv.com.

ABOUT THE INTERNAL AUDIT FOUNDATION

The Internal Audit Foundation strives to be an essential global resource for advancing the internal audit profession. The Foundation's research and educational products provide insight on emerging topics to internal audit practitioners and their stakeholders and promote and advance the value of the internal audit profession globally. Through the Academic Fund, the Foundation supports the future of the profession by providing grants to students and educators who participate in The IIA's Internal Auditing Education Partnership Program. For more information, visit www.theiia.org/Foundation.