White Paper

MASTERING RISK WITH DATA-DRIVEN GRC

A STEP-BY-STEP APPROACH TO INTEGRATING GOVERNANCE, RISK MANAGEMENT, & COMPLIANCE (GRC) PROCESSES TO DELIVER TRANSFORMATIONAL VALUE

Galvanize

Contents

Overview

The world is changing. The emerging risk landscape in almost every industry vertical has changed. Effective methodologies for managing risk have changed (whatever your perspective: internal audit, external audit, consulting, compliance, enterprise risk management, or otherwise). Technology itself has changed, and consumers expect to realize more value from technology that is more approachable, at a lower cost.

How do these factors drive change?

Emerging risk landscapes

Risk has the attention of top executives. Risk shifts quickly in an economy where "speed of change" is the true currency of business. It emerges in entirely new forms in a world where globalization and automation are forcing shifts in the core values and initiatives of global enterprises.

Evolving governance, risk, & compliance methodologies

Across risk and control oriented functions spanning a variety of audit functions, global organizations are acknowledging a need to provide more risk coverage at lower costs (measured in both time and currency), which is driving re-inventions of methodology and automation.

Empowerment through technology

In most organizations, there is no coordinated effort to leverage organizational changes emerging from newer technologies such as cloud, mobile, and social media. These factors are essential in developing an integrated approach to mastering risk management. The emerging opportunity is to leverage the change that is occurring, to develop new programs—not just for technology, but also for the critical people, methodology, and process issues. The goal is to provide senior management with a comprehensive and dynamic view of the effectiveness of how an organization is managing risk and embracing change, set in the context of overall strategic and operational objectives.

Where are organizations heading?

The term "data-driven GRC" represents a consolidation of methodologies, both functional and technological, that dramatically enhance the opportunity to address emerging risk landscapes. This maximizes the reliability of organizational performance.

This paper examines the key opportunities to leverage change—both from a risk and an organizational performance management perspective—to build integrated, data-driven GRC processes that optimize the value of audit and risk management activities, as well as the investments in supporting tools and techniques.

Stakeholders of GRC processes & technology

The Institute of Internal Auditors' (IIA) "Three Lines of Defense in Effective Risk Management and Control" model specifically addresses the "who and what" of risk management and control. It distinguishes and describes three role- and responsibility-driven functions[2]:

- Those that own and manage risks (management – the "first line")
- Those that oversee risks (risk, compliance, financial controls, IT – the "second line")
- Those functions that provide independent assurance over risks (internal audit – the "third line")

The overarching context of these three lines acknowledges the broader role of organizational governance and governing bodies.

> *"Traditional audit roles are expanding to risk and compliance, creating a need for GRC technology to support the three lines of defense in effective risk management: Operational Management, Risk Management and Compliance Functions, and Internal Audit. Bridging the current gaps between these lines of defense is critical to improving communication and integrating GRC activities across an organization."*

Richard Chambers, President and CEO, The Institute of Internal Auditors

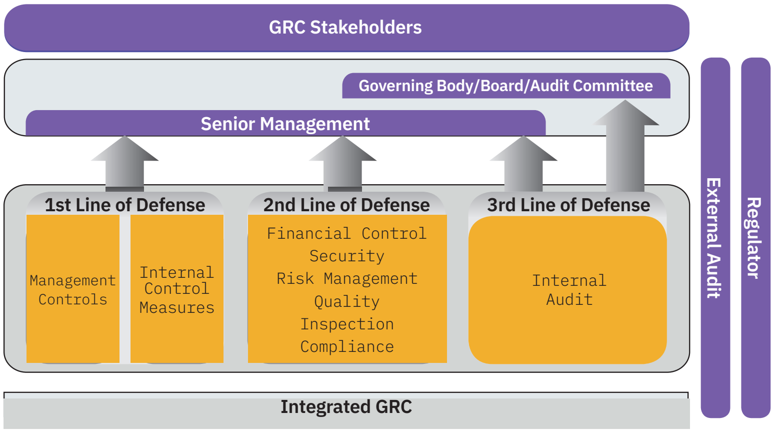

Figure 1: *The IIA's "Three Lines of Defense"*[3]

Technology deficiencies in the Three Lines of Defense

Since the emergence of Sarbanes-Oxley, the use of technology in risk- and control-related processes has truly started to take meaningful shape in many organizations. However, when looking across the risk and control-oriented functions in most organizations, technology is still typically used on a departmental or point solution basis.

