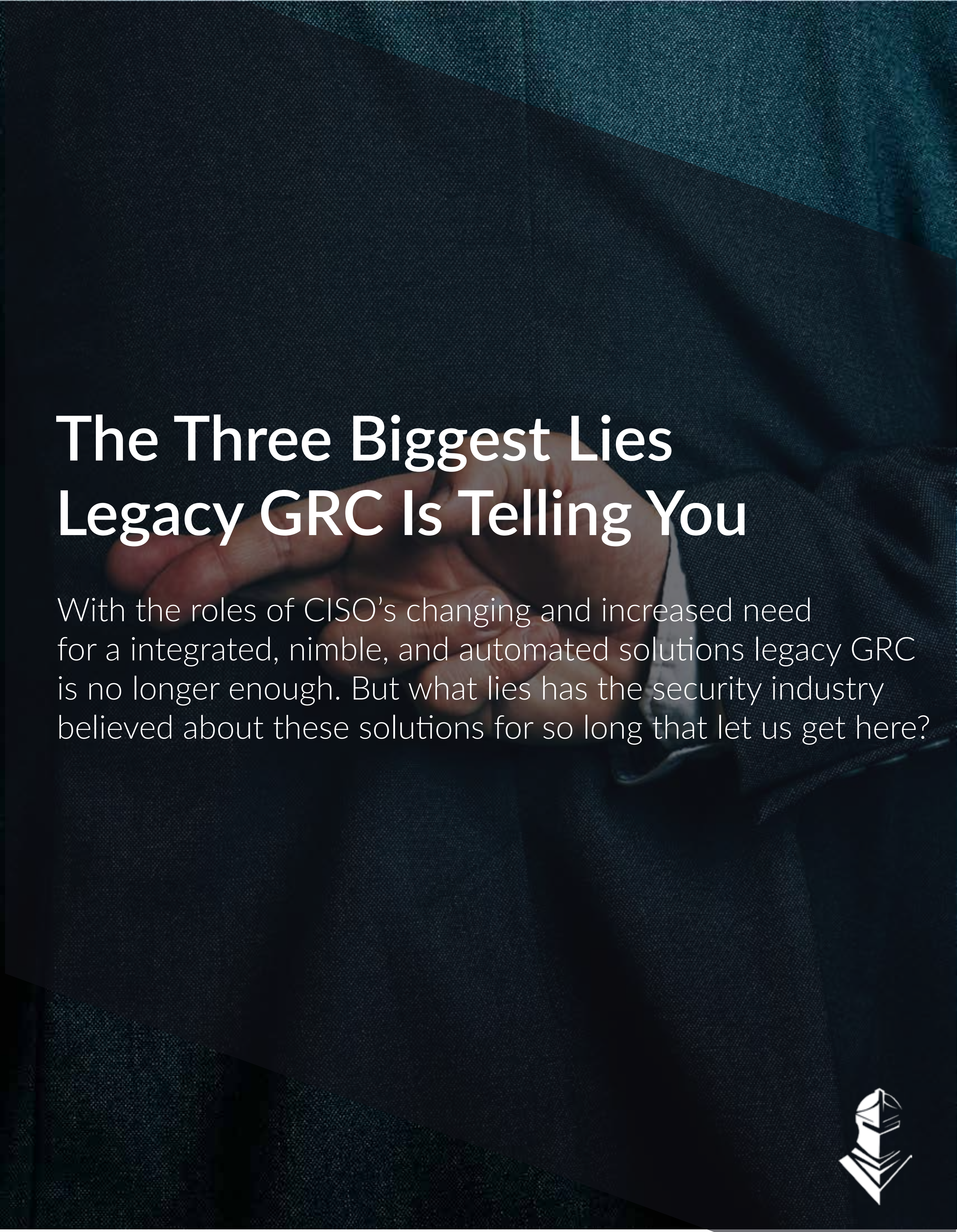

The Three Biggest Lies Legacy GRC Is Telling You

With the roles of CISO’s changing and increased need for a integrated, nimble, and automated solutions legacy GRC is no longer enough. But what lies has the security industry believed about these solutions for so long that let us get here?

Introduction

Today, every organization strives to optimize the speed with which they access information. Data is being stored, processed, transmitted and utilized in almost every day-to-day occurrence in both business and in life. The tech ecosystem has observed and taken part in deploying large amounts of capital used both in funding and purchasing cybersecurity and information security technologies- the goal being to help secure and manage all of this data. Both public and private organizations have heavily invested time and resources into implementing complex technologies and point solutions in order to reach security.

