December 2020

Pathlock Business Controls Automation

Redefining Control Automation, Monitoring & Enforcement

SOLUTION***PERSPECTIVE***

Governance, Risk Management & Compliance Insight

Table of Contents

TALK TO US . . .

We look forward to hearing from you and learning what you think about GRC 20/20 research. GRC 20/20 is eager to answer inquiries from organizations looking to improve GRC related processes and utilize technology to drive GRC efficiency, effectiveness, and agility.

Pathlock Business Controls Automation

Redefining Control Automation, Monitoring & Enforcement

Monitor, Respond, and Automate Effectively

Dynamic & Distributed Business is Difficult to Control

Organizations fail to monitor and manage controls effectively in an environment that demands agility. Too often internal control management and enforcement is a periodic exercise only, reviewed and updated annually or quarterly at best. Outdated, manual controls result in inevitable failure of governance, risk management, and compliance (GRC) that provides case studies for future generations on how poor internal control management leads to costly, time consuming, and avoidable material weaknesses or significant deficiencies at many organizations. Improperly implemented controls can turn into a drop in market share or loss of consumer confidence, even for those with strong brands.

GRC is a "capability to reliably achieve objectives [GOVERNANCE], while addressing uncertainty [RISK MANAGEMENT], and act with integrity [COMPLIANCE]." Internal controls are a critical foundation to all three aspects of GRC and a key component to all three lines of a defense in depth strategy. Controls aid the organization in reliably achieving objectives, managing uncertainty by mitigating risk, and are a critical part of proving compliance obligations and enabling the organization to act with integrity. Good internal controls are the foundation upon which predicable business behavior, transactions, access, and processes rely.

Gone are the years of simplicity in business operations. Digital transformation is accelerating change in risks, regulations, globalization, employees, distributed operations, competitive velocity, technology, and business data - encumbering organizations of all sizes. Keeping this risk, complexity, and change under a reasonable level is a significant challenge for boards, executives, business owners, as well as GRC professionals throughout all levels of the organization. This challenge is even greater when internal control management is not a consistent, continuous, and monitored process in the organization - providing a real time view of these risks as they evolve and quantifying the financial impact when they materialize. Organizations need to understand how to design effective controls, implement them, and continuously review whether the risks they were designed to control are effectively mitigated.

Corporate governance and organizational culture have largely been based on trust vs. facts. In this context, the organization trusts their employees, contractors, and other third parties working on its behalf. It is understood that these individuals will read and remember policies and procedures, hold themselves accountable to them, and apply

those policies and procedures in their daily activities. The reality is that people are human, and when dealing with thousands of employees and millions of transactions, even the best organizations will be at risk when relying on trust alone. Employees make mistakes, they cut corners, and their own motives and goals may not align with the organizations. Properly executed controls are the only strategy which can make sure all employees follow the procedures that align to the good of the organization, while also empower the business with immediate, clear, and actionable information to course correct when necessary. Additionally, organizations will finally have real-time insight into what individuals are actually doing across the enterprise to mitigate user access and process risks.

Siloed Approaches Lead to Inevitability of Failure in Controls

Internal control management is often misunderstood, misapplied, and misinterpreted as a result of scattered and uncoordinated approaches that get in the way of sharing data. This is particularly true when internal control management is a set of manual processes scattered throughout documents, spreadsheets, and emails instead of a holistic single source of truth for monitoring controls. Internal controls are pervasive; there are a variety of departments that manage controls with varying approaches, models, needs, and views on what controls are and how they should be measured and managed. Enterprises often struggle to unify the department and process-level controls as they continue to develop broader GRC and enterprise/operational risk management strategies that span these departments.