[2] *The Institute of Internal Auditors (2013) "The Three Lines of Defense in Effective Risk Management and Control"* *https://na.theiia.org/training/templates/Pages/The-Three-Lines-of-Defense-in-Effective-Risk-Management-and-Control.aspx*

[3] *Excerpted from The Institute of Internal Auditors (2013) "The Three Lines of Defense in Effective Risk Management and Control"* *https://na.theiia.org/training/templates/Pages/The-Three-Lines-of-Defense-in-Effective-Risk-Management-and-Control.aspx*

Third line (internal audit) use of risk & control technology

For the past decade, surveys of internal auditors have consistently identified more effective use of technology as among the most pressing issues facing the profession. Specifically, the responses to the surveys referred to the need for increased use of technology for audit analysis, fraud detection, and continuous auditing. Other surveys also highlight a shortage of sufficient technology and data analysis skills within audit departments.[4]

During the past decade, the role of the internal audit function itself has changed considerably. Internal audit's traditional focus on cyclical audits and testing internal controls is evolving into one in which they're expected to assess and report on the effectiveness of management's processes to address risk overall. This often includes providing guidance and consultation to the business on best practices for managing risk and compliance within process areas and maintaining effective control systems.

The use of technology is an increasingly critical component of these best practices and in some cases internal audit is able to champion the implementation of high-impact, high-value technology within the business's risk management and compliance processes, based on their own experience in using technology for assurance purposes.

There is considerable variation in the extent to which internal audit departments leverage technology. However, it's fair to say that for audit to be truly valuable and relevant within the context of organizational strategy, a significant improvement is required across the board.

Internal audit as a profession is not moving forward at the pace of technology. Some specific statistics from recent research reveals:

- Auditors feel they aren't keeping pace with technology innovation, with 83% of a PwC survey stating slow technology adoption in their organizations.[5]
- Audit programs for specific business process areas and industries are usually developed through a combination of previously used programs and those shared on various audit-related websites. This approach does not address organization-specific risk.
- Next generation testing techniques, especially data analytics, are overwhelmingly under-used.[6]

Second line (risk, compliance, financial controls, IT) use of risk & control technology

Outside of audit, in other areas of risk and compliance, some organizations have acquired specialized departmental software. However, the majority use only basic Office tools to maintain inventories of risks, document controls, and perform risk assessments.

In larger enterprises, it is not unusual to have a variety of technologies and approaches applied in different business areas. This approach is usually more costly and less effective than one based on a common platform. Effective testing methods using technology are usually unavailable or left unconsidered. In fact, second line of defense functions often rely heavily on inquiry-based methods such as surveying, which are proven ineffective at identifying the actual manifestations of risk in the organization.

If the business uses analytics software for investigations or monitoring transactions, in many cases it involves standard query tools or some form of generic business intelligence (BI) technology. Although good for providing summary level information or high-level trends, BI tools struggle to show the root cause of problems. And while they may have certain capabilities to prevent fraud and errors from occurring, or to flag exceptions, they are not sufficient to effectively trap the typical problem transactions that occur.

First line (management) use of risk & control technology

While in some cases, first line management have access to better technology for use on specific pain point areas (e.g., continuous transaction monitoring technology used within finance departments), there is a common tendency for management to rely far too much on core business systems for effective control.

While the large ERP and other system vendors seem to have extensive capabilities for preventing control deficiencies, the reality is that these are extremely extensive and complex systems and internal controls are usually the afterthought of those implementing them, not a core focus. For example, in many cases certain control settings are turned off to enable the ERP system to run more efficiently.

An integrated approach to managing risks and monitoring controls, and collaboration with the second and third lines of defense using a common, independent methodology and technology platform is the most effective way to address and mitigate risk.

[4] *PricewaterhouseCoopers, 2018, State of the Internal Audit Profession Study*
[5] *PricewaterhouseCoopers, 2018, State of the Internal Audit Profession Study*
[6] *Protiviti, 2018, Internal Audit Capabilities and Skills*

From current state ...

