Gartner Research

Debunking 5 Common GRC Software Myths

Gartner

Gartner

Debunking 5 Common GRC Software Myths

> Myths about the ROI of implementing GRC technologies prevent compliance teams from efficiently managing their organization's risks. Compliance leaders need guidance on how to debunk these myths to build consensus on making strategic technology investments.

Chief compliance officers must efficiently work with cross-functional teams to operationalize controls and build continuous risk management processes that enable organizations to ensure risk management objectives are met. To keep pace with that change and maximize efficiency to drive better risk outcomes, many compliance teams are using governance, risk and compliance (GRC) technology tools. According to the 2022 Gartner Budget and Efficiency for Compliance Survey, 49% of compliance leaders plan to increase spend on compliance technology — with 30% of leaders reporting an increase in spend of over 10% in the coming year.

By efficiently leveraging GRC technology tools, compliance teams can:

- *Implement compliance risk frameworks and controls, including policies the organization is required to comply with.*
- *Assess the most significant risks facing the organization.*
- *Optimize risk mitigation efficiency by automating high-frequency, low-value tasks.*

Despite the benefits these tools provide, the GRC market is overwhelming to navigate, which can leave compliance leaders uncertain as to whether they're achieving the right ROI, which in turn makes them reluctant to invest. To help compliance leaders navigate this change and achieve more positive risk outcomes with GRC tools, this research debunks five common myths that present barriers to investing in technology.

Myth 1: The technology I buy will provide a framework for my risk management methodology.

Truth: Compliance leaders often underestimate the importance of documenting their risk management methodology and fully understanding all stakeholder use cases before looking for a vendor.

Recommendation: Buyers should work with stakeholders to document their existing risk management methodology and processes to select the vendor that best aligns with the overall risk management strategy.

Organizations that don't clearly understand the end goal of how GRC technology will support their risk management methodologies and processes run into challenges during implementation and driving user adoption. GRC implementations fail when teams do not spend adequate time mapping compliance risk management processes to strategic business outcomes. Generally, GRC tools are known for flexibility in their data taxonomy and workflows to support different methodologies. This flexibility allows users to customize the tool based on their organization's risk management needs. Before selecting a vendor, stakeholders should have a common understanding of the methodology and processes that can be operationalized with technology.

An additional challenge includes approaching technology projects with a need to fulfill one specific requirement (i.e., risk scoring or control consolidation) without considering other stakeholders' requirements in the broader enterprise risk management ecosystem. This can lead to scope creep and drive higher implementation effort and costs than previously estimated.

Mapping the organization's risk management process goals is time-consuming. However, it gives purchasing teams leeway to determine the best solution fit for broader program objectives. Compliance teams should keep in mind that broader use cases require more flexibility on end-user requirements. Making these compromises provides a single source of truth for risk data and could yield the benefit of achieving aligned assurance. This effort can lead to better adoption, satisfaction and change management across all assurance leaders for the new tool.

Myth 2: I should be able to find a single technology solution to meet all my compliance risk management objectives.

Truth: Despite product positioning, no one GRC solution can both fully satisfy and be effective for all compliance risk management objectives.

Recommendation: Buyers should be open to evaluating point solutions to integrate with core GRC capabilities to ensure effective product execution.

GRC core capabilities support enterprise risk management processes. However, software vendors often position their products to effectively cover many use cases, including those specific to compliance functions. This range of support can help vendors capture a larger portion of market share by selling to multiple personas. A vendor's positioning on a use case does not necessarily equate to the product's ability to execute on the buyer's current pain point. Thus, buyers need to invest time analyzing the relative strengths and shortcomings of tools aligned to their functional requirements to avoid a mismatch with the product's technical capabilities.

Compliance users require discrete product capabilities that deviate from core GRC capability related to risk frameworks and control management. These capabilities can include whistleblower hotline, conflict of interest (COI) disclosures and privacy management (data subject access requests). But not all vendors can offer the depth of capability required for success. Compliance buyers should consider software in the broader risk management software ecosystem to meet these needs.

An example of how this could be applied in the GRC space relates to capabilities within the third-party risk management (TPRM). There are GRC tools that can help manage due diligence and onboarding that integrate with data feeds to support ongoing vendor monitoring. Users need to evaluate both the core GRC tool and the integrations to ensure it can meet program requirements. Compliance teams should pilot the GRC or a GRC-adjacent tool to pressure test their use cases before committing to buy.

Myth 3: My budget is too small to purchase GRC technology.

Truth: The benefits of GRC do not depend on an "all or nothing" investment approach.

Recommendation: Compliance leaders can begin their digital transformation journey by leveraging other teams' technology tools and vendor relationships to gain benefits from core GRC capabilities.

