JULY 2026

SAPinsider

Intelligence Benchmark SERIES

Benchmarking the Capabilities that Define SAP Leaders

GRC and Risk Intelligence for SAP

By Robert Holland
Chief Research Officer

RESEARCH PARTNER
SAP

SPONSORED BY
Saviynt

Executive Summary

Governance, Risk, and Compliance (GRC) in SAP environments has been about managing user access, enforcing internal controls, assessing corporate risk, and streamlining audits. However, that mandate is expanding to include the governance of artificial intelligence (AI) usage and solutions, something for which GRC teams may not be entirely prepared. This points to 2026 being an inflection year. The technical and financial foundations of GRC have caught up to the ambition organizations expressed a year ago, while structural governance and native SAP tooling have not kept pace with that momentum. Understanding both sides of the story, the acceleration and the lag, is essential for any organization planning GRC investment through 2027.

Between March and June 2026, SAPinsider surveyed its global community to benchmark how GRC practices are evolving inside the SAP ecosystem, and to measure what is changing. The clearest signal in this year's data is money (Figure 1). Respondents reporting a significantly increased GRC and risk intelligence budget more than tripled year over year, from 7% to 23%. For the first time no respondents reported a budget decrease of any size, compared with 7% reporting a significant cut in 2025. Combined, nearly three in four respondent organizations (72%) increased their GRC budget in some form this year, up from roughly 47% last year.

FIGURE 1

GRC and Risk Intelligence Budgets

That funding shift tracks a change in what is driving investment. Cybersecurity, fraud, and risk exposure grew from 56% to 68% this year making it the most important driver of GRC strategy. Slipping slightly from last year is the need for technology modernization and transformation, although this was still reported as important by half (50%) of this year's respondents. Regulatory complexity edged up modestly (from 16% to 21%), while interest in emerging technologies and AI as a GRC driver softened slightly (from 36% to 31%). This is a sign that AI is increasingly treated as embedded infrastructure rather than a standalone investment driver.

23%

of respondents report that they have seen a significant increase in GRC budget this year.

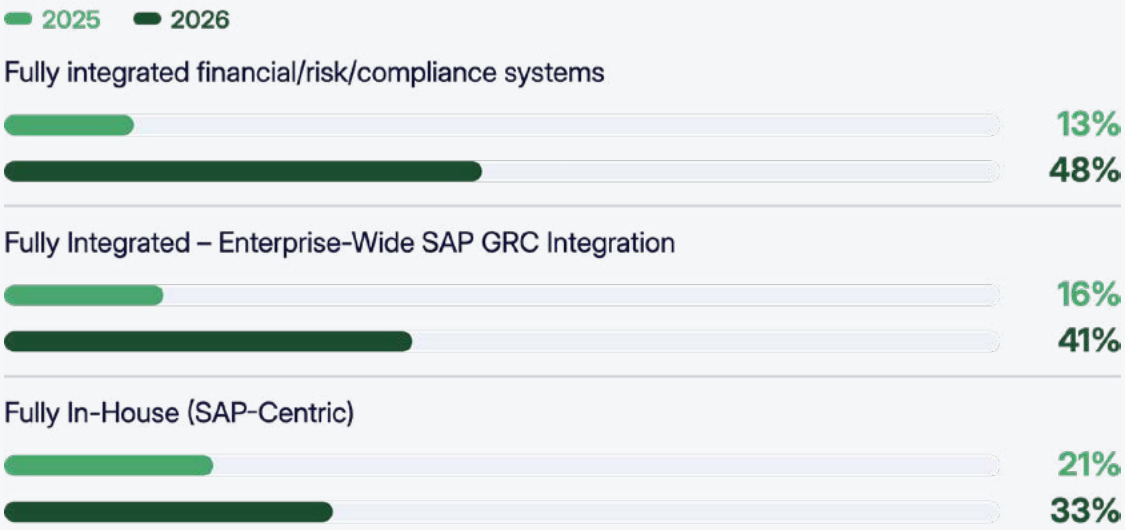
For customers planning next year's budget cycle, this shift changes the framing GRC leaders should use to secure investment. When budgets were flat or shrinking, the winning argument for GRC spend was compliance avoidance: fund this or risk a finding. That argument no longer matches where the money is going. Boards and CFOs are now funding GRC as a resilience and business-continuity function tied directly to cyber and fraud exposure, with a much larger AI portion in the future, which means the strongest business cases in 2027 will be the ones framed around operational risk reduction and incident-response readiness rather than regulatory checkbox compliance. Organizations that continue pitching GRC investment purely as an audit or compliance necessity risk under-selling their case and losing ground to peers who have already reframed the conversation around enterprise resilience.