Considering the mix of technologies used and the generally disjointed way in which technology is applied across GRC-related processes, it is clear that a new approach integrating common methodologies and supporting toolsets is required.

Two significant categories of opportunity exist to supercharge risk and control processes with technology:

1. Aligning stakeholders across GRC functions on methodology and, in turn, technology platforms (i.e., horizontal maturity growth) to drive organizational collaboration and value.
2. Integrating technological capability across the entire tool stack for risk and control processes (i.e., vertical maturity growth) to drive organizational capability and value.

... To future state: Introducing data-driven GRC

The future state of maximized value and relevance within the strategic corporate agenda for risk and control-oriented functions will be achieved through a data-driven approach to risk and control related processes.

Data-driven GRC is a methodology for leveraging technological tools to evaluate and monitor strategic risk at an executive or board level, in real time, by analyzing transactional level business data.

Accomplishing this requires the ability to:

+ Reliably identify front line controls relevant to key strategic risks
+ Test controls using empirical evidence (i.e., data) within the organization (reducing or eliminating unsound validation mechanisms like inquiries, sampling, etc.)
+ Schedule and automate such tests to occur on an regular basis for ongoing evaluation of the related controls
+ Link real-time results of testing directly to corporate risks, driving real-time organizational risk assessment.

Data-driven methodology for GRC processes

The short route to building data-driven capabilities (as well as generally leveraging technology effectively) across GRC-related functional areas is to simplify and clarify the fundamental methodology, so that different functional and organizational stakeholders can work from a common place from a process perspective. Following a phased approach to building this methodology is the core driver of successful data-driven GRC.

Step 1: Design a simple, practical GRC methodology

Whether in audit, compliance, ERM, quality, security, or any other GRC function, a basic process for defining risks, controls, tests, and resulting issues needs to be put in place. It should be directly tied to the organization's corporate risk agenda, as seen at the executive management and board levels.

Begin by identifying corporate risks at a strategic level and assessing them on "potential impact" and "likelihood of occurrence." Based on this risk assessment, coordinated plans spanning various functional areas (audit, compliance, etc.) to achieve adequate risk mitigation should be developed. The plans should identify the projects and initiatives that will be undertaken to reduce residual risk to a comfortable level.

Once mitigation plans are developed, specific key objectives within each project should be defined, so tactical level risks that threaten the achievement of those objectives may be isolated. The controls that mitigate those tactical risks then need to be identified. Finally, tests of those controls must be designed and executed.

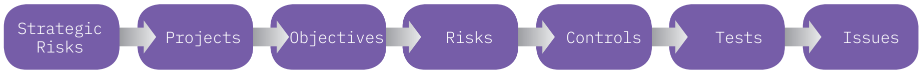

Figure 2: *The flow of fundamental GRC processes*

Step 2: Leverage data analysis in controls testing

Step 1 was about establishing a simple, consolidated process for assessing risks, defining controls, and executing tests: GRC 101.

Now that the basic process for assessment and mitigation of key risks has been defined, what typically becomes the organization's greatest weakness is the execution of truly effective tests to evaluate controls. Put simply, the challenge is that "you don't know what you don't know." In today's fast-moving world, it is far too easy to fail to spot the occurrence of a control deficiency or a previously unrecognized risk.

To gain more effective insight into the occurrence of control deficiencies and the existence of control gaps, next-generation testing methods need to be leveraged.

Next-generation testing methods are, fundamentally, the application of technological tools to controls testing. Automated testing is designed to eliminate traditional audit and evaluation methods such as inquiry, observation, sample-based inspection, and other manual methods that have proven to be statistical failures in generating reliable confidence intervals. Testing with technology also avoids time spent on investigating substantially non-value issues. Next-generation testing methods are predicated on analyzing systems and sources of actual data. Methods include transactional data analytics, complete population surveys, automated IT infrastructure and application assessment tools, statistical and trending data analytics, activity monitoring tools, and more.

