June 2026

SAPinsider

DETAILED FINDINGS

Benchmark Intelligence Report:

GRC and Risk Intelligence for SAP

By Robert Holland

RESEARCH PARTNER SAP | SPONSORED BY Saviynt

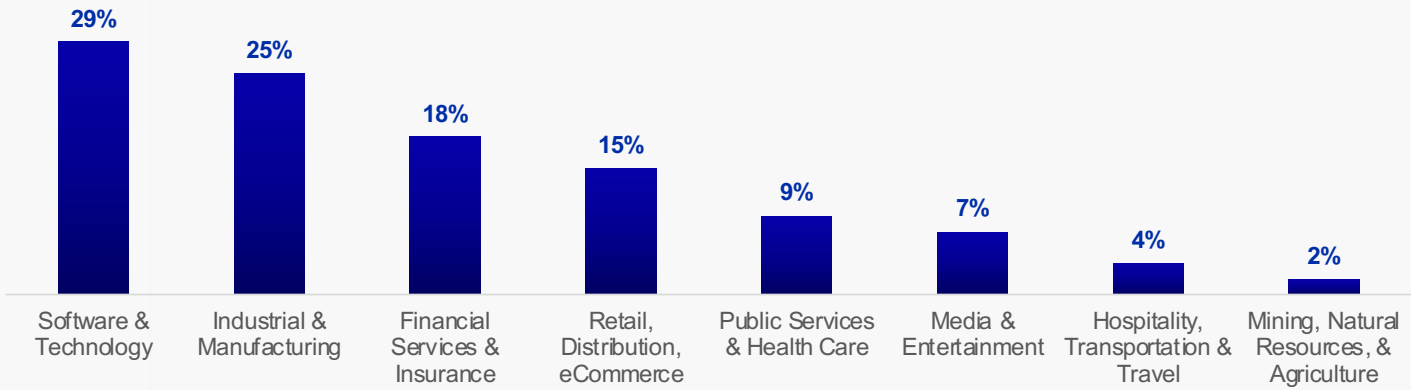
SAPinsider

1

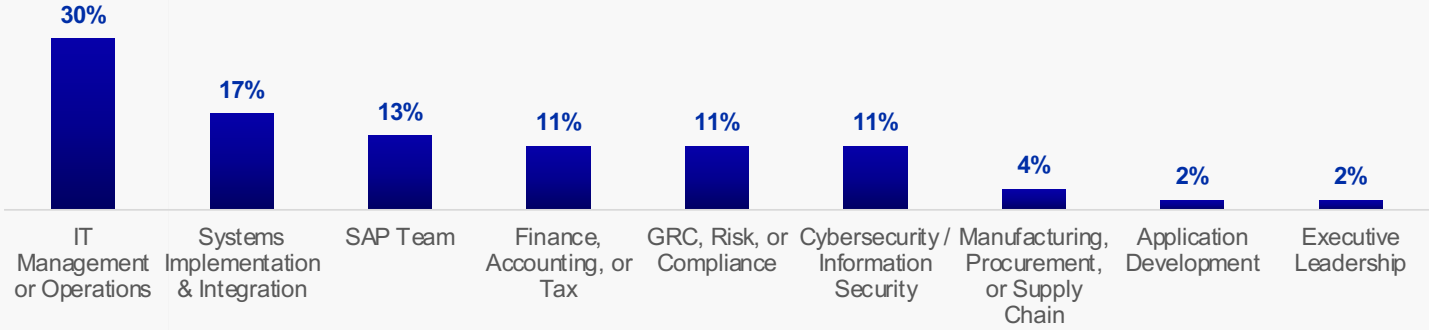
Industry and Role

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. This report explores how leading enterprises are responding to these challenges, how GRC funding is changing, and the technologies and strategies enabling smarter, more agile global GRC operations.

Industry



Role



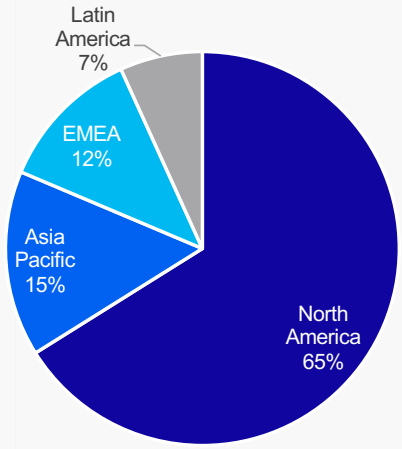
SAPinsider

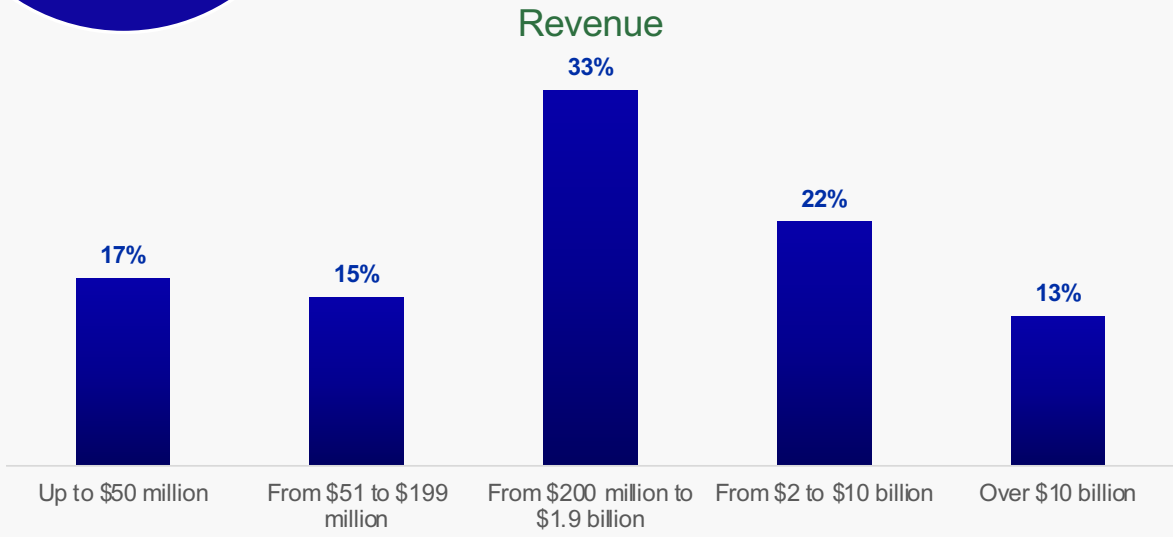
2

Region and Revenue

Respondents were primarily from North America with the next largest respondent group being from Asia Pacific followed by EMEA.

A third of respondents came from organizations that SAP categorizes as large enterprise. Another third are medium enterprise while the remaining third are from companies with annual revenues below $200 million.





SAPinsider

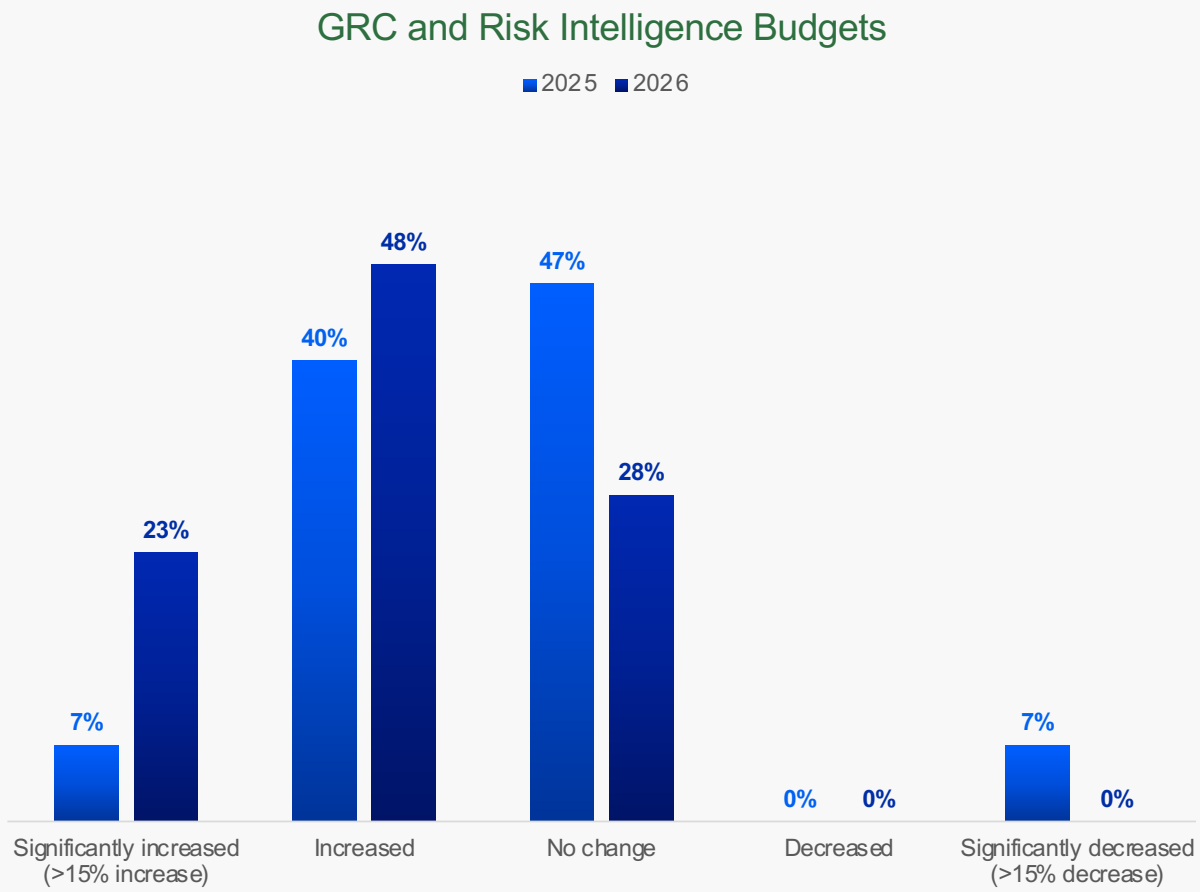
3

Strategic Foundation

Respondents reporting a significantly increased GRC and risk intelligence budget more than tripled compared to last year signifying the increased importance of GRC in SAP environments.

Additionally, no respondents reported a decrease of any size in budget compared to 2025, and nearly three in four respondents (72%) increased their GRC budget in some form this year.

This funding shift points to 2026 being an inflection year for GRC with the technical and financial foundations of GRC having caught up with the ambition that was beginning to be expressed in 2025.



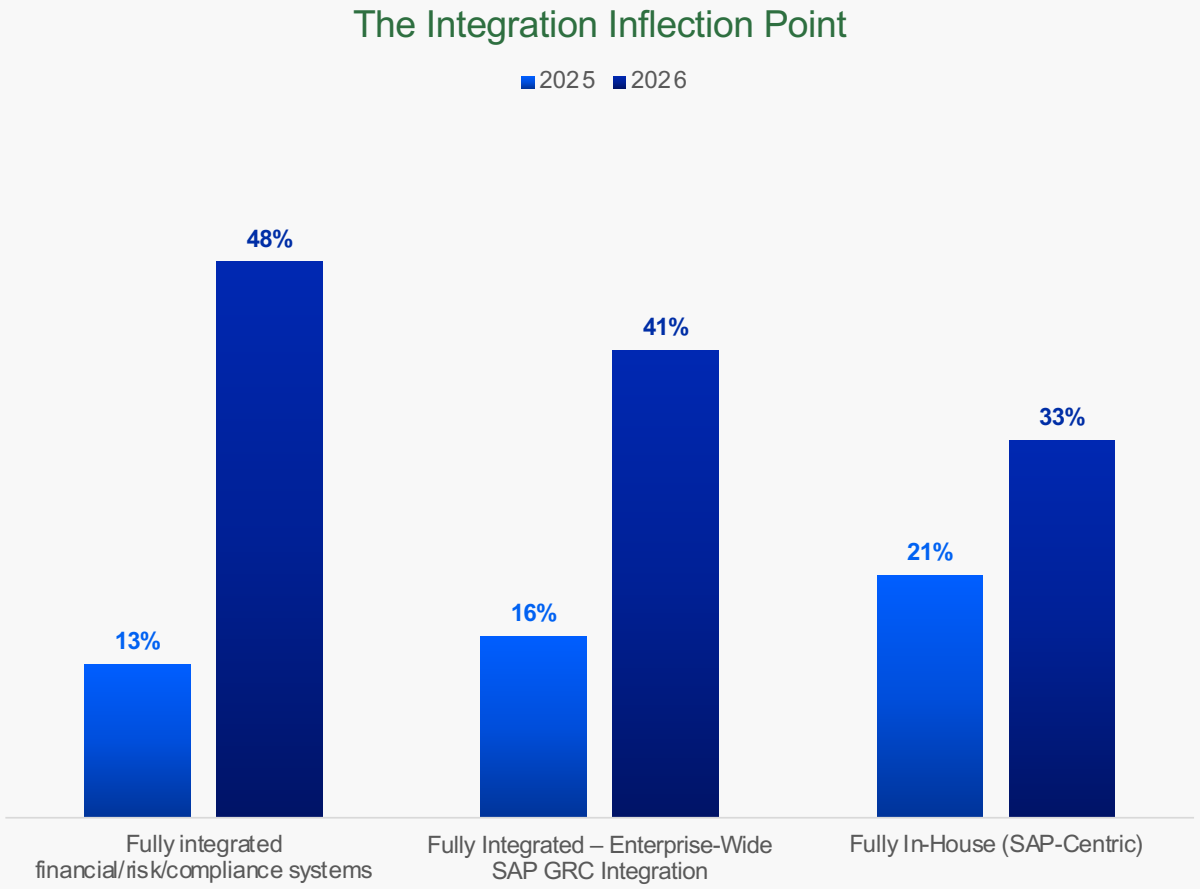
SAPinsider

4

Integrated Inflection Point

Organizations are not drifting toward integration incrementally; they are committing to it. They are also committing more decisively to one sourcing model rather than sitting in the hybrid middle.

This suggests organizations have concluded that partial integration architectures create more coordination overhead and audit exposure than they solve. Running some GRC functions in-house and others through outsourced partners, without a clear line of accountability, appears to have reached a breaking point in 2026, forcing a decision one way or the other. Customers still operating fragmented or hybrid architectures should read this as a forcing function rather than a trend to watch passively. The gap between organizations that have committed to a single operating model and those still straddling two will widen quickly, and the pilots and half-measures that were tolerable a year ago are becoming a competitive disadvantage.



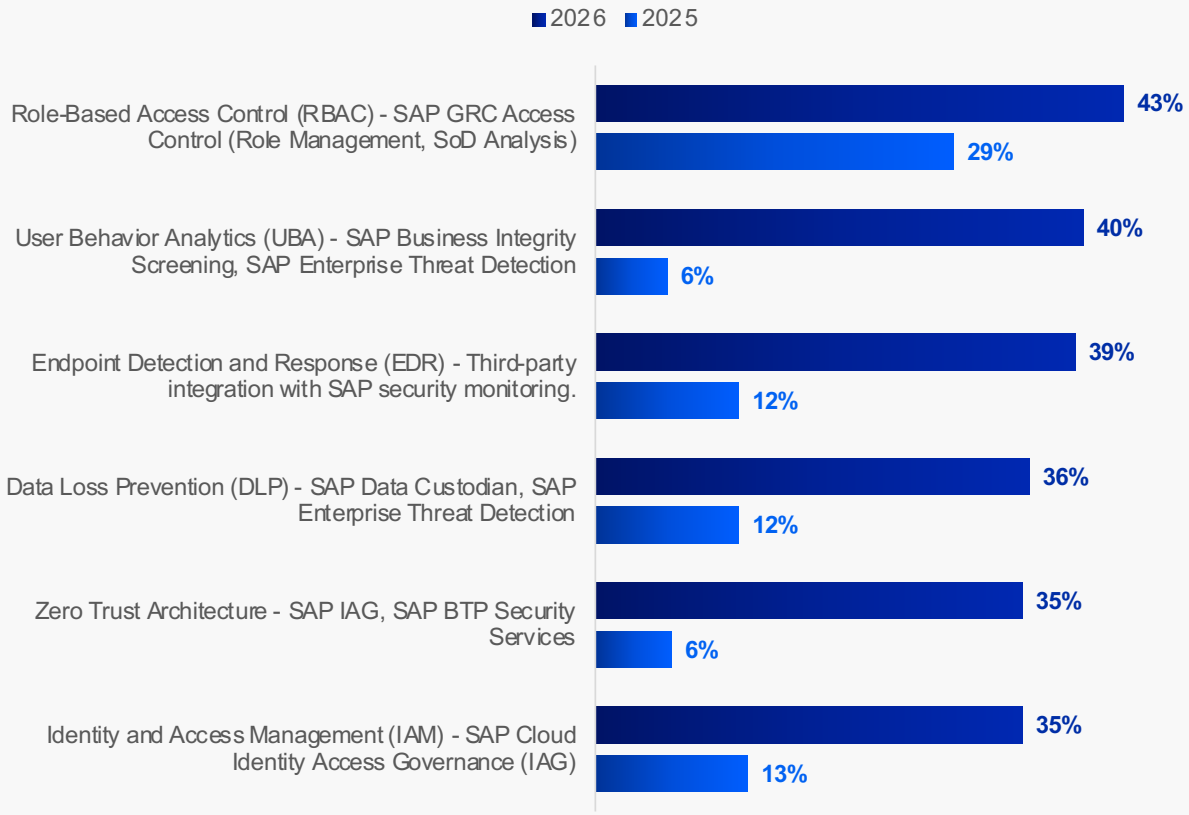
SAPinsider

5

Importance of Identity and Governance

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%, the single largest increase among all strategic actions 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.

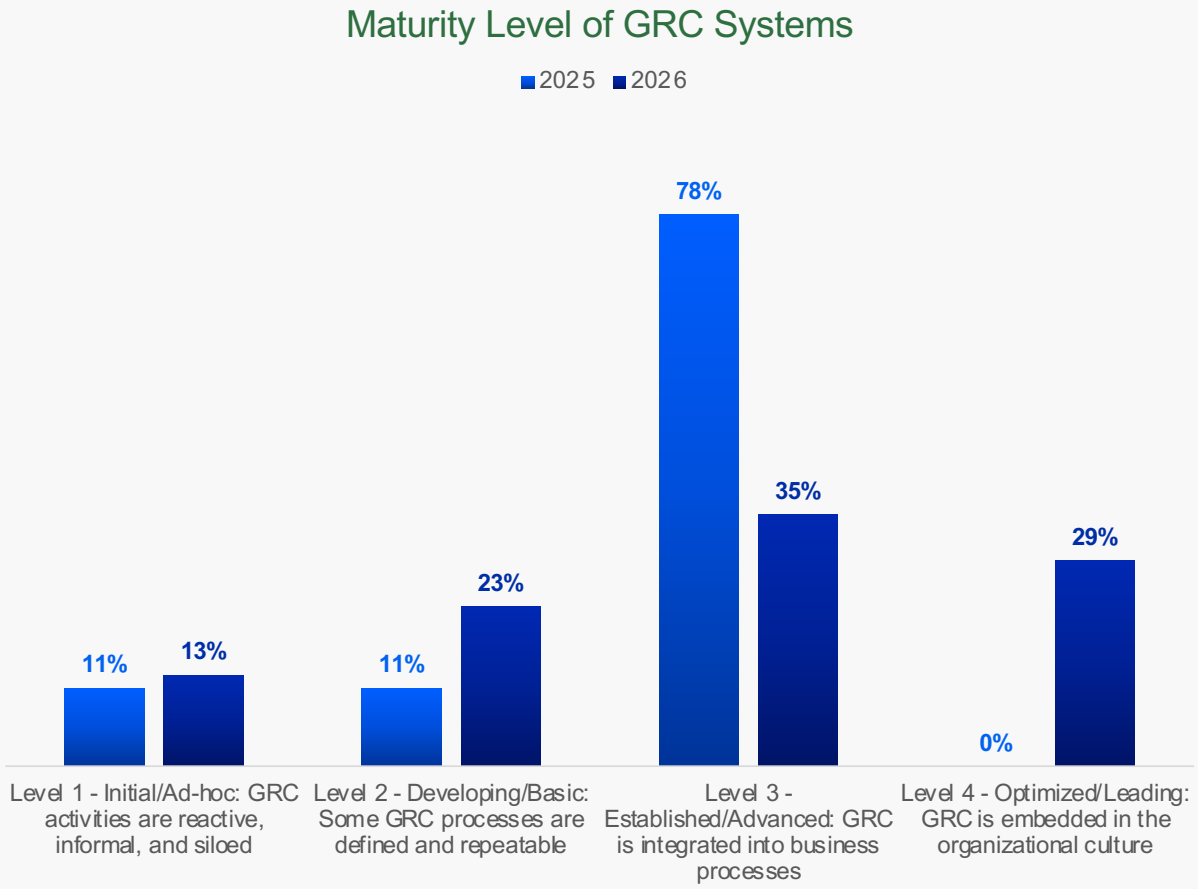
Top GRC Technologies or Frameworks Currently In Use



6

Maturity Self-Perception Recalibrates

The decrease in those reporting that they have reached an established level of maturity should not be read as a decline in actual maturity. Instead, it appears that respondent organizations are grading themselves more honestly, 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.

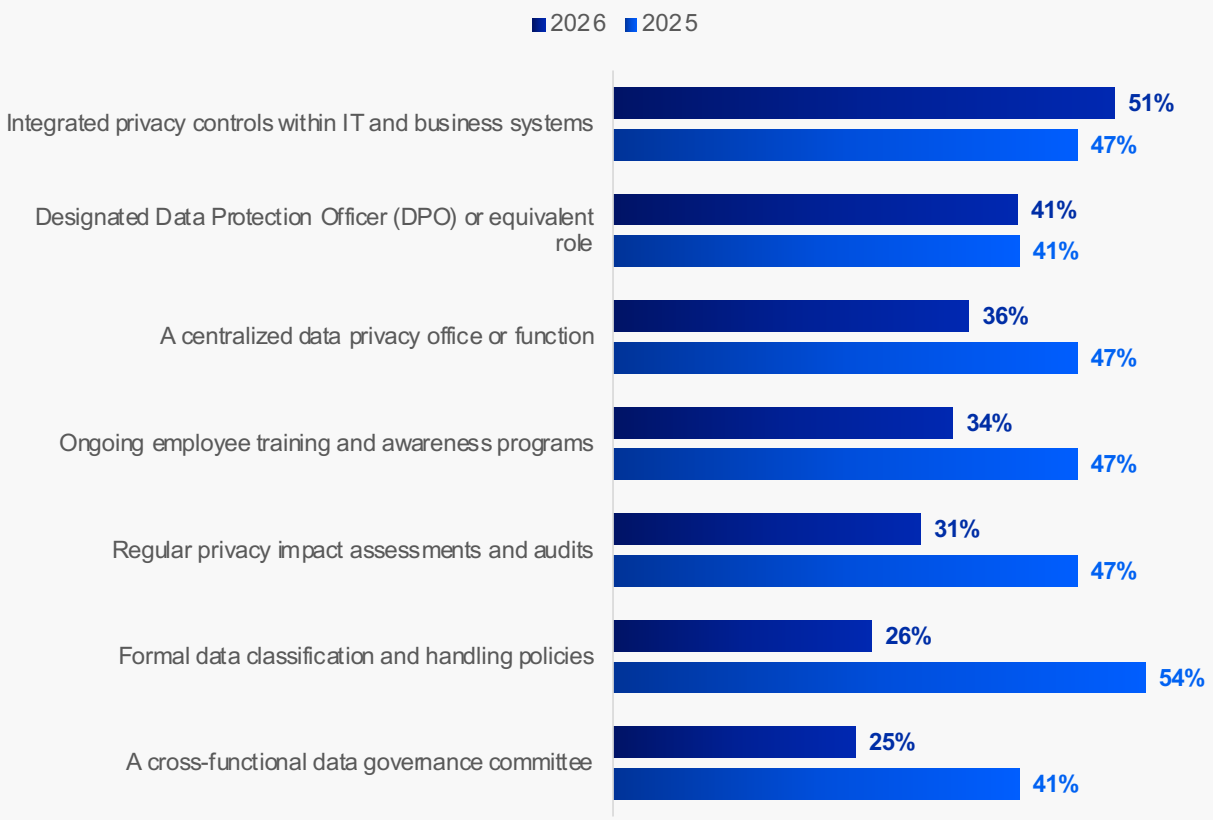


7

Solutions in Scope

Organizations are investing heavily in connecting and securing their environments, but the governance processes meant to keep those environments accountable are not being rebuilt at the same pace. Embedding privacy controls into systems is a reasonable and efficient response to resource constraints, but it is not a substitute for the formal ownership, documentation, and review cadence that auditors and regulators expect to see. For planning purposes, this means procurement and IT investment decisions in 2027 should not treat a new SAP GRC or security purchase as a completed governance action; every technology investment should carry an explicit companion commitment to rebuild or sustain the formal governance structure around it, or organizations risk discovering the gap during an audit rather than a planning cycle.

Data Privacy Governance Structures in Place



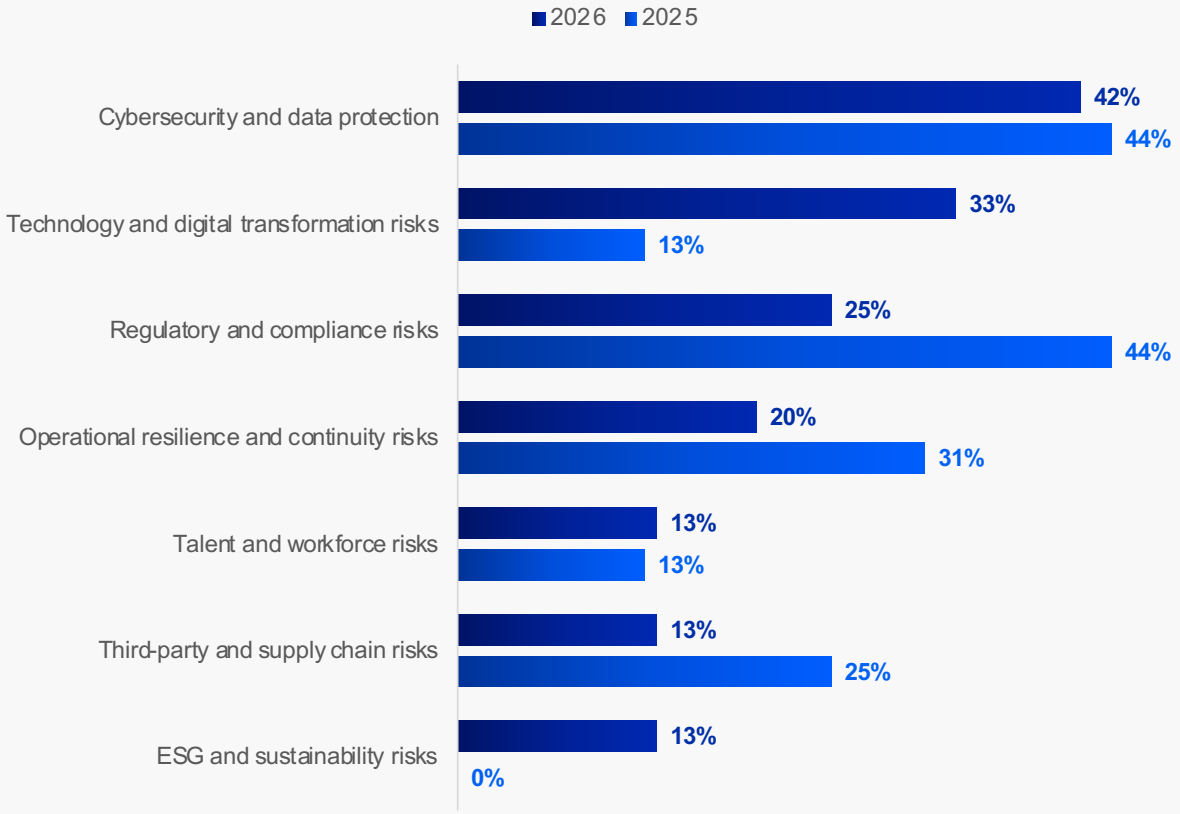
8

AI & Automation

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. 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% of organizations, 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.

Risk Areas Being Prioritized



SAPinsider

9

Business Requirements to Execute GRC Strategy

Automated and intelligent risk detection remains the dominant requirement for respondents and grew modestly this year, confirming that predictive, automated risk handling is the stable anchor capability organizations build everything else around. But the more interesting change is the trade-off between the requirement that surged, integrated identity, access, and SoD governance (14% to 40%), and the decrease in the need for centralized, validated, and accessible data across risk, compliance, and audit functions (43% to 27%). Compared with the fact that data privacy governance structures eroded and that lack of data ownership is now the top-cited data quality challenge, this decline looks less like a solved problem and more like a deprioritized one.