While doing so, organizations have run into a few major problems- the most pertinent ones stemming from implementing too much too fast, with no overarching framework to measure their best practices against. Either the small to medium business has implemented some best practices but hasn't used any framework to align with, or the enterprise has chosen one of not many more frameworks or standards to align with (often adding others due to compliance requirements). Both of these approaches were executed in a way that lacks measurement, visibility into their cybersecurity posture, and organization. Governance, Risk and Compliance (GRC) programs were born out of the early 2000s, when mandates such as the Sarbanes-Oxley Act (2002) were released. As the pace of regulatory change increased in parallel with the growing risk landscape, organizations began to struggle to manage a number of regulatory standards, standard frameworks, hybrid or custom frameworks, and vendor questionnaires- too many redundant compliance requirements across an increasing number of unique applications.

Thus, governance, risk, and compliance (GRC) technologies were developed to aid organizations of all sizes to keep up with the pace of regulatory change, organize risk and compliance data, and help Chief Information Security Officers and their teams make more informed and efficient decisions. Organizations were searching for ways to reduce the redundancy of compliance requirements centralize their programs, ideally on one single platform.

These developments were built on a solid vision, but were not executed in a way that could evolve and change with the modern day organization-- much less the regulatory change, cybersecurity program complexity, and needs of both security and business leadership. CISOs and security leaders need to easily communicate their posture to executive management, have a single source of truth to reference all of their program data, and show program success based on metrics that everyone can get behind. The operational teams within the cybersecurity program need to know where to remediate for the best return on investment (ROI), they need to manage compliance as a continuous, "always on" function and consistently be in sync on what the most effective plan of action is both now and in the future.

These objectives are difficult to achieve in a single product. Many of the first GRC technologies took to a bottom-up as opposed to a top-down approach to building their technologies, focus on on operational functionalities and features that would allow risk and compliance teams to get as granular as possible with relationships between assets and risks, departments, policies and procedures. This approach, however, led to complex solutions that serve their purpose and are excellent for many functions, but rarely help organizations achieve the vision of an agile, always-on, continuous and risk-aware information security program.

According to Gartner, 69 percent of organizations are not confident that their current GRC activities will be enough to meet their future needs.

In addition, enterprise organizations often take anywhere between 1,000 to more than 10,000 hours to complete a cybersecurity risk or compliance assessment. Gartner coined the term "Integrated risk management (IRM)" to speak to the future needs of information security organizations-- in the context of what everyone only knew as GRC at the time. We see legacy GRC players shifting over to IRM in terms of messaging, but in the current state, the technology of these players remains fundamentally the same. After combing through hundreds of reviews of leading GRC products, speaking directly with hundreds more legacy GRC users who came to CyberSaint seeking a true IRM solution, here are some lessons learned and how to see past the marketing that GRC platforms are doing to convince customers like you that they're still worth investing in.

Lie #1: Good things come to those who wait... there's a direct correlation between time to implement and amount of value

Every technology company has had to debate between developing high-value configuration, or allowing for heavy customer-facing customization when building a product. Many in the GRC space opted to have users customize whatever they want with intricate linkages between assets, controls, risks, scoring mechanisms, and business processes. More customization options were added over the years, so much so that even those who bought described implementation as something that you must "know what you're getting into".

We've read through every Gartner and Forrester report, every review from those using legacy GRC, and spoke to our partner, Gartner, and other analyst firms about the subject. The consensus is that it takes at least 3 months, if not more, to simply implement the technology after buying it. Most of the time, these jobs are completed by a third party instead of the organization itself or the vendor. The more popular industry leaders average a 6-12 month, and some even 12+ months, implementation time in order to be used by the customer.

When GRC buyers choose a product that is supposed to make their program more efficient and effective, they shouldn't have to wait months to use it. As mentioned before, legacy GRC serves a purpose, but getting immediate time-to-value is not a common thread among these players. In the era of emerging integrated risk management, information security organizations should be able to access and utilize intricate linkages between assets, controls, risks, scoring mechanisms, and business processes without heavy customization-- instead, making as many of these functionalities out-of-the-box as possible, with agile customer-facing configuration, is the means to the fastest time-to-value in the future state of integrated risk management. A longer implementation time does not equate to more value, as the future of GRC (IRM) is leaning towards more rapidly deployed capabilities that bring just as much, if not more, value to users.

Lie #2: Your cyber program is complex, therefore you must need a complex solution

According to a recent survey of more than 800 audit committee and board members conducted by KPMG, the top challenge the company faces is the effectiveness of the risk management program. Yet, 42% of survey respondents report that their risk management program and processes still require "substantial work."

As CISOs and information security teams know and have experienced, cybersecurity risk management and compliance gets quite complex. Unfortunately, what many organizations opt for is a complex tool that ends up costing them much more in the areas of time and effort that expected, just to become usable-- and also average in the hundreds of thousands in dollars to license, not including implementation costs. Even then, the risk management technology architecture itself cannot meet the needs of the senior management, or the BoD. The organization of data in these platforms becomes so complex over time that the solution itself tends to be heavily fragmented and most organizations out of the hundreds we've spoken to who use them end up using spreadsheets, slide decks, and word documents in addition to (or sometimes instead of) those solutions for risk and compliance assessments, risk and compliance management and reporting.