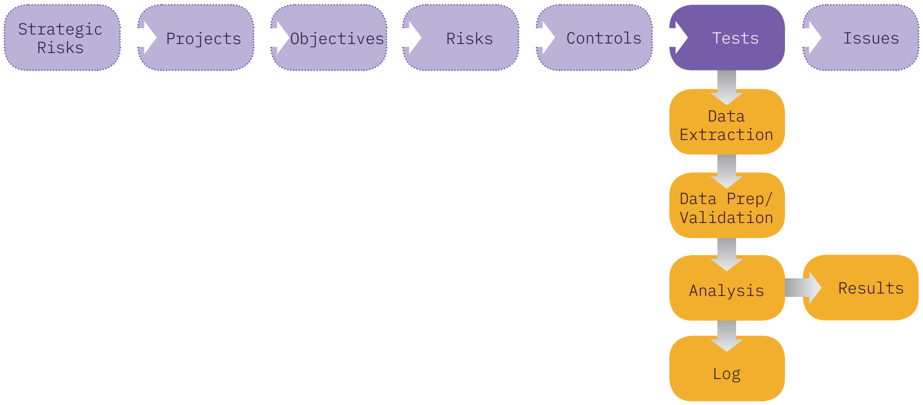

Figure 3: *Methodology for controls testing using data analysis*

Step 2 of data-driven GRC methodology focuses on conducting better tests on better "sources of truth" (i.e., better data). This is accomplished by leveraging technology to:

1. Extract relevant data
2. Validate completeness and prep for analysis
3. Analyze based on pre-designed business rules
4. Generate result sets that include potential exceptions (e.g., red flags indicating the occurrence of a control deficiency, or existence of a control gap).

In Step 2, analyses should be designed with the intent of attaining better coverage and improved confidence intervals when looking back on historical evidence.

Step 3: Integrate GRC & data analysis methodology

In the third step, an organization may begin the strategic integration of next-generation and analytical techniques with GRC processes. Ideally in this phase, the organization's risk and control-oriented functions will begin to standardize on required coverage models, such as leveraging next-generation testing in at least 50% of testing. They will also directly integrate the reporting from next-generation testing into the overall issue management process, providing executive dashboarding of the results and issues, and visual reporting at the level of the strategic risk agenda.

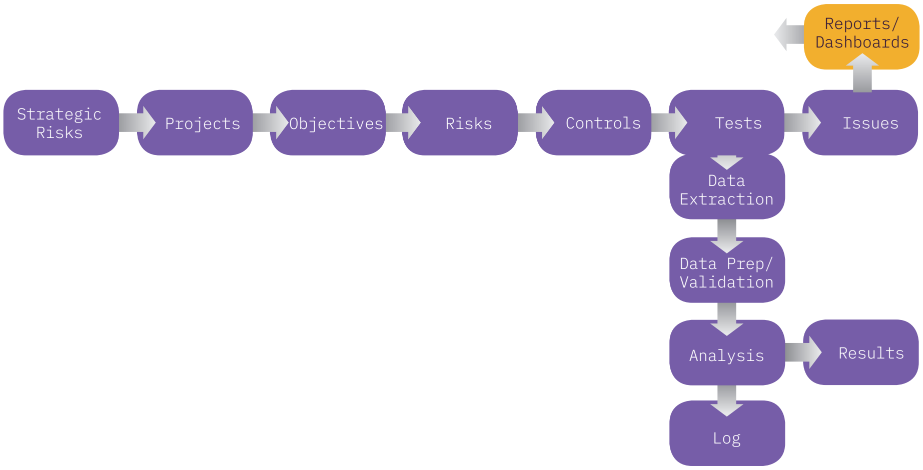

Figure 4: *Integrated GRC and data analysis methodology*

Step 4: Leverage continuous monitoring for real-time insight

Once an organization is leveraging next generation testing, and data analytics in particular, the next step in strengthening value delivery is to do so at the speed of today's economic realities. It is no longer adequate—at least from the perspective of an executive or board-level stakeholder—to only uncover and report on a specific risk or issue on an annual, or even quarterly basis. Tests need to be automated and running on an ongoing basis. With the technology that is now available, it is easy to take the successes developed in building integrated GRC and data analysis and automate it to continuously audit or monitor in near real-time going forward.

Where appropriate, responsibility for the maintenance of this level of monitoring may be passed from the second and third lines of defense forward to management. Even in this case, internal audit or other risk and control functions can review the results of the monitoring tests to gain the required assurance. By simply layering in automated scheduling, investigation of exceptions, and visualization of transactional results, the outcomes of monitoring become linked directly to the overall risk and control architecture. This enables an ongoing review process of how effectively the business is managing risks, driven by the evidence of data from actual activities. This in turn drives an appropriate response by all stakeholders; for example, performing additional audit procedures or implementing more effective control systems.