The management of internal controls has become increasingly challenging as the organization has:

- *Multiple lines of businesses operating globally* across many jurisdictions and systems, requiring customized controls in each region or business.
- *Proliferation of business applications* with employees having access to dozens of systems and processes. Over time there are significant gaps and rights issues as the average user compiles access to systems and permissions they are no longer using.
- *Web of third-party relationships and transactions* with contractors, consultants, temporary workers, service providers, and outsourcers that have access to data, systems, and processes.
- *Mergers and acquisitions* that exponentially grow the systems, processes, and controls - with rationalization efforts often delayed until years down the road.
- *Isolated systems that monitor controls* from a single application perspective but fail to see the issues and rights across systems in a heterogenous environment.
- *Migration of applications to the Cloud* furthering the need for a complete strategy to manage internal and external threats.

- *Increase in transaction volume and velocity*, increasing the chances for risky or fraudulent transactions and pushing the limits of manual control strategies.

For some organizations, internal control management is only a point in time view of routine financial controls, resulting in nothing more than a cursory look into one or more siloed ERP systems, and does not provide an enterprise view of controls across roles, business systems, processes, and operations. While completing a control assessment process might tick the box for some basic compliance exercises, it has got in the way of true control implementation to protect organizations from a growing internal threat.

Internal control silos — where distributed systems and processes maintain their own controls, data, and analytics — pose a major challenge to achieving a complete control strategy. Documents, spreadsheets and data warehouses are not up to the task – they fail to understand the complex interrelationships that span systems, operations, transactions, lines of business, and processes. While many individual business applications focus on their specific controls, they ignore the aggregate picture. When an organization approaches internal controls in scattered silos without acknowledging control and process interrelationships across departments, they leave behind a critical opportunity to be intelligent about risk and control. This is due to the fact that processes intersect, compound, and interrelate to create a larger risk exposure than each silo is independently aware of. A siloed approach to internal controls fails to deliver insight and context, rendering the chance of making a connection between controls, risk management, objectives, and performance nearly impossible. Today it is critical that the control design, implementation, and monitoring program is centralized. This way, everyone is working off the same data and that control data is clean, reliable, and timely.

Making sense of internal control management and its varying factions across operational, financial, employee conduct, regulatory, security, and IT risks can be bewildering. An internal control management strategy that is siloed and myopic makes governance a challenge.

Providing 360° Contextual Awareness of Controls

Organizations need complete 360° situational awareness and visibility into internal controls across systems to stay compliant and protect the business. What complicates this is the exponential effect of risk and control on the organization. Business operates in a world of chaos. A small event cascades into a significant issue. Dissociated siloed approaches to internal controls that do not span data, systems, employee, third party access/roles, and processes can leave the organization with fragments of truth that fail to see the big picture of risk and controls across the enterprise, as well as how it supports their strategy and objectives. The organization has to have holistic visibility and 360° awareness into control and risk relationships across the enterprise. Complexity of business and intricacy, and interconnectedness of control data, requires that the organization implement an enterprise view of internal controls monitoring, automation, and enforcement.

Advances in technology for internal control management, automation, and continuous monitoring now enable organizations to achieve a real-time, integrated view of enterprise risks and controls across business systems, applications, processes and roles without

human intervention. This not only enables an enterprise perspective of GRC, but also allows the organization to increase efficiency, effectiveness, and agility in internal control management. These developments are enabled through a federated and connected view of internal controls that leverages artificial intelligence, machine learning, and integrated process automation to make the internal control management process more efficient, effective, and agile. This in turn enables organizations to spend more time focusing on the analysis and impact of risk in the context of the organization, its strategy, objectives, and the users conducting business and less on managing and implementing the basic controls needed to assess risk posture. Technology makes it easier to normalize, correlate, and share data, while still maintaining independence of thought and action across the organization.

The bottom line: Gone are the days where internal controls were focused on random sampling and manual testing with point-in-time snapshots that led to lengthy audit cycles and lack full awareness. Today's organization require full visibility into internal controls across systems, processes, transactions, and relationships. They need a unified internal control automation, monitoring, and remediation platform to deliver 360° contextual awareness of internal controls.