Because most teams believe they must purchase the entire suite of software to solve all their use cases, they avoid making purchasing decisions. Understanding all requirements helps prioritize use cases. In circumstances in which compliance leaders are primarily working to minimize inefficiency in their risk assessment and mitigation process, teams can take a small step to improve their efficiency by adding licenses or modules to existing technology within their organization. Some trade-offs on functionality or user preference may be necessary, but adapting key use cases in existing technology can quickly provide efficiency gains while broader scoping of requirements is investigated.

Another option is to work with existing vendors to determine if they have GRC modules that can be added to existing contracts. This approach harmonizes data repositories and ensures compatibility with existing enterprise architecture.

Example Use Cases of Leveraging GRC Tech From Existing Applications

Department	Add License or Module	Example Use Case
Human Resources and ERP systems	Modules	GRC add-on can help manage COI disclosure workflow
IT Security — GRC	Licenses	Existing GRC technology can be used to support risk identification, assessment and mitigation
IT Service Management (ITSM) — Workflow	Modules	ITSM providers offer GRC modules that can be added. Additionally, the workflow could be configured to support key risk management process activities (e.g., collecting evidence for controls and approval workflows).
Procurement — P2P System	Licenses and Modules	P2P technology may have vendor onboarding and due diligence capability.
Sales/Marketing — CRM	Modules	GRC modules can sit on top of CRM tools to support key risk management process activities (e.g., collecting evidence for controls and approval workflows).

Source: Gartner

Myth 4: We need an enterprise data strategy before selecting software.

Truth: Compliance leaders can gain workflow efficiency in the risk management process without waiting on an enterprise data model.

Recommendation: Partner with enterprise architecture (EA) teams to ensure their GRC tools are compatible with the organization's existing technology environments.

To effectively prevent and detect risk, compliance leaders need data that is accessible and reliable. A lack of a cohesive enterprise data strategy is often a barrier to data quality. Standard taxonomies across applications in structured data is important for analytics that predict behavior. But the truth is most organizations don't need to start with predictive analysis to improve how they conduct ongoing monitoring of compliance controls. GRC software provides a single source of truth for risk monitoring that enables compliance leaders to demonstrate they are monitoring and mitigating risk.

To achieve desired risk outcomes, compliance leaders should work with their EA teams early to understand how a new risk technology tool will interact with the organization's enterprise data infrastructure. This insight will improve communications efficiency and help select a vendor that is compatible with the organization in its current state.

Myth 5: We do not have the skills or resources required to effectively implement the technology.

Truth: Many vendors offer post implementation support to upskill existing compliance team members for an additional cost.

Recommendation: Ask the vendor about the level of post implementation support available to help support the technology.

Compliance leaders are often concerned about the special skills required for risk technology. The truth is that advances in technology have improved product configurability for end users who are not technology experts. Vendors increasingly build solutions that are called "no-code" platforms. These tools generally have a drag-and-drop, graphic configuration that makes it easier for a compliance team to serve as a system administrator. Vendors offer support with training as part of the implementation package. Other vendor services include system administration certifications, peer user exchanges, and coaching by the account manager or managed services packages. Therefore, it's possible for existing team members to take on some of the system management obligations.

Notably, some platforms are more complex and require specialized skill sets. To bridge this skill gap, teams can partner with existing IT team members to leverage technical skills regardless of the vendor selected. Some vendors offer managed service hours bundles to support system updates and one-time projects at additional cost.

Vendor-managed services can add cost to the life of the technology, but it could also bridge the gap until the business case is made to add specialist skills to the compliance team.

Conclusion

Navigating technology purchasing decisions in the GRC space can be complex. Compliance leaders can scale technology as programs grow and change — and they don't need to look for a perfect solution to achieve an ROI.

Evidence

Corporate Compliance and Ethics and Privacy Budget and Efficiency Survey.
Benchmarking Survey, Refresh, Biennial, Legal and Compliance Leaders

Actionable, objective insight

Position your function for success. Explore these additional complimentary resources and tools:

Webinar

Join a Virtual Event

Hear the latest insights from Gartner experts at an upcoming or recorded event.

Watch Now

eBook

Future of Compliance 2030

Explore 10 key program shifts to stay ahead and out of trouble.

Download Now

Guide

Strategic Planning for Your Function

Turn your strategy into action with these tools and templates.

Download Now

How We Help

Gartner for Legal, Risk & Compliance Leaders

Discover how we can help you tackle your mission-critical priorities.

Learn More

Already a client?
Get access to even more resources in your client portal. Log In

Connect With Us

Get actionable, objective insight to deliver on your mission-critical priorities. Our expert guidance and tools enable faster, smarter decisions and stronger performance. Contact us to become a client:

U.S.: 855 811 7593

International: +44 (0) 3330 607 044

Become a Client

Learn more about Gartner for Legal, Risk & Compliance
gartner.com/en/legal-compliance/products/gartner-for-compliance

Stay connected to the latest insights

Attend a Gartner conference
View Conference

Gartner®