SAPinsider

BENCHMARK REPORT

Governance, Risk, and Compliance

State of the Market 2022

Craig Powers

May 2022

REPORT SPONSORS

pathlock VERTEX

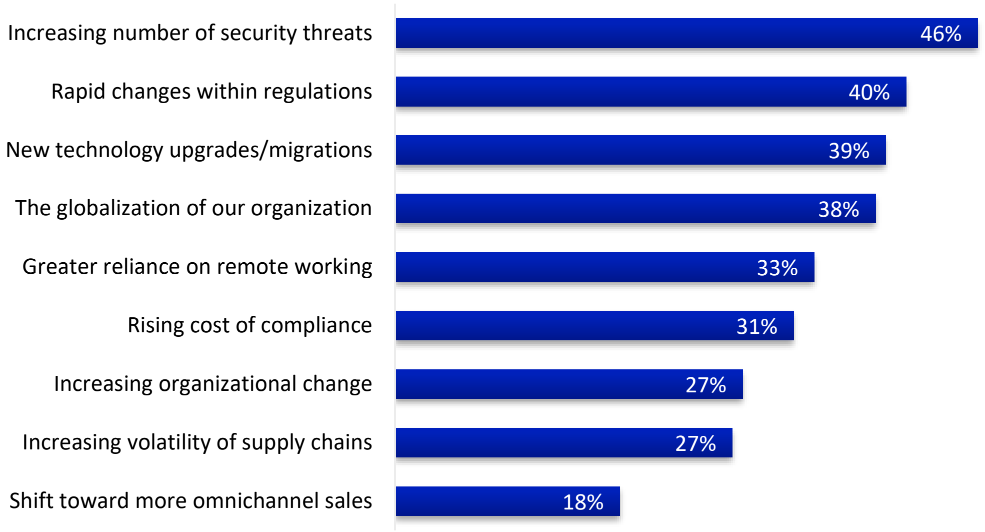
TABLE OF CONTENTS

Executive Summary

Governance, Risk, and Compliance (GRC) teams are facing an increasing set of challenges, including changing regulations, evolving business models, and rising security threats. The latter has increased in importance for GRC teams, where companies are capitalizing on their inherent expertise in dealing with risk and applying that to potential security threats.

To assess where companies are in their GRC journeys, SAPinsider surveyed 124 members of our community in March through May of 2022. Our data reveals increasing security threats and attacks as the most common driver for GRC strategy among respondents' organizations. That is a shift from last year, when new technology upgrades and migrations were the top driver (**Figure 1**).

Figure 1: Drivers of GRC Strategy



Source: SAPinsider, May 2022

Security as a key driver is reflected in the top requirements, areas of investment, and skillsets on which GRC teams are focused in 2022. Security monitoring and threat detection was the top requirement, rated as "very important" by 432% of respondents—an uptick from 30% in 2021.

Cybersecurity is the top area identified for significant GRC-related investment, listed by 61% of respondents. It was also the top last year, when 52% of respondents indicated cybersecurity as a top area of investment. Cybersecurity skills have also moved to the most-often listed skillset priority for GRC teams—indicated by 49% of respondents vs. 36% in 2021.

While security has become a top focus for GRC teams, there are still a myriad of other responsibilities on their plates. Much like last year, rapid regulatory changes, new technology upgrades and migration, and globalization are bringing new areas of risk. With so much on their plate, are companies looking to invest more in GRC?

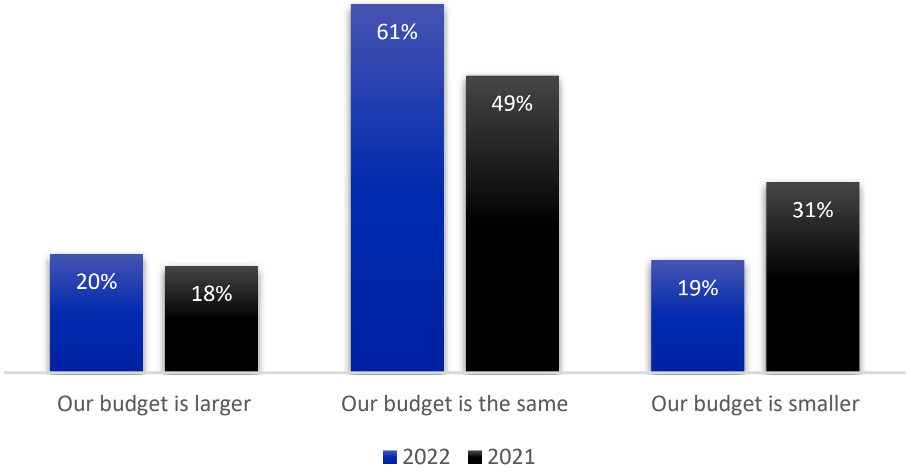
INSIDER PERSPECTIVE

"For each department, there's a very high probability having issues related to GRC. We have specific GRC SMEs embedded in my security department. When I have challenges with. compliance, risk, and ethics issues, we speak to the SMEs for that."