The pace of regulatory change is putting pressure on organizations to respond quickly to new requirements, but these systems have not been able to take a complex program, or a complex problem, and make it simpler. Especially for larger institutions, the combination of responding to the complex regulatory landscape, managing a myriad of regulatory requirements, control sets, reporting mandates, is a necessary function.

40% of large institutions said they were extremely or very concerned about the ability of their risk technology to respond to new regulatory requirements, as did 44% of mid-size institutions and only 12% of small institutions (Deloitte).

We appreciate these legacy GRC solutions because they certainly serve their purpose, and have pioneered governance, risk and compliance for some time, but instead of pushing simplicity and ease of use, they add a volume of customization such that the end result is even today, in many cases, far too complex to be effective. The visualization, communication, and reporting aspects of GRC, now IRM, are among the most pressing in today's business landscape, yet the data within legacy systems proves too fragmented to achieve these objectives.

In our eyes at CyberSaint, IRM platforms should be able to fulfill the most fundamental GRC functions it needs to without adding to a CISO's program complexity. IRM platforms should be built on metrics, should automate executive, Board-level, and auditor reporting, and should automate risk mitigation action planning so that everyone buys into the best path forward, and visualizes the data within risk and compliance programs so that infosec management can make more informed decisions, faster, and with more conviction from business peers.

Lie #3: GRC and IRM are the same... that's why legacy GRCs are marketing themselves as IRM in recent years

According to Gartner, "Integrated risk management (IRM) enables simplification, automation, and integration of strategic, operational and IT risk management processes and data."

Legacy GRC systems have begun to coin themselves as IRM platforms in order to attach themselves to this shift in market need. They promise more efficient decision making through enhanced communication and more, but ultimately the pure simplicity and metrics-driven approach in communicating program activity is what allows CISOs, CIOs, CEOs, and Board members to speak the same language. Even with the intricacies and granular functionality of legacy systems, most are built on qualitative, not quantitative data, making it difficult to communication governance, risk and compliance activities to non-security stakeholders, and causing decision making processes to be less data driven than they could be. Deloitte reports that some of the top priorities for investment from the BoD and executive management include risk analytics and risk reporting: risk analytics (53%), real-time risk monitoring (51%) and risk dashboards (44%)-- all functions that require a platform built on metrics to effectively achieve. In order to make many legacy players truly integrated, they would have to deconstruct their entire product and build on an entirely new architecture.

With an increased reliance on security teams as a business function, these silos that GRC platforms create are not proving to provide the value they once did for the new needs of GRC programs-- the integrated risk management needs. While Gartner coined the term "integrated risk management" as the future of GRC, the firm did what leading advisory firms do - examined the market needs and the responses of their clients cross-referenced with the current state and potential for the market to actually shift.

The market is evolving and legacy players aren't just going to become full-blown IRM immediately-- they have to work towards the vision. IRM is a recognition that the needs of an information security organization, especially executive management and non-security leadership, have changed in terms of how information security is positioned. As a result, the requirements for a high-value solution have also changed.

The change takes time. You may be asking why would a firm like Gartner start producing a Magic Quadrant for IRM rather than GRC if none of the leading GRC platforms are truly IRM solutions - Gartner's Magic Quadrant is periodic, not gradual like the shifting of the market, and Gartner needed to pick a time to benchmark the industry and recognize that the need for an IRM solution outweigh the need for a GRC.

The definition of IRM from Gartner is looking to the future, and it certainly seems like legacy GRCs are labeling themselves as IRM to stay relevant, it's far easier to alter the copy on a website than completely rethink the approach to a flagship product. The purpose of IRM, though, is to "enable simplification, automation, and integration..." and under that definition there is quite a lot of work to be done for traditional GRC offerings.

IRM requires a new breed of risk and compliance technologies that augment, simplify, and enhance the already complex and fragmented operational programs and technologies within the information security organization. These technologies are the catalysts for eliminated manual effort at the assessment and remediation level, rapid and informed decision making from CISOs and information security leaders, fluid communication between CISOs, CIOs, and the Board of Directors, measurement, visibility, and simplicity that allows key stakeholders from all business units to **see all, know all, and do all** that they can to keep their organizations secure.

As we've said, the change will not happen overnight. These intricate solutions have deep rooted systems that would shock an information security organization if ripped out, there is little chance the organization would be able to get away without significant cultural and process changes that would take time and resources to recover and restructure.

That's why, as an IRM solution built from the ground up to support the simplification automation and integration of an organization, we integrate with existing GRC solutions (see pricing page for more information) to allow organizations to adopt IRM capabilities without the need to re-imagine their organization from the outset. We all can, and should, lean into the integrated risk management vision.