The Integration Inflection Point

Organizations reporting their financial systems as fully integrated with risk and compliance data for real-time insight jumped from 13% to 48%. Organizations describing their GRC systems as fully integrated enterprise-wide across departments rose from 16% to 41%. And the sourcing model itself polarized: fully in-house SAP GRC management rose from 21% to 33%, while hybrid models (the dominant model in 2025 at 58%) fell to 41%, with fully outsourced management emerging from 0% to 14%. Organizations are not drifting toward integration incrementally; they are committing to it. They are also committing more decisively to one sourcing model or the other rather than sitting in the hybrid middle.

FIGURE 2

The Integration Inflection Point



The move towards fully integrated or fully in-house systems is shown in Figure 2. It starts with the level of integration of financial systems with risk and compliance data for real-time insights. In 2025, 53% of respondents reported that their financial systems were only partially integrated with just 13% reporting full integration. This year, 48% report full integration while 43% are now partially integrated as the number of respondents reporting minimal integration dropped from 33% last year to just 7% this year.

Looking at the level of integration of GRC systems and initiatives across departments, last year the two most likely responses from respondents were mostly integrated (37%) or partially integrated (26%). This year, 41% report full enterprise-wide integration while only 22% report they are mostly integrated and just 3% report no integration down from 11% last year.

Last, although a hybrid approach to managing GRC systems and initiatives is still the most likely scenario (41%), this has dropped from 58% last year just as a fully in-house SAP-centric approach to integration has risen to 33%. These three factors demonstrate the inflection point where organizations are fully committing to integrated GRC across the enterprise using a single sourcing model where possible.

Identity and Access Governance Moves to the Front Line

Identity, access, and segregation-of-duties (SoD) governance is this year's fastest-rising theme, showing up consistently across strategy, requirements, and technology adoption. As a strategic action, integrating identity, access, and entitlement governance jumped from 38% to 54% (Figure 3), the single largest increase among all strategic actions that organizations are taking to strengthen GRC. As a requirement for enabling the business to fully execute GRC strategy, it surged even further, from 14% to 40%. This moves integrated identity, access, and SOD governance from a minor consideration to the second-most-cited requirement in the survey.

The underlying technology adoption data confirms this is more than sentiment. Those currently using Zero Trust architecture grew from 6% to 35% year-on-year. At the same time, use of User Behavior Analytics grew from 5% to 40%. Endpoint Detection and Response grew from 12% to 39%, and Data Loss Prevention from 12% to 36%.

Nearly every access and security control category in the survey roughly tripled in current adoption over the past year. The one meaningful exception worth flagging is Privileged Access Management, which declined slightly (from 41% to 32%). This could be a ceiling effect, since it was already the most broadly adopted control in 2025, with much of the movement now showing up in active implementation rather than net-new adoption.

INSIDER
INSIGHT

"We have an increased budget for GRC this year, but with the greater visibility we need into evolving threats, AI, and the need to mitigate risk it will be challenging to meet all our needs."