~ Michael Agbamuche,
Asset Security Advisor
Oil and Gas Company

Much like in 2021, GRC budgets are remaining stagnant at most respondents' organizations. However, there are far fewer organizations shrinking their GRC budgets in 2022 (**See Figure 2**). This finding aligns with our broader research around CIO Priorities in 2022, which shows that investment in technology and processes is bouncing back.

Figure 2: GRC Budgets Year-Over-Year



Source: SAPinsider, May 2022

INSIDER PERSPECTIVE

"We are super busy with reduced teams and workers. To help with this, we have automated distribution of compliance tests to owners and reviewers. We also have additional continuous monitoring and continuous auditing efforts that go on outside the process that are partially or fully automated depending on the control, which helps reduce risks."

~ Sr. Global IT Auditor
Furniture Company

While budgets are largely stagnant, GRC teams are also staying the same size at 68% of respondents' organizations. This aligns with last year, and it seems in 2022 that GRC professionals are once again being stretched—making increased efficiency from processes and technology more important.

These GRC experts are faced with a heightened focus on security risks, but that doesn't mean the requirements around more traditional areas of GRC are lessening. In fact, it's easy to see vectors of risk outside of security are also growing. Regulatory changes put pressure on compliance and audit teams, as do new business models that bring new standards to follow. User access is becoming more complicated as companies adopt new technologies, and with rising cloud technology adoption, there are more systems that require integration.

How are the most successful GRC teams meeting these growing requirements without adding staff? Looking at those respondents that are most satisfied with their GRC processes overall, the leading organizations are taking more action around centralization, automation, and integration.

This year's survey revealed several other trends regarding respondents' HR technology plans:

- 52% of respondents are using SAP S/4HANA, while 40% are using SAP ECC. Other top applications relevant to GRC include SAP Ariba (36%), SAP Concur (35%), and Salesforce (33%).
- CIOs (36%) most commonly drive agenda, strategy, and investment around GRC. CFOs (30%), Chief Accounting Officers (26%), and Chief Compliance Officers (24%) are the next most

common. Respondents frequently chose more than one option, so many companies have executives sharing GRC responsibility.

- Top regulations that respondents' organizations are focused on in 2022 include GDPR (38%), E-commerce sales tax/VAT (37%), international accounting standards/IFRS (36%), new revenue recognition standards (35%), International tax/tariffs (31%), and Sarbanes Oxley (SOX) (30%).

- When asked how many applications integrated with SAP that are or should be included in their compliance scope, 32% of respondents indicated 6-10 applications while another 30% have 11-20 applications tied to compliance.

Required Actions

Based on our research, organizations should make the following plans around their GRC strategies:

- **Define GRC's role in cybersecurity.** GRC and cybersecurity are crossing over at some organizations, and vendors are combining the two under one umbrella. What role can GRC skillsets play in cybersecurity at your organization? It could be about risk analysis, access control or identity management. With stretched GRC professionals, it's important to figure out what resources can be dedicated to cybersecurity.

- **Prioritize your risks.** With expanding responsibilities for GRC, there are more areas of risk to cover. Which risks pose the biggest threat to the business? It's important to prioritize those risks from last acceptable to most acceptable. This can help optimally allocate stagnant GRC budgets and staffs.

- **Take stock of your applications that touch GRC.** It's likely your organization has many applications that need GRC attention. Nearly two-thirds of SAPinsiders have more than five applications to consider for GRC. As a step towards centralization and integration, compile a list of those applications to develop more transparency, set priorities based on business factors and keep them updated along with business collaboration.

- **Align with business users to ensure process compliance.** Ultimately, it is the business users that determine compliance through their actions. Keep them in the GRC loop with changing regulations and company standards. If they are doing the right thing, that's less work for the audit staff.

Chapter One: GRC State of the Market Overview

GRC staff are not always connected. Often, they are spread in different areas of a business. Still, they collectively face a growing set of challenges. With budgets and teams largely staying the same year-over-year, GRC staff must evolve to protect organizations from risk. Next, we'll look at the key drivers and subsequent actions common among GRC teams in 2022.

Best Practices Model – DART

SAPinsider grounds all its research insights in our proprietary DART model. This research model provides practical insights that connect business **D**rivers and **A**ctions to supporting **R**equirements and **T**echnologies. Drivers represent internal and external pressures that shape organizational direction. Organizations take Actions to address those Drivers. They need certain people, processes, and capabilities as Requirements for those strategies to succeed. Finally, they need enabling Technologies to fulfill their Requirements.

In this report, the top drivers for GRC initiatives are the increasing number of security threats and attacks requiring more monitoring and detection, rapid changes within compliance and data privacy regulations are adding to GRC staff workload, new technology upgrades/migrations such as the move to SAP S/4HANA and the cloud, and the globalization of organization and business opening up new compliance and audit requirements. To satisfy these drivers, respondents are taking action on improving the level of GRC automation to streamline processes, centralizing and automating controls monitoring and management capabilities, providing strategic and centralized visibility into potential risks and fraud, bridging on-premise and cloud-bases security and access management processes, and streamlining user provisioning and access management.

To support their GRC strategies, there are several requirements that our survey respondents indicated they needed, including security monitoring and threat detection, agility to respond to changes in regulatory and/or business requirements, centralized and validated data, and automated and advance exception detection and remediation. Respondents are using a wide variety of technologies to meet these requirements.

Respondents' answers to our survey and interview questions revealed clear trends that are summarized in **Table 1** and will be examined throughout this report.

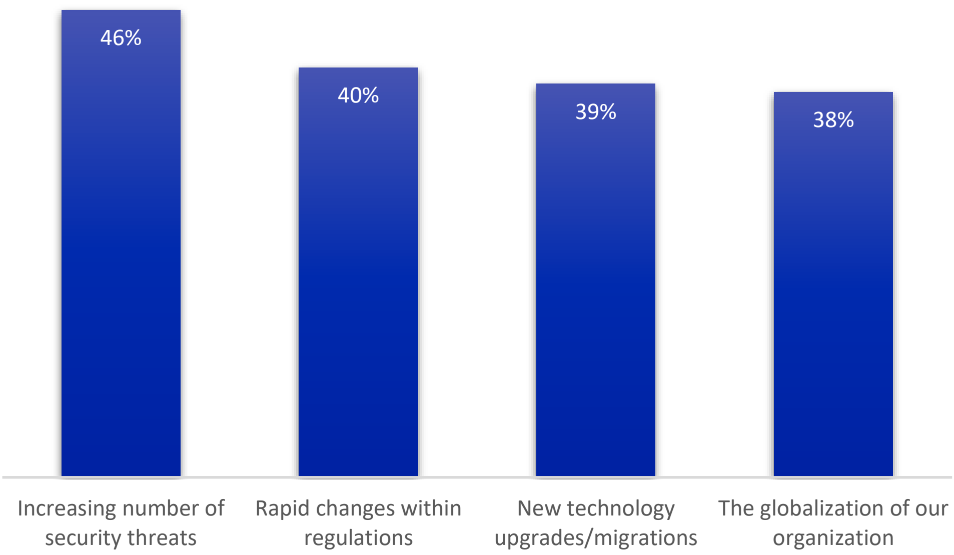
Table 1: DART model framework for GRC

Drivers	Actions	Requirements	Technologies
• Increasing number of security threats and attacks requiring more monitoring and detection (46%) • Rapid changes within compliance and data privacy regulations are adding to GRC staff workload (40%) • New technology upgrades/migrations such as the move to SAP S/4HANA and the cloud (39%) • The globalization of organization and business opening up new compliance and audit requirements (38%)	• Improve the level of automation within my GRC landscape to streamline processes (42%) • Centralize and automate my controls monitoring and management capabilities (42%) • Provide strategic and centralized visibility into potential risks and fraud (37%) • Bridge my on-premise and cloud-based security and access management process (37%) • Streamline user provisioning and access management (35%)	• Security monitoring and threat detection (77%) • Agility to respond to changes in regulatory and/or business requirements (76%) • Centralized and validated data (71%) • Automated and advance exception detection and remediation (65%) • Tight integration between my GRC and operational applications/ cross application SoD (64%) • Automated user access management and provisioning (63%)	• Data privacy and protection (49%) • Access Control (49%) • Process Control (39%) • Audit Management (37%) • Risk Management (33%) • Segregation of Duties Automation (32%) • Trade Compliance (32%) • GRC Automation (31%) • Fraud Management (30%) • GRC Analytics and Planning (30%) • Identity Management for Cloud access (30%)

What Drives GRC Strategy?

Increasing security threats and attacks requiring more monitoring and detection (46%) was the most cited driver for GRC strategy among our survey respondents. Rapid changes within compliance and data privacy regulations (40%) describe the next major driver, followed by new technology upgrades/migrations such as the move to SAP S/4HANA (39%) and the globalization of organizations opening up new compliance and audit requirements (38%) (**Figure 3**).

Figure 3: Top GRC Drivers



Source: SAPinsider, May 2022

GRC strategy at respondents' organizations is increasingly driven by security threats and attacks. This area is typically handled by security departments, but GRC skills in addressing risk and access control are being tapped to assist with broadening security challenges. Cybersecurity and GRC have become so intertwined that increasing security threats moved to the top driver in 2022, supplanting new technology upgrades and migrations—the top driver from 2021.

Regulatory challenges are behind two other major GRC drivers—rapid changes to data privacy regulations and globalization opening up new regulatory requirements. This highlights the challenges that businesses and audit teams face to keep up with the latest rules and laws.

Beyond the top drivers, a rise in the impact of increasing volatility of customer demand and supply chains is noteworthy. This was picked as a top driver among 27% of respondents, a big jump from just 9% a year ago. In our research with CIOs, we found that supply chain disruption was top of mind when setting their agendas. This disruption

INSIDER PERSPECTIVE

"Being a public company, we must control our data. We have data privacy requirements and more requirements coming from different places. Our tools need to be built for that type of change, but at the same time support our business processes."

~ Adarsh Hegde
Senior Manager, Digital Transformation,
HP

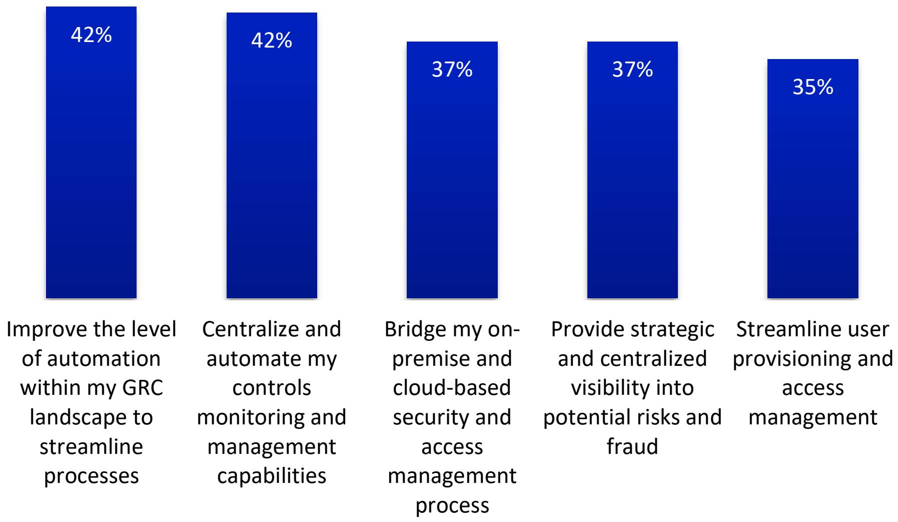
brings about risk for an organization, and that risk is moving up the list of priorities at many organizations.

As businesses go global, supply chain disruption and regulatory requirements become bigger issues. Globalization also bring more touchpoints, more potential for attacks, which increases the chance for security threats.

How Do SAPinsiders Address Their Drivers?

Much like in 2021, automation and centralization are top themes among the actions SAPinsiders are taking to address top drivers. Improving the level of GRC automation was the top action cited (42%) along with centralizing and automating controls monitoring and management (42%), closely followed by bridging on-premise and cloud based security and access management processes (37%), and providing strategic and centralized visibility into potential risks and fraud (37%) (**Figure 4**).

Figure 4: Top GRC Strategies



Source: SAPinsider, May 2022

Centralization and automation are key actions that can stretch the capabilities of GRC professionals, limiting the number of systems they need to access in order to find risk and compliance data and shortening the amount of time they spend on risk and compliance tasks. Easier access to key information also allows GRC professionals to be agile and react to changes in regulation or internal requirements.

New technologies are also impacting the actions that companies are talking, particularly when it comes to bridging on-premise and cloud-based security and access management and reducing cross-application risk. Both categories took big jumps from our 2021 numbers. Bridging on-premise and cloud-base security and access management rose to 37% from 18%, while reducing cross-application risk moved from 9% in 2021 to an action

INSIDER PERSPECTIVE

"With automated user access, you basically remove the constraint of a person not understanding what they need to do their job. That's where automation helps you, you are pre-deciding this role should have this access. It helps the user to avoid overthinking what they should need, and they can just get started on Day 1."

~ Adarsh Hegde
Senior Manager, Digital Transformation
HP

taken by 23% of respondents this year. The theme of access also shows up again among the top actions, as 35% of respondents are looking to streamline user provisioning and access management.

Overall, companies are still looking to automate and centralize GRC processes, however there is more focus on the risk and security issues associated with the integration of many apps across their organization's technology stack.

The Number of Applications Impacts Compliance Priorities

How does the number of applications integrated with SAP that are included in compliance's scope impact the actions that companies take? When companies have 11-20 applications in their compliance scope, they are slightly more likely to be bridging on-premise and cloud-based security. However, they are more than twice as likely to be providing strategic and centralized visibility into potential risks and fraud than those that have 6-10 applications in their compliance scope.

With a greater number of applications, it becomes more difficult to individually track areas of potential risk and fraud. That's where a centralized view of risk that goes across applications can help—if a GRC professional can access risk data related to applications in a single place, that saves the time of analyzing risk by logging into several different systems.

The number of applications integrated to SAP in the compliance scope also impacts what is driving GRC strategy at organizations. The top drivers for respondents' organizations with 11-20 applications are increasing security threats and globalization. Those with 6-10 applications are more driven by rapid changes in data privacy regulations and new technology upgrades and migrations. For those companies that have five or less applications, the top driver is the rising cost of compliance.

It's likely that the companies with more applications are also larger organizations, and larger organizations are more likely to be targets for security attacks. Smaller organizations may not be as concerned with those challenges, instead focusing on upgrading their systems and staying compliant with the latest regulations with smaller compliance teams.

INSIDER PERSPECTIVE

"We have more than 30 integrated apps. We try to make access control easy for everyone with the way it is structured in our system. As long as they are logged into the system network domain, they are authenticated with active directory."

~ Michael Agbamuche,
Asset Security Advisor,
Oil and Gas Company

Key Takeaways

Based on our research with respect to GRC, the following takeaways are clear:

- **Centralize application risk data for efficiency.** This is particularly relevant as your company adds more applications to its technology stack. Having a one-stop shop to analyze risk across applications saves time and enables GRC professionals to see where cross-application risk may exist.

- **Identify how changes in the business impact supply chains.** Supply chain disruption is a growing area of risk, and as businesses change and move into new countries, there are new regulations to follow. Disruption may be difficult to predict but preparing for changes may help create a more resilient organization.

- **Evaluate GRC processes for automation potential.** GRC automation is the top action overall in our survey, and automation is key to not only efficiency but accuracy for GRC teams. Find the repeatable processes that will work well for automation and save time and resources.

- **Determine how access is impacted by new technologies.** If your company is implementing a new system, such as SAP S/4HANA, there are likely going to be different role definitions that impact how access is granted. New systems also add new access touchpoints, bringing more risk.

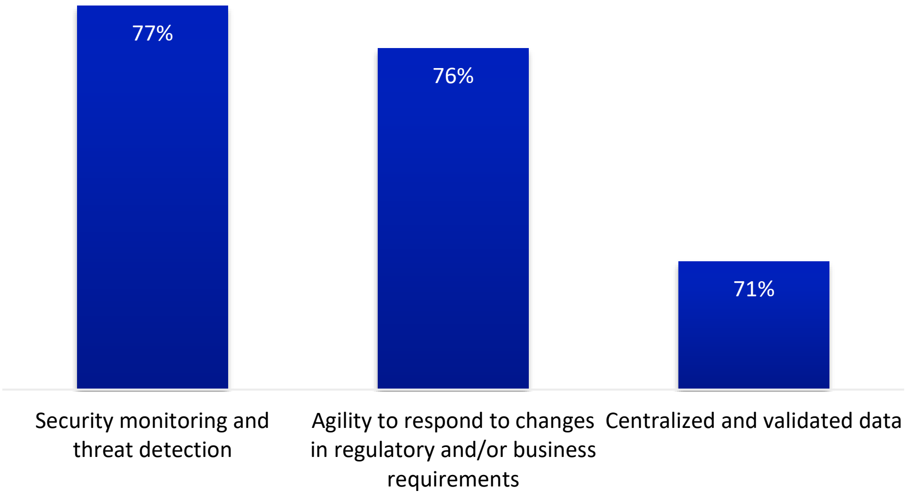
Chapter Two: How Do SAPinsiders Approach GRC Technology?

Next, we'll examine the top GRC requirements and technologies at respondents' organizations. We'll also look at the top GRC solution and technology investments that companies are planning for 2022.

Top GRC Requirements

Security monitoring and threat detection is the top requirement in our survey, indicated as important or very important by 77% of respondents. It was also the leader in "very important" category, listed by 43% of our respondents. Other top requirements include agility to respond to changes in regulatory or business requirements (76%), centralized and validated data (71%) and automated and advance exception detection and remediation (65%) (**Figure 5**).

Figure 5: Top GRC Requirements



Source: SAPinsider, May 2022

Security monitoring and threat detection repeats as the top requirement from 2021, when it was at 76%. This suggests that secruity threats are now fully a part of GRC responsibilities. Given that 43% of respondents now view it as very important vs. 30% last year, security monitoring and threat detection are only going to become more ingrained in GRC processes.

Agility to respond to changes in regulatory/business requirements is a new option this year and instantly became one of the top requirements. This option was added because

INSIDER PERSPECTIVE

"A great challenge for us is insider threats. That is really something that anyone can't predict. Most times we are basically doing catchup. When something happens, some particular systems are shut down, we try to determine what got into the system. It's almost like being reactive rather than being proactive. We are putting a system in place to try to predict some of these threats."

~ Michael Agbamuche,
Asset Security Advisor,
Oil and Gas Company

of feedback from other studies, including executive research, which indicated that companies are striving to be more resilient in the face of changing business models, regulatory shifts, supply chain disruption, and globalization.

The requirement for automated and advance exception detection and remediation was also added this year based on feedback from the GRC market. This ties into threat detection as a top requirement—companies are looking to their GRC staffers and technology to help stop threats before they become an issue.

Other significant requirements include tight integration between GRC and operation apps (64%), improved audit tracking (64%), and single sign-on capabilities (63%). These, along with the top requirement for centralized and validated data, show companies are wanting more integration, consolidation, and visibility from their GRC efforts.

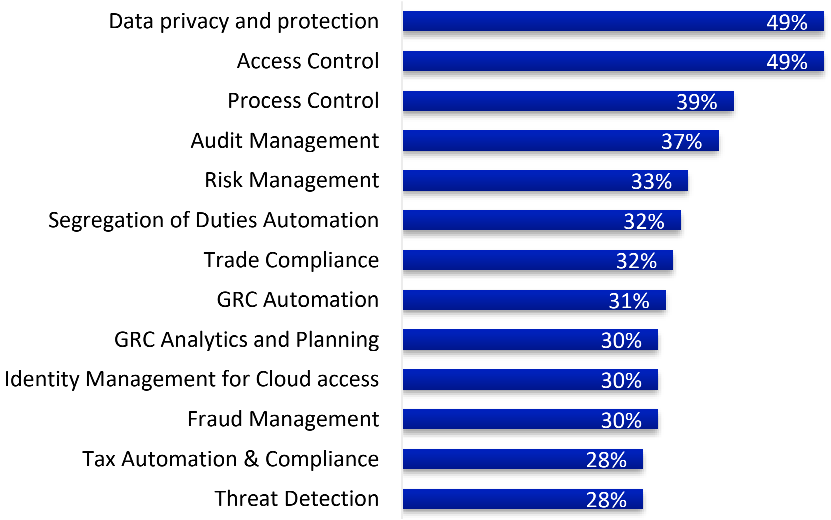
Overall, companies are looking to become more resilient and agile, and that includes GRC, where compliance requirements and risk vectors are changing and growing. The expertise of GRC teams in identifying risk is being tapped to identify and detect security threats.

Which GRC Technologies Do Respondents Use?

The most common GRC tool we asked about currently in use is data privacy and protection, which is in use at 49% of respondents' organizations, up from 28% in 2021. With the rise in data privacy laws like GDPR, companies have been putting in processes and systems in place to comply with those regulations.

Access Control is also in place for nearly half of respondents (49%). Access tools are increasing in importance as companies bring in cloud technologies alongside legacy systems. Identity management has become more popular for managing access as cloud software has proliferated. In kind, identity management for cloud access tools are now in use at 30% of organizations surveyed, up from 17% in 2021 (**See Figure 6**).

Figure 6: GRC Technologies in Use or Have Been Used



Source: SAPinsider, May 2022

INSIDER PERSPECTIVE

"I'd say we are edging up on the mature end of the scale, although since our external auditors always find something small each year, it's not 100% perfect because we have not predicted every test and it's not possible to throw enough resources at it to be 100% perfect either."

**~ Sr. Global IT Auditor
Furniture Company**

More classic GRC tools are among the next most common technologies in place—process control is in use or has been used at 39% of respondent organizations, followed by audit management (37%), risk management (33%) and segregation of duties (SoD) automation (32%). The more generic "GRC Automation" is in use at 31% of organizations.

Despite security being a top theme among drivers and requirements, adoption of threat detection software is tied with tax automation and compliance as the lowest levels of current use (28%). However, threat detection is currently being implemented at 29% of respondents' organizations (tied for the highest rate of current implementation) and is being evaluated by another 29% of respondents. It will be interesting to check back next year to see how adoption rates have changed for threat detection, given how security threats are driving GRC strategy.

Overall, adoption is trending up for many GRC technologies. Most technologies in our survey have higher rates of current usage as well as higher rates of current implementations in process. On the other side, there are far fewer respondents who are saying they have "no plans" to adopt GRC technologies.

Companies are increasingly looking to get more out of their staff by giving them tools to succeed. GRC technologies are necessary in many cases to meet top requirements such as agility to respond to changes in regulatory or business requirements and centralized and validated data.

How Leadership Impacts Technology Adoption

Depending on the organization, different executive roles ultimately lead GRC strategy. The titles can range from CIO and CTOs to CFOs or even GRC-specific leaders such as Chief Compliance Officers, Heads of Internal Audit or Risk Management.

Among our respondents, the title of the executive in charge of GRC has a significant impact on GRC technology adoption.

In respondents' organizations where a CFO held GRC responsibilities, there are higher current usage rates for many technologies, including data privacy and protection (62%), access control (55%). The most significant difference is in GRC Automation adoption--over half (52%) of respondents with CFOs leading GRC are currently using GRC Automation technology. That's more than 20% higher than the rest of the respondents.

GRC strategy leaders with GRC-specific titles also impact technology adoption. When looking at companies with a Chief Compliance Officer, Head of Risk Management, or Head of Internal Audit in charge of GRC strategy, adoption rates are higher for core GRC functionalities. Specifically, current usage rates are higher for access control (60%), process control (50%), and risk management (43%).

CFOs and GRC teams deal directly with governance, risk, and compliance issues every day. Other technology leaders' teams may not be as focused on those areas, and they may not see the need for investment in GRC technologies.

Key Takeaways

When it comes to equipping organizations with the capabilities and technologies required to implement an effective GRC strategy, consider the following:

- **Ensure leaders understand your organization's GRC requirements, and the technologies that enable them.** It's clear that in organizations where the executives driving GRC strategy have direct ties to GRC topics, there is greater adoption of GRC technologies. If your GRC team needs certain technologies to accomplish their goals, leadership needs to be keenly aware of what is needed and why.

- **Assess if you have the tools needed to comply with data privacy regulations.** GDPR and similar regulations seem to be having an impact on technology adoption. Does your company have what it needs in place to keep personal data safe? Evaluate your processes and technology to find out and plan on what might need to be done.

- **Play the long game with GRC initiatives if necessary.** It's hard to push GRC technology adoption when budgets aren't growing—but we are still seeing usage grow. Tools such as threat detection may be low on the adoption scale, but it appears more companies will soon have threat detection in place—that's after multiple years of security threats being a top driver and security threat detection and remediation being a top requirement. Continue to emphasize GRC needs to those in charge of investment, and it may eventually bear fruit.

- **Evaluate your compliance agility and resilience.** Three-quarters of respondents' organizations see agility to respond to compliance changes as important. How have your GRC processes handled sudden changes in regulations or company policies? Find out if there are any process or technology upgrades that can make you more agile.

INSIDER PERSPECTIVE

"Tax compliance is critical for our company and governments are becoming more demanding and implementing more aggressive audits."

**~ Finance and Tax Compliance Professional
Consumer Goods Company**

Chapter Three: How Top GRC Organizations are Succeeding

We asked respondents to evaluate how satisfied they are with their current GRC processes on a scale of 1 to 10, with 10 being completely satisfied. Overall, respondents were generally satisfied with an average score of 7.6 and 8.0 being the median score. Still, there are distinct differences between those that are above the median score and those that are below.

For those above median satisfaction, their organizations are more likely to be taking action around centralizing and automating controls monitoring and management (58% vs. 42% of those below the median). These leading organizations are also looking more often to provide strategic and centralized visibility into fraud risks (38% vs. 29%), more focused on preparing to support new legal and regulatory requirements (25% vs. 16%).

On the other end, respondents with satisfaction under the median are at organizations focused more on streamlining user provisioning and access management (39% vs. 29%) and providing more intelligence within GRC processes (26% vs. 8%).

In terms of actions, those above median satisfaction are more likely focused on centralizing and automating GRC processes, while those under median satisfaction are still looking to fine tune the processes. Leaders have moved beyond this step—likely because they are sound in their processes and are now looking to create greater efficiencies by automating and integrating across the business.

Respondents above median satisfaction are much more likely than those under median satisfaction to find improved audit tracking very important (42% vs. 13%), more likely to find centralized and validated data very important (29% vs. 18%), much more likely to find single sign-on very important (42% vs. 21%), and much more likely to find mass user lock/unlock capabilities very important (62% vs. 39%). Leading organizations are also more likely to find tight integration between GRC and operational apps very important (29% vs. 16%) and much more likely to find automated user access management and provisioning important or very important (75% vs. 50%).

Overall, leaders see topics are centralization, automation, and integration to be among their very important requirements more often than those less satisfied with their GRC processes.

When it comes to investment and skillsets, those above median satisfaction are more likely to have larger budgets (29% vs. 13%) and more likely to have growing teams (25% vs. 11%). Leaders are more often looking to invest in cybersecurity (70% vs. 50%) and data privacy (50% vs. 34%), and tax compliance (29% vs. 13%).

Leaders are generally focused on areas of security more often than those below median satisfaction. Those with above median satisfaction are more often emphasizing cybersecurity skillsets (63% vs. 47%). Respondents' organizations under median satisfaction are emphasizing controls monitoring management (50% vs. 38%) and automation (45% vs. 33%) more often.

Those organizations under median satisfaction may still be looking to find skillsets to move forward with GRC while leaders already have those in place. Leading organizations can now focus more on the security aspect of GRC.

Required Actions

Our research reveals that SAP customers should apply the following key steps to build a successful GRC strategy:

- **Fine tune your processes to enable automation.** Top GRC organizations are automating processes, while others are still figuring out processes that work for their business. Automation is key to optimizing GRC staff resources, but processes need to be sound first. Focus on getting processes to the point where they can be successfully automated.
- **Centralize your risk and compliance data.** The best GRC teams are focused on centralizing and validating data. Risk prioritization is helpful to companies trying to optimize their risk avoidance. It's difficult and more time-and-resource-consuming to prioritize risks across a business without a holistic view of risk and compliance information.
- **Focus GRC efforts on improving user access provisioning and management.** Access control is top of mind for companies with leading GRC processes. Prioritize those processes and technologies that make user provisioning and access easier to manage with functionalities such as single sign-on, mass user lock/unlock capabilities, and access management automation.
- **Utilize your GRC skillsets to bolster your company's security efforts.** Focus on cybersecurity is a primary characteristic of companies with GRC process satisfaction above the median. Determine what skillsets, such as risk analysis, can assist with cybersecurity. This makes your GRC staffers more valuable to the business. GRC groups that are more focused on cybersecurity are also more likely to see growing GRC budgets and staffs.

INSIDER PERSPECTIVE

> **"Our focus this year is on improving controls and we are specially focused on using automation and taking advantage of the data we produce."**
>
> **~ GRC Professional**
> **Retail Company**

Methodology

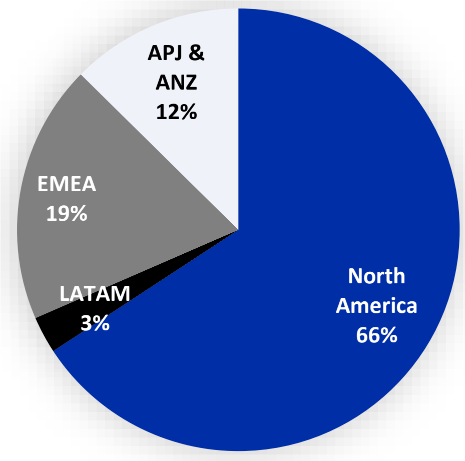
In April and May of 2022, SAPinsider examined the experiences of business and technology professionals around how they are approaching GRC. Our survey was administered to 124 members of the SAPinsider community and generated responses from across a wide range of geographies, industries, and company sizes. Respondents completed an online survey and provided feedback in customer interviews that questioned them on topics such as:

- Which GRC tools are your organization currently using?
- How satisfied are you with your company's GRC processes?
- What are the requirements for your GRC strategy?
- What is driving your GRC strategy?

The demographics of the respondents included the following:

- **Job function:** Functional areas reported by respondents include: Information Technology (33%); Human Resources/Benefits Administration (14%); GRC/Risk/Audit/Compliance/Legal (13%); Professional Services/Consulting (10%); Operations (7%); Security/Information Security (7%), Finance/Tax (6%) Managed Services (5%); Other (3%); Quality/Standards (2%).
- **Market sector:** The survey respondents came from every major economic sector, including: Industrial (34%); Software and Technology (30%); Media and Entertainment (10%); Retail and Distribution (10%); Financial Services and Insurance (7%); Public Services & Health Care (6%); and Hospitality, Transportation, and Travel (3%).
- **Geography:** Of our survey respondents, 66 were from North America; 19% from Europe, the Middle East, and Africa (EMEA); 12% were from Asia-Pacific, Japan, and Australia (APJ & ANZ); 3% were from Latin America (LATAM).

PARTICIPANT PROFILE



Appendix A: The DART^{TM} Methodology

SAPinsider has rewritten the rules of research to provide actionable deliverables from its fact-based approach. The DART methodology serves as the very foundation on which SAPinsider educates end users to act, creates market awareness, drives demand, empowers sales forces, and validates return on investments. It's no wonder that organizations worldwide turn to SAPinsider for research with results.

The DART methodology provides practical insights, including:

- **Drivers:** These are macro-level events that are affecting an organization. They can be both external and internal and require the implementation of strategic plans, people, processes, and systems.
- **Actions:** These are strategies that companies can implement to address the effects of drivers on the business. These are the integration of people, processes, and technology. These should be business-based actions first, but they should fully leverage technology-enabled solutions to be relevant for our focus.
- **Requirements:** These are business and process-level requirements that support the strategies. These tend to be end-to-end for a business process.
- **Technology:** These are technology and systems-related requirements that enable the business requirements and support the company's overall strategies. The requirements must consider the current technology architecture and provide for the adoption of new and innovative technology-enabled capabilities.

Report Sponsors

VERTEX

Vertex, Inc. is a leading global provider of indirect tax software and solutions. The company's mission is to deliver the most trusted tax technology enabling global businesses to transact, comply and grow with confidence. Vertex provides cloud-based and on-premise solutions that can be tailored to specific industries for major lines of indirect tax, including sales and consumer use, value added and payroll. Headquartered in North America, and with offices in South America and Europe, Vertex employs over 1,200 professionals and serves companies across the globe.

pathlock

Pathlock brings simplicity to customers who are facing the security, risk, and compliance complexities of a digitally transformed organization. New applications, new threats, and new compliance requirements have outpaced disparate, legacy solutions. Pathlock provides a single platform to unify access governance, automate audit and compliance processes, and fortify application security. With integration to 140+ applications and counting, Pathlock customers can confidently handle the security and compliance requirements in their core ERP and beyond.

Whether it's minimizing risk exposure and improving threat detection, handling SoD with ease, or unlocking IAM process efficiencies – Pathlock provides the fastest path towards strengthening your ERP security & compliance posture.

Learn more at www.pathlock.com.

SAPinsider

SAPinsider comprises the largest and fastest-growing SAP membership group worldwide. It provides SAP professionals with invaluable information, strategic guidance, and road-tested advice, through events, magazine articles, blogs, podcasts, interactive Q&As, white papers and webinars. SAPinsider is committed to delivering the latest and most useful content to help SAP users maximize their investment and leading the global discussion on optimizing technology.

For more information, visit SAPinsiderOnline.com.