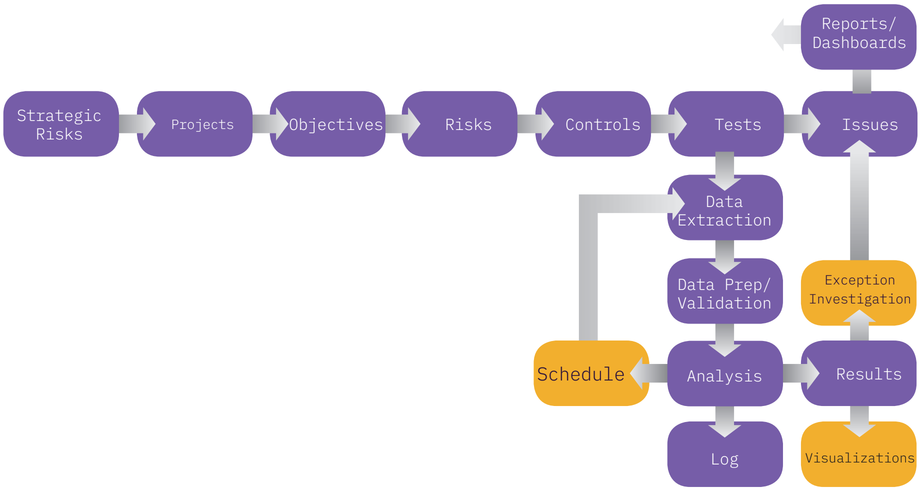

Figure 5: *Expanding data analysis to continuous monitoring (shown in green)*

Step 5: Integrate GRC & continuous monitoring methodologies for data-driven GRC

Finally, we come to the key step in achieving compliance with data-driven GRC methodology. In this fifth step, the organization links the outcomes being generated by continuous monitoring activities with the risk and control context within which they fit. The volume, value, and trending of identified issues are automatically fed back into each process or a technology-enabled rule set, which in turn guides the assessment of risks at the strategic risk level, to accurately reflect where data indicators of those risks sit in terms of potential impact severity and likelihood of occurrence. This is the key phase in the entire process enabling data-driven GRC, as it is where all of the work done can lead to meaningful, real-time decisions from executive management and the board that mitigates risk levels they were previously blind to, in turn optimizing the reliability of organizational performance.

The key enabler to fully integrating the data-driven program methodology is to develop a scorecard or rule set that objectively and quantifiably defines the threshold of unfavorable activity within the organization, which triggers a risk to be driven up the strategic agenda. The entire process is now fully illustrated below:

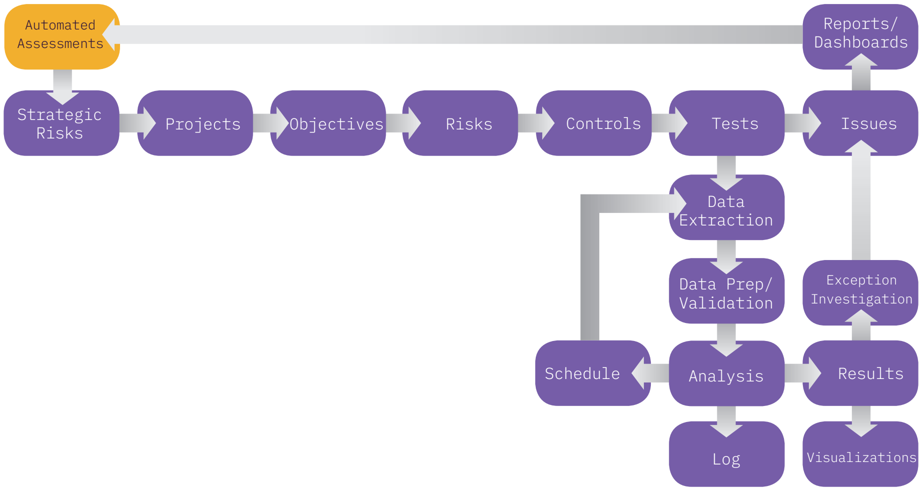

Figure 6: *End-to-end integrated data-driven GRC methodology*

Technology solutions

Data-driven GRC is not achievable without a technology platform that supports the steps illustrated above, and integrates directly with the organization's broader technology environment to acquire the data needed to objectively assess and drive GRC activities. From a technology perspective, there are four main components required to enable the major steps in data-driven GRC methodology:

1. Integrated risk assessment

Integrated risk assessment technology maintains the inventory of strategic risks and the assessment of how well they are managed. As the interface of the organization's most senior professionals into GRC processes, it must be a tool relevant to and usable by executive management. This technology sets the priorities for risk mitigation efforts, thereby driving the development of project plans crafted by each of the functions in the different lines of defense.

2. Project & controls management

A project and controls management system (often referred to more narrowly as audit management systems or eGRC systems) enables the establishment of project plans in each risk and control function that map against the risk mitigation efforts identified as required. Projects can then be broken down into actionable sets of tactical level risks, controls that mitigate those risks, and tests that assess those controls. This becomes the backbone of the organization's internal control environment and related documentation and evaluation, all setting context for what data is actually required to be tested or monitored in order to meet the organization's strategic objectives.

3. Risk & control analytics

If you think of Integrated Risk Assessment as the brain of the data-driven GRC program and the project and controls management component as the backbone, then risk and control analytics are the heart and lungs. An analytic toolset is critical to reaching out into the organizational environment and acquiring all of the inputs (data) that are required to be aggregated, filtered, and processed in order to route back to the brain for objective decision making. It's important that this toolset be specifically geared toward risk and control analytics so that the filtering and processing functionality is optimized for identifying anomalies representing individual occurrences of risk, while being able to cope with huge populations of data and illustrate trends over time.

4. Knowledge content

Supporting all of the technology components, knowledge content should be acquired in support of individual risk and control objectives and may include items such as:

- Risk and control templates for addressing specific business processes, problems, or high-level risk areas
- Integrated compliance frameworks that balance multiple compliance requirements into a single set of implemented and tested controls
- Data extractors that access specific key corporate systems and extract data sets required for evaluation (e.g., a SAP-supported organization may need an extractor that pulls a complete set of fixed asset data from their specific version of SAP that may be used to run all required tests of controls related to fixed assets)
- Data analysis rule sets (or analytic scripts) that take a specific data set and evaluate what transactions in the data set violate the rules, indicating control failures occurred.

Mapping these key technology pieces that make up an integrated risk and control technology platform against the completely integrated data-driven GRC methodology looks as follows:

When evaluating technology platforms, it is imperative that each piece of this puzzle directly integrates with the other; otherwise, manual aggregation of results will be required, which is not only laborious but also inconsistent, disorganized and (by definition) violates the data-driven GRC methodology.

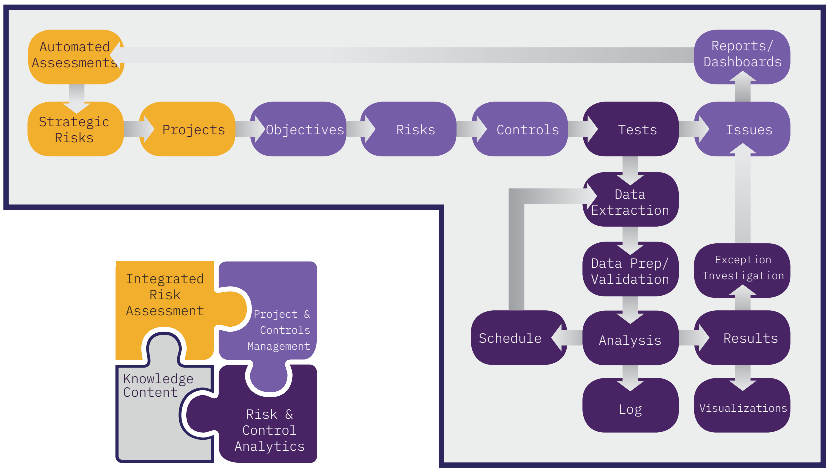

Figure 7: *Mapping of data-driven GRC methodology to an integrated GRC technology platform*

GRC technology checklist

- ❑ **Centralized project and controls documentation:**
Project and Controls Management systems are in place within the organization, documenting risks and controls and the techniques used to maintain and assess controls effectiveness.

- ❑ **Continuous risk monitoring:**
Risk and Control Analytics systems conducting Continuous Transaction Monitoring and Continuous Controls Monitoring activities are running in key business process areas, identifying exceptions and providing dashboards of risk indicators that are integrated into the Project and Controls Management Systems.

- ❑ **Integration with management activities:**
The Project and Controls Management systems connect directly into an Integrated Risk Assessment and Planning system, used by leadership to determine key areas to address in the organization's mitigation efforts across the lines of defense.

- ❑ **Risk control matrix and test plan:**
For each project undertaken to support mitigation efforts, a well thought-out risk control matrix identifies key tactical risks and mitigating controls. A test plan leveraging primarily next-generation testing techniques is also in place to provide assurance around controls effectiveness.

- ❑ **Automated control tests:**
Where appropriate, tests are linked to analytics maintained in a secure central repository. The analytics are run automatically on a repeated basis, and the results identified are automatically routed for review and resolution, and linked into the risk and control structure.

- ❑ **Analysis-driven remediation and risk assessment:**
Results identified through all testing techniques automatically drive remediation actions and assessments of the impact severity and likelihood of occurrence of strategic-level organizational risks.

- ❑ **Risk dashboard:**
The status of audit and compliance activities is monitored by audit, compliance, and senior management through dashboards that provide up-to-the-minute views of contextual risk exposure and issues under resolution.

A value delivered technology maturity model for leaders across all lines of defense

In the above sections we stepped through developing a program based on data-driven GRC methodology, as well as the technology that is required to support such an approach. The use of fully integrated technology should result in a dramatic improvement in the efficiency of the GRC processes themselves, as well as in the effectiveness of the risk management procedures and control systems that are established in the enterprise.

We identified that through the adoption of proper technology solutions, five levels of capability may be enabled:

1 Basic GRC processes

2 Risk and control data analysis

3 Integrated GRC + data analysis

4 Enterprise continuous monitoring

5 Data-driven GRC processes

The model below illustrates a grid where these advancing capabilities fit with respect to their functional application across the different lines of defense. When GRC is examined holistically in most organizations, basic GRC processes are typically in place in the third line of defense (internal audit) as well some second-line functions. There is also some data analysis being performed, but typically only in the third line, disconnected from or only manually integrated into the GRC processes. While these are important activities, this haphazard approach provides only somewhat narrow tactical value to the organization relative to what is possible with modern technology.

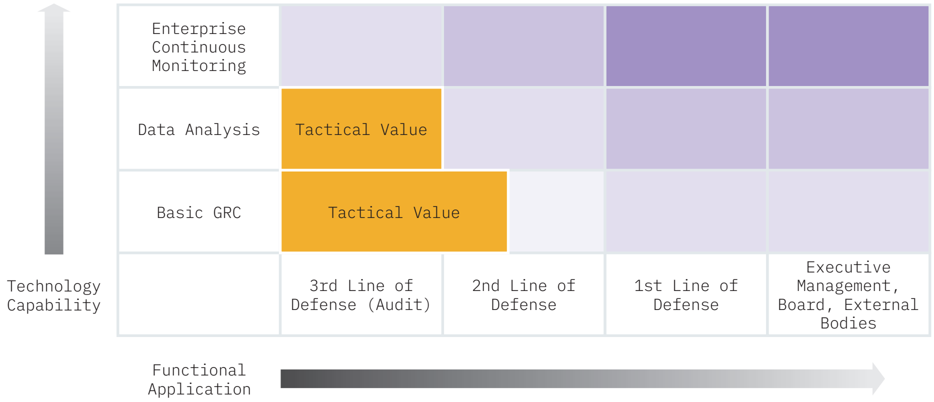

Figure 8: *Current state*

As dedicated GRC professionals actively improve an organization's GRC processes, and coordination begins to occur across the lines of defense, higher-value GRC programs evolve. As data analysis is integrated into GRC process testing to achieve integrated GRC and data analysis across risk and control-oriented functions, high-impact, high-value outcomes begin to emerge at a strategic level in the organization. The same can be said for strong enterprise continuous monitoring programs that automate control monitoring and remediation efforts across the lines of defense.

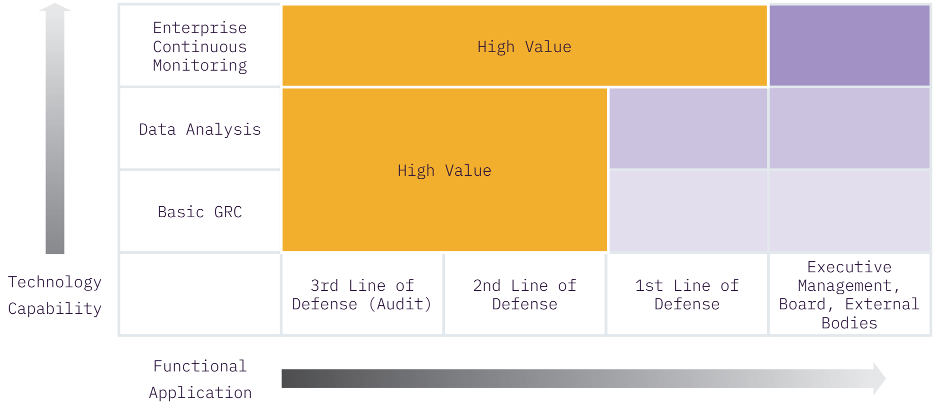

Figure 9: *Transformational GRC programs*

Final Thoughts

The connection between organizations with highly efficient and data-driven processes for assurance, risk management, and control, and those that perform better as businesses is clear. So, what can an audit or risk management leader do to help their organization move towards transformational value delivery through data-driven GRC?

There are a number of key issues to consider:

- Leaders responsible for risk and control-oriented functions (including audit, risk management, compliance, and others) can develop a coordinated strategy that recognizes the fundamental value of an integrated technology approach.
- The piecemeal use of disconnected and unintegrated technology in audit, risk management, and compliance activities are unlikely to deliver high-impact value or be cost-effective overall.
- Internal audit needs to remain independent; an integrated technology platform does not preclude this.
- Data-driven GRC methodology will, in-time, prove a necessity in managing organizational risk and become a cornerstone of enterprise performance management.
- Risk and control technology platform integration offers many benefits, but should not involve unnecessary complexity.

- Large and involved systems that require a massive amount of planning, configuration, and maintenance are also unlikely to be cost-effective overall.
- Methodology and technology can be simple with the right approach to implementing each.
- Technology should be considered a cornerstone of risk management and overall GRC strategy.
- To achieve truly data-driven GRC processes requires a significant shift in thinking and approach.
- Resource planning and budgets should take this sufficiently into account.

Galvanize has decades of experience working with thousands of customers worldwide and developing detailed materials and methodologies to support transformational governance, risk, and compliance management.

For a free assessment of how your organization can best integrate technology into your GRC processes, call 1-888-669-4225 or visit *wegalvanize.com***.**

Dan Zitting, CPA, CISA, GRCP, is chief customer experience officer at Galvanize and an advocate for the use of leading technologies—in particular cloud, mobile, data analysis, visualization, and social—in the transformation of the GRC-related professions and organizational performance management.

John Verver, CA, CISA, CMC, is advisor to Galvanize and a longtime proponent of the role of technology in audit, risk management, compliance and continuous monitoring.

About Galvanize

Galvanize builds award-winning, cloud-based security, risk management, compliance, and audit software to drive change in some of the world's largest organizations. We're on a mission to unite and strengthen individuals and entire organizations through the integrated HighBond software platform. With more than 7,000 customer organizations in 140 countries, Galvanize is connecting teams in 60% of the Fortune 1,000; 72% of the S&P 500; and hundreds of government organizations, banks, manufacturers, and healthcare organizations.

Whether these professionals are managing threats, assessing risk, measuring controls, monitoring compliance, or expanding assurance coverage, HighBond automates manual tasks, blends organization-wide data, and broadcasts it in easy-to-share dashboards and reports. But we don't just make technology—we provide tools that inspire individuals to achieve great things and do heroic work in the process.

Learn more about what you can accomplish with Galvanize
1.888.669.4225 | wegalvanize.com | info@wegalvanize.com