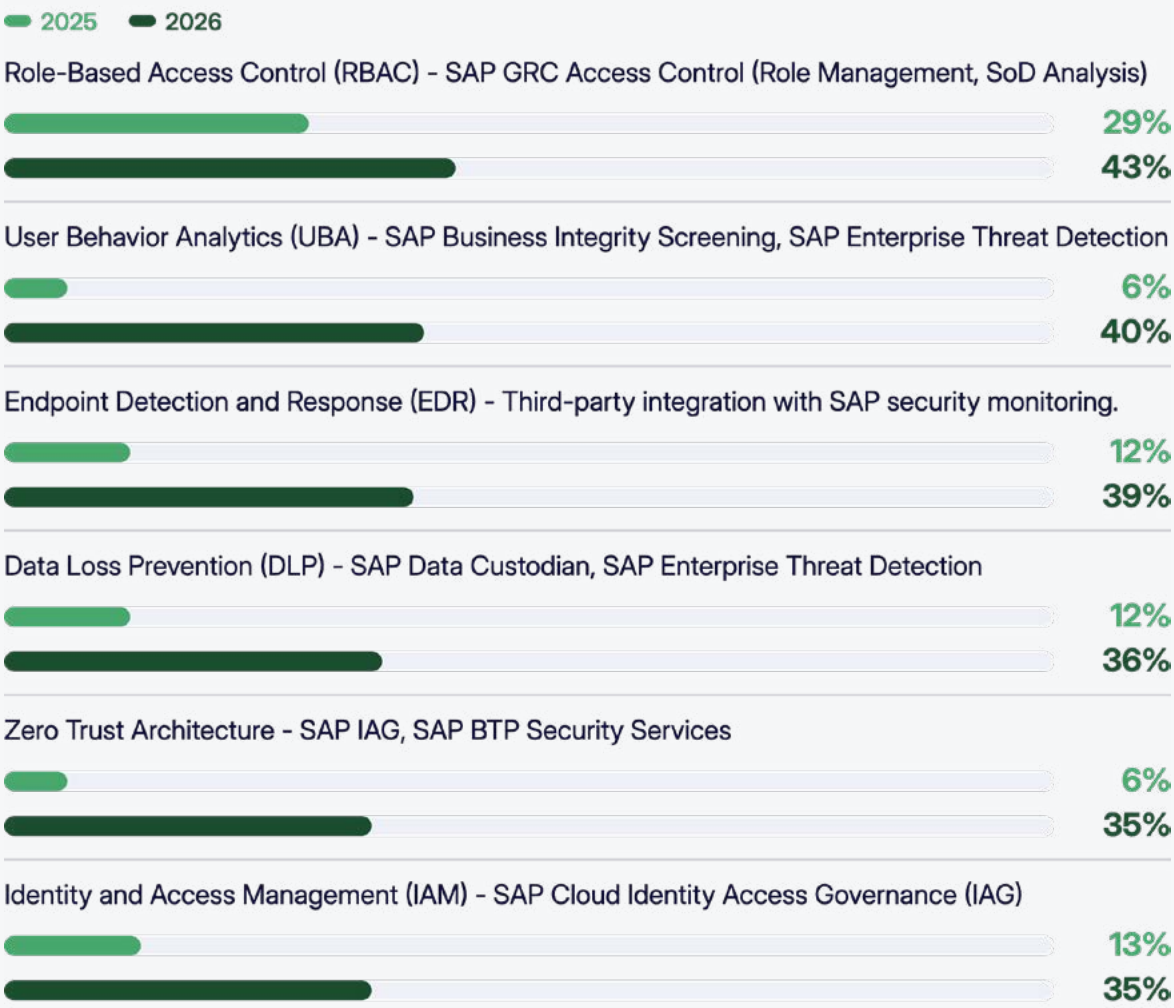
SECURITY/IT SPECIALIST, SOFTWARE AND TECHNOLOGY COMPANY

In contrast, although identity and access governance rose in priority for respondents, agility to adapt GRC processes to evolving requirements saw a significant drop in the number of respondents focusing on the topic falling from 19% to just 3%. Whether this is because organizations feel they have already solved issues regarding process flexibility and are now redirecting attention toward harder technical controls or because of an urgent need to focus on identity, access, and SoD is unclear.

The decline in agility as a stated business requirement is the more telling part of this shift. Organizations appear to be moving away from a mindset where GRC needed to remain flexible enough to adapt to whatever came next, and toward a mindset where the identity layer itself becomes the fixed, automated control that enforces policy by design. In practice, this means identity is displacing the network as the perimeter organizations defend, and it changes the skills and roles GRC teams need to prioritize going forward. Customers building GRC roadmaps should expect identity engineering and access analytics capabilities to become as central to the GRC function as traditional audit and controls-testing skills have historically been and should staff and budget accordingly rather than treating identity as a security-team-only concern.

FIGURE 3

Identity and Access Technology Adoption Nearly Triples

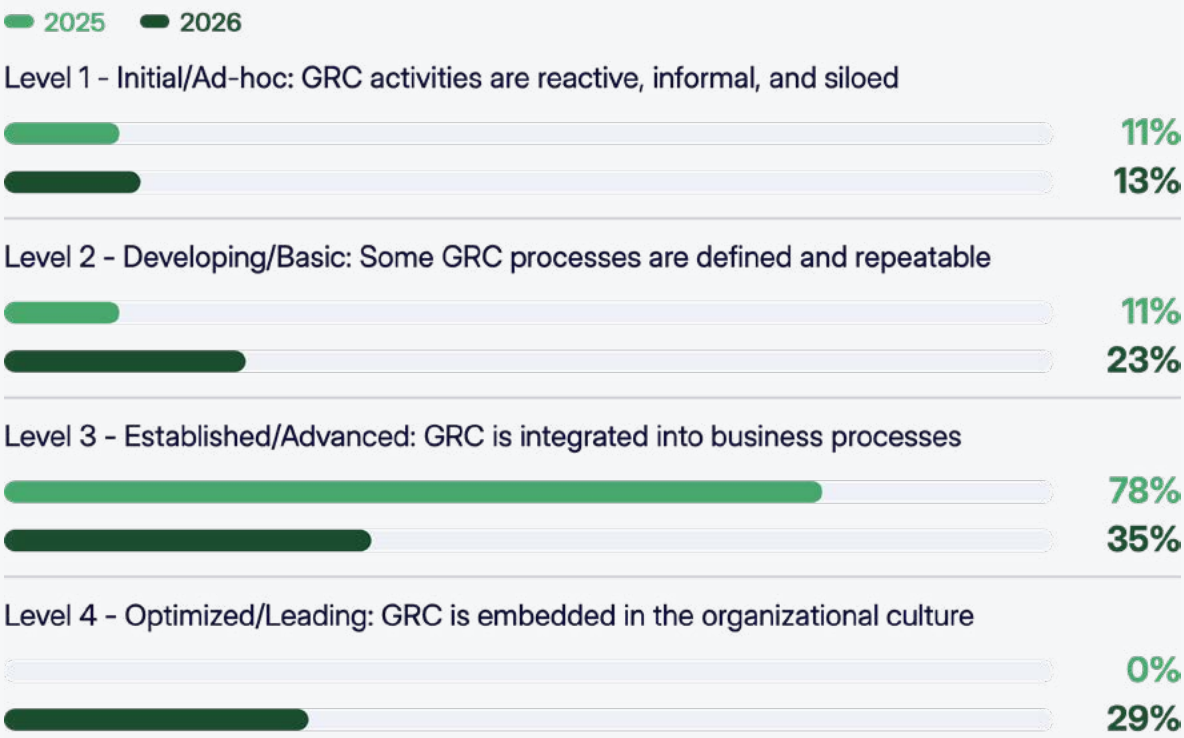


Maturity Self-Perception Recalibrates

In 2025, an unusually high 78% of respondents rated their organization's GRC maturity as "Established/Advanced," a concentration that suggested self-assessment inflation rather than a genuine maturity curve. In 2026, that figure dropped sharply to 36% (Figure 4), while a new top tier, that of "Optimized/Leading," where GRC is embedded in organizational culture and driven by continuous, data-informed improvement, captured 29% of respondents, up from effectively zero the prior year. "Developing/Basic" also doubled, from 11% to 23%.

FIGURE 4

GRC Maturity Self-Assessment Becomes More Differentiated



This should not be seen as a decline in actual maturity. Instead, it appears that respondent organizations are grading themselves more honestly and producing a real distribution across the maturity spectrum rather than a single crowded midpoint. That is a healthier signal for the ecosystem and demonstrates a more credible self-assessment among those focusing on the GRC needs of their organizations.

78%

of respondents rated their GRC maturity as established or advanced.

The practical value of this recalibration is that benchmarking itself has become a more trustworthy exercise than it was a year ago. When nearly every organization rates itself as established, a maturity assessment tells leadership very little about where the real gaps are. A genuine spread means organizations can locate themselves honestly against peers rather than as a reassurance exercise for the board. For planning purposes, this is an invitation for GRC leaders to treat self-assessment as a diagnostic tool rather than a marketing document internally, and to use the emergence of a credible top tier as a concrete target state to plan toward rather than an abstract aspiration.

SAP Tooling

While there is good news to be found in the focus on fully integrated GRC and more organizations having an optimized GRC strategy, responses remain disjointed in some areas. The lowest-scoring question in the entire survey measured which SAP solutions organizations currently use to monitor, assess, and report on GRC or risk. SAP Analytics Cloud leads at just 41% adoption, and that is primarily for reporting purposes such as risk dashboards, scorecards, predictive analytics, and integrated reporting. At the same time the third most used solution continues to be manual or spreadsheet-based risk tracking which sits at 22%, or nearly one in four respondent organizations. Despite the surge in integration and budget discussed previously, adoption of SAP's purpose-built GRC suite remains fragmented, and a meaningful minority of organizations are still tracking risk manually.

Part of the challenge may well be the fact that there are so many SAP solutions that can be used to monitor, assess, and report on GRC and risk. While 27% of respondents report using the integrated GRC suite, another 6% are using just SAP Process Control. Also being used by respondents are SAP Cloud Identity Access Governance (21%), SAP Business Integrity Screening (21%), SAP Enterprise Threat Detection (17%), SAP Business Continuity Planning (16%), SAP Financial Compliance Management (11%), SAP Risk Management (6%), and SAP Privacy Governance, Compliance, & Risks (2%). While each of these solutions serve different needs, they present a complex landscape of solutions that may be difficult to parse.

INSIDER
INSIGHT

"We have had manual solutions in place for years but found them to be inaccurate no matter how conscientious people were. Our focus is now on implementing integrated GRC solutions from SAP as part of our move to SAP S/4HANA so that we no longer have to rely on a manual process or an outside system."

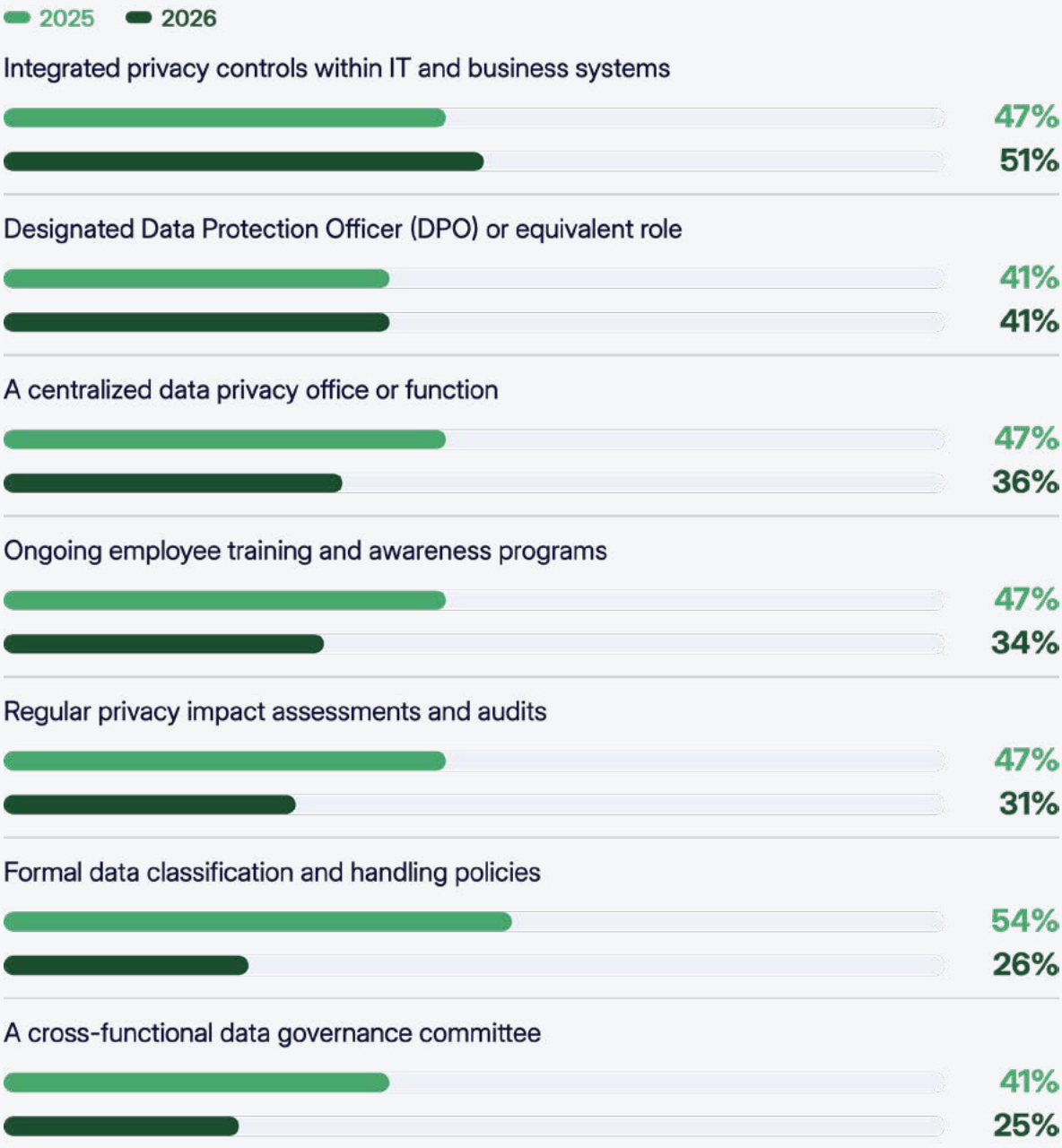
SENIOR GOVERNANCE MANAGER, GLOBAL MANUFACTURER

Data Privacy Governance Structures

The second area of concern is data privacy governance, where the results this year are more than just lagging what was reported in 2025. Coverage declined across nearly every structural governance mechanism year over year. Formal data classification and handling policies fell from 54% to 26% of organizations (Figure 5), regular privacy impact assessments and audits decreased from 47% to 31%, and ongoing employee training programs dropped from 47% to 34%. However, privacy integrated directly into IT and business systems rose modestly from 47% to 51%.

FIGURE 5

Erosion of Data Privacy Governance Structures



Read together, this suggests organizations are shifting privacy governance away from formal committees and policy documentation and toward embedding controls directly into technology. While this may be a rational response to resource constraints, it is one that leaves a documentation and audit-trail gap that regulators and auditors will likely flag. This finding is reinforced by the responses around data quality where lack of ownership or accountability for data quality is now the top-cited challenge at 44%, up from 35% last year. The combination of these changes points to an organizational accountability gap rather than a technology gap.

33%

of respondents identified technology and digital transformation risk as their most pressing risk concern.

Risk Priorities Pivot Toward Transformation

Among risks that are being prioritized over the next 12-to-18 months, technology and digital transformation risk nearly tripled in citation, from 13% to 33%, becoming the second-highest priority behind cybersecurity and data protection (Figure 6). Regulatory and compliance risk, which led the 2025 priority list at 44%, eased to 25% in 2026. Risk assessment cadence tightened in parallel: quarterly risk register updates rose from 13% to 30%, while biannual updates collapsed from 19% to 5%.

Together, these shifts suggest the risk conversation inside SAP organizations is pivoting away from keeping up with regulatory mandates toward managing the risk of platform transformation itself. This is a natural and important bridge to the broader SAP S/4HANA and SAP Business AI Platform migration wave already underway across the ecosystem.

This crossover signals a deeper change in how organizations think about the GRC function itself as it shifts from a primarily defensive discipline focused on satisfying external mandates toward a discipline that is expected to actively reduce the risk major business transformation programs like SAP S/4HANA migrations and AI platform adoption. That shift has organizational consequences that go beyond risk categorization. It means GRC leaders need a seat at the planning table for

INSIDER
INSIGHT

"Our goal is to automate GRC tasks so that we can remove mundane tasks from our core staff. This will free up significant time that we can use to improve our overall processes and strategies."

SENIOR ADMINISTRATOR, CONSTRUCTION COMPANY

transformation programs from the outset, not a review role bolted on near go-live. It also means transformation program budgets and timelines should build in GRC involvement as a core workstream rather than a compliance gate at the end. Organizations that continue to treat GRC as a downstream checkpoint for transformation initiatives will find their risk frameworks increasingly disconnected from where the enterprise's actual risk is concentrating.

FIGURE 6

Priorities Pivot Towards Transformation Risk

Required Actions

This year's benchmark report tells a story of uneven but real progress. Budgets are up, integration has leapt forward, identity and access governance has moved to the center of GRC strategy, and organizations are assessing their own maturity more honestly. At the same time, native SAP GRC tooling adoption remains fragmented, formal data privacy governance is eroding even as technical controls improve, and the risk agenda is shifting toward transformation risk faster than most governance structures are adapting to match it.

For SAPinsiders benchmarking their own organization against these findings, three actions stand out as immediate priorities.

Audit which GRC and risk tools you are using and close the manual-tracking gap this year.
With usage of SAP tools fragmented across different solutions and nearly a quarter of organizations still relying on manual or spreadsheet-based risk tracking, this is the single largest gap between the industry's stated ambition and its actual tooling. Organizations should inventory their current GRC toolchain against SAP's GRC offerings and treat any remaining manual processes as a near-term modernization priority rather than an acceptable interim state.

Rebuild formal data privacy governance structures in parallel with technical controls.
The decline in centralized privacy offices, cross-functional governance committees, and regular privacy impact assessments is a genuine regression, not a reallocation of effort that technology can offset. Organizations should reinstate or strengthen these formal structures now, before the accountability gap identified in the data quality findings becomes an audit finding or a regulatory exposure and before the AI governance that is increasingly falling on GRC teams overwhelms existing structures.

Treat identity and access governance investment as the leading indicator of GRC maturity and fund it accordingly.
Given that Zero Trust, UBA, EDR, and DLP adoption all roughly tripled this year, and that identity/access governance is now the fastest-growing business requirement in the survey, organizations that have not yet made comparable investments should benchmark themselves against these adoption rates immediately. Those already investing should use this year's budget momentum, with 71.6% of organizations reporting increased funding, to accelerate identity and access maturity further while the funding window remains open, rather than treating 2026 gains as a one-time catch-up.

DART
MODEL FRAMEWORK

STRATEGY AND NEEDS FOR GRC AND RISK MANAGEMENT

DRIVERS

- Cybersecurity, Fraud & Risk Exposure (68%)
- Technology Modernization & Transformation (50%)
- Emerging Technologies & Innovation (31%)

ACTIONS

- Integrating identity, access, and entitlement governance (54%)
- Automating GRC processes to reduce manual effort and improve efficiency (51%)
- Centralizing control testing, monitoring, and remediation workflows (44%)
- Unifying access and security governance across hybrid environments (40%)

REQUIREMENTS

- Single sign-on and federated identity management for secure, seamless access (82%)
- Automated and intelligent risk detection, exception handling, and remediation (81%)
- Integrated identity, access, and segregation of duties (SoD) governance (81%)
- Security monitoring and threat detection integrated with compliance workflows (79%)
- Intelligent and real-time risk and GRC reporting and quantification (73%)

TECHNOLOGIES

- Role-Based Access Control (RBAC) (43%)
- User Behavior Analytics (UBA) (40%)
- Endpoint Detection and Response (EDR) (39%)
- Data Loss Prevention (DLP) (36%)
- Identity and Access Management (IAM) (35%)
- Zero Trust Architecture (35%)
- Encryption and Tokenization (33%)
- Privileged Access Management (PAM) (32%)
- Attribute-Based Access Control (ABAC) (25%)

APPENDIX | THE DART™ 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 is 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 they 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

We're transforming identity. Turn on visibility, control, intelligence, and rapid time-to-value on the world's #1 converged identity platform, born in the cloud to power and protect the world's largest and most complex organizations everywhere. Now is the time to make the move to a more flexible and extensible access governance solution – one that addresses governance for all applications, not just SAP. Saviynt Identity Cloud's Application Access Governance (AAG) capabilities are recognized as industry-leading, not only for SAP, but for any application, including AD, databases and SaaS solutions. Stay ahead of application governance risk with fine grained integration and control that delivers enhanced security and audit readiness.

For more information, visit **saviynt.com**

RESEARCH PARTNER

SAP is creating opportunities through learning and development for all with free, self-guided, and premium learning resources, opportunities to engage in the SAP Community and to experience SAP solutions hands-on.

Learn more at **https://learning.sap.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 **SAPinsider.org.**