Pathlock Business Controls Automation

Redefining Control Automation, Monitoring & Enforcement

Pathlock Technologies provides an Enterprise Business Controls Automation platform, which is a solution that GRC 20/20 has researched and evaluated that can manage controls, monitor activity, quantify impact, and automatically remediate risks across a breadth of 140+ systems, dozens of processes, and billions of transactions. The Pathlock solution delivers an enterprise internal control management platform that can be used to manage, deliver, and report on the range of controls across the business in a contextual understanding of the risk posture of the organization.

GRC 20/20 finds that the Pathlock solution enables organizations to be efficient, effective, and agile in their internal control management strategy and processes. There is clear value to the solution, whether deployed for a single control area or ideally for a cross-application view of controls. Pathlock is suited for use across multiple industries, with the flexibility to provide controls related to a number of difference risk and compliance frameworks.

GRC 20/20's evaluation, research, and interactions with Pathlock clients have determined the following:

- **Before Pathlock.** Clients of Pathlock typically were using manual processes encumbered by documents, spreadsheets, data warehouses, and emails that only gave them a point in time visibility into internal controls and leveraged random sampling instead of full visibility into all transactions. Others were using siloed (e.g., ERP specific) internal control solutions that were expensive, difficult to maintain, and only provided a small glimpse into the risks present across the

enterprise. These outdated approaches fell short in providing the control and security needed for large enterprises to be successful.

- **Why Pathlock.** Organizations choose Pathlock as they are looking for a single integrated platform to standardize, automate, and manage internal control monitoring, management, risk remediation, and reporting processes across their entire enterprise landscape. Clients were looking for a single information architecture that can handle a unified approach to internal controls that can contextually understand the relationships and impacts of controls throughout the organization in a heterogeneous business application environment. Clients state they chose Pathlock as it had the greatest breadth of integrations to mission critical systems and the deepest functionality to not only assess risk posture but also prevent risky transactions.

- **How Pathlock is used.** Pathlock's flexible architecture allows the platform to work in a variety of internal control management environments, from a single internal control monitoring in a specific ERP environment, to a cross-system/process of integrated approaches, to internal controls. Given the flexibility and breadth of the platform, many of the customers surveyed were large enterprises and corporations with complex application landscapes.

- **Where Pathlock has excelled.** Organizations state that Pathlock has reduced costs, streamlined activities, and improved the quality of their internal control management, monitoring, and reporting processes. With increased visibility into control contexts across the systems and processes, Pathlock customers eliminate the overhead of managing manual internal control assessment processes previously managed in spreadsheets, documents, data warehouses, and emails. Clients find that the solution is flexible to adapt to their heterogeneous environments and provides the flexibility to grow and mature alongside their internal control program over time. Overall, users find the solution was particularly easy to configure, implement, and rollout in their organization.

What Pathlock Does

GRC 20/20 has evaluated the capabilities of the Pathlock platform and finds that it delivers an intuitive and robust internal control management solution to manage the range of controls across the variety of systems, processes, and transactions in even the most complex organizations. The solution allows organizations greater agility in managing and monitoring controls in the context of today's demanding requirements and dynamic environments. Pathlock automates what were once labor-intensive and error-prone tasks associated with managing and assessing internal controls. The functionality Pathlock provides is essential for organizations needing to eliminate a maze of manual processes, documents, spreadsheets, data warehouses, email, and narrow (e.g., ERP specific) point solutions.

The Pathlock solution provides an integrated and unified information and application platform that facilitates internal control management across a range of business applications and processes. The enterprise internal control management platform is built

to manage the breadth and depth of internal controls in one system, replacing disparate systems and manual processes. What is unique about Pathlock in the market is that it provides one single internal control management platform that allows for management of internal controls across:

- **Business systems.** Pathlock natively supports over a hundred business systems to monitor and enforce controls across ERP, cloud, legacy business, and enterprise systems with real-time connections. This integration allows for the ability to read-write data to these systems, monitor business activity within and across systems, and automatically remediate risks identified when policies and controls are breached.

- **Users.** Pathlock monitors the breadth of users, their actions, activities, and behavior across systems to govern and analyze access, manage privileged users, and conduct 'can do' analysis to take actions only on exceptions that poise the greatest risk to the organization. To date, millions of users and billions of transactions have been monitored and controlled through the Pathlock platform.

- **Activities and transactions.** Pathlock monitors the breadth of business transactions and can see and analyze behavior across systems/applications. This enables 360° monitoring of transactions, delivers segregation of duties and SOX compliance across systems and not just within a single system, achieves data security and privacy, and enforces business policies and user behavior. This is enhanced by 'did do' analysis to understand behavior and risk exposure from actual business activity, not just user privileges and permissions.

- **Risks, exposures and impacts.** Pathlock delivers a detailed understanding of risk and exposure to the business in context of internal control issues and failures. It measures bottom-line financial impact, allowing organizations to sort through the noise and address the largest risks in a timely manner.

Pathlock effectively and efficiently enables an organization's end-to-end internal control management strategy by providing a platform to manage the lifecycle and breadth of internal controls across the organization and its business systems, applications, processes, and transactions. Pathlock achieves this through a single integrated platform, that is flexible enough to work with virtually any business application or process.

Foundational Capabilities in Pathlock

The Pathlock solution can be implemented to address the complex requirements of an integrated internal control management program across business systems, or it can be implemented to address particular internal control needs within a specific business application or process. Many organizations may start with addressing a specific narrow internal control area but will often expand the Pathlock implementation quickly to address a complete range of internal control areas across multiple systems and processes.

Specific capabilities that Pathlock delivers that enable organizations in managing internal controls are:

- **Analytics and dashboards.** Pathlock delivers risk analytics that sort through the noise to highlight the most critical risks across business systems, access, and transactions. This allows for timely remediation of key issues to improve risk posture.

- **Alerts and notifications.** Pathlock provides notification through various channels, including email or integration to ITSM solutions (such as ServiceNow) and SIEM tools (such as Splunk).

- **Integrations.** Pathlock integrates directly to other key systems in the enterprise landscape to further existing technology investments. Common tools integrated to include SAP GRC, ServiceNow, Okta, SailPoint, Splunk, and more.

- **Workflow and task management.** Pathlock provides capabilities to manage workflow and tasks associated with control implementation and risk remediation. This includes alerts on pending tasks that are soon due and escalation of missed tasks.

- **Pre-built, customizable business controls.** Pathlock monitors a breadth of prebuilt business controls across finance, operations, technology, security, and regulatory requirements – all of which can be customized to an organization's specific needs. This allows for an accelerated time to value and reduced implementation risk.

- **Access governance.** Pathlock delivers the ability for full access governance across business systems to provide full visibility into segregation of duties, can do analysis, and management of privileged users. The platform provides insight into what users can do within and across business applications to uncover risks that span these systems and processes, allowing organizations to quickly take control and remediate key issues.

- **Activity monitoring.** Pathlock automates the full control and monitoring of internal controls and quantifies the financial impact of control issues surrounding transactions. Instead of random, manual sampling of a small subset of transactions, Pathlock delivers automated monitoring and enforcement of all transactions. This includes transactions in key business processes such as procure to pay, general accounting, order to cash, inventory management, human resources, time, and expense.

- **IT general controls monitoring.** Pathlock automates and monitors IT controls and configurations such as identity and access, logging and events, incident management, system configurations, and security and privacy controls.

- **Insider threat monitoring.** Pathlock enables organizations to focus on where their greatest threats reside – inside their organizations. With Pathlock,

organizations protect against insider threats from the inside out to ensure that risk of fraud, data leakage, and privacy is controlled both internally and externally.

Benefits Organizations Can Expect with Pathlock

Organizations are most likely to move to the Pathlock platform because they found that their manual document-centric approaches took too many resources to administer, only addressed specific areas of internal control, and allowed risks to slip through the cracks. Other organizations choose Pathlock because their existing internal control management solutions were only focused on specific business systems and did not give them visibility into controls across systems, processes, users, and transactions. Others found competing systems to be ineffective, complicated and costly in the complexity, and required too much work to implement the controls needed for their specific environment.

Specific benefits organizations can expect from implementing the Pathlock solution are:

- ***Significant efficiencies in time through automation*** of workflow and tasks, as well as reporting. Specifically, the time it takes to test controls and build reports from documents and spreadsheets now is just a matter of seconds. One organization reported they reduced control monitoring efforts by 90%.
- ***Reduction in errors*** by automating the validation of controls, thus removing common errors in manual processes and reconciliation that was incomplete or incorrectly entered.
- ***Decrease in false negatives*** as the solution can fully monitor all transactions and controls to avoid the oversight common with random sampling and manual processes.
- ***Data integrity***, with Pathlock being the system of record for all internal control management information, across all enterprise systems and processes.
- ***Collaboration and synergies*** by providing a single platform with a consistent interface to manage controls across business applications - instead of disparate applications using a broad array of technologies without integration or consolidated visibility.
- ***Consistency and accuracy of information*** as all internal controls conform to consistent processes, monitoring, and enforcement within a single solution with a uniformed and integrated control and monitoring process and information architecture.
- ***Accountability with full audit trails*** of who did what and when, to ensure no transactions are making it past the business controls implemented.

- *Efficiency in reporting* where reporting is real-time, integrated, and automated to provide visibility to point in time risks, as well as historical changes in risk posture.

- *Reduced audit fees* with Internal and External Audit teams being able to rely on findings and reporting produced by Pathlock.

Considerations in Context of Pathlock

Every solution has its strengths and weaknesses and may not be the ideal fit for all organizations in all situations. While GRC 20/20 has identified many positive attributes of Pathlock to enable organizations to deliver a consistent enterprise internal control management and monitoring platform — readers should not see this as a complete and unquestionable endorsement of Pathlock and its solution.

Pathlock provides a unified internal control management architecture. It manages the range of controls with an enterprise approach to control analytics, assessment, monitoring, and enforcement across business systems and processes. Overall, organizations should have a high degree of satisfaction with their use and implementation of Pathlock as their unified internal control management platform to manage the breadth of controls present in most enterprises. Client's particularly find value in Pathlocks ability to monitor and even prevent risky transactions before they become an issue or loss to the organization. Existing clients are eager to implement the updated user interface design that Pathlock is currently implementing to give the solution a more modern look and feel.

GRC 20/20 finds that Pathlock provides value in managing an enterprise internal control management program in a complex enterprise business environment. It enables and embeds internal control management across business applications, users, processes, transactions, departments, and functions. As many organizations respond to growing risk and regulatory exposure across their business application environment, they often require a solution like Pathlock to manage and automate this process.

About GRC 20/20 Research, LLC

GRC 20/20 Research, LLC (GRC 20/20) provides clarity of insight into governance, risk management, and compliance (GRC) solutions and strategies through objective market research, benchmarking, training, and analysis. We provide objective insight into GRC market dynamics; technology trends; competitive landscape; market sizing; expenditure priorities; and mergers and acquisitions. GRC 20/20 advises the entire ecosystem of GRC solution buyers, professional service firms, and solution providers. Our research clarity is delivered through analysts with real-world expertise, independence, creativity, and objectivity that understand GRC challenges and how to solve them practically and not just theoretically. Our clients include Fortune 1000 companies, major professional service firms, and the breadth of GRC solution providers.

Research Methodology

GRC 20/20 research reports are written by experienced analysts with experience selecting and implementing GRC solutions. GRC 20/20 evaluates all GRC solution providers using consistent and objective criteria, regardless of whether or not they are a GRC 20/20 client. The findings and analysis in GRC 20/20 research reports reflect analyst experience, opinions, research into market trends, participants, expenditure patterns, and best practices. Research facts and representations are verified with client references to validate accuracy. GRC solution providers are given the opportunity to correct factual errors, but cannot influence GRC 20/20 opinion.

GRC 20/20 Research, LLC
4948 Bayfield Drive
Waterford, WI 53185 USA
+1.888.365.4560
info@GRC2020.com
www.GRC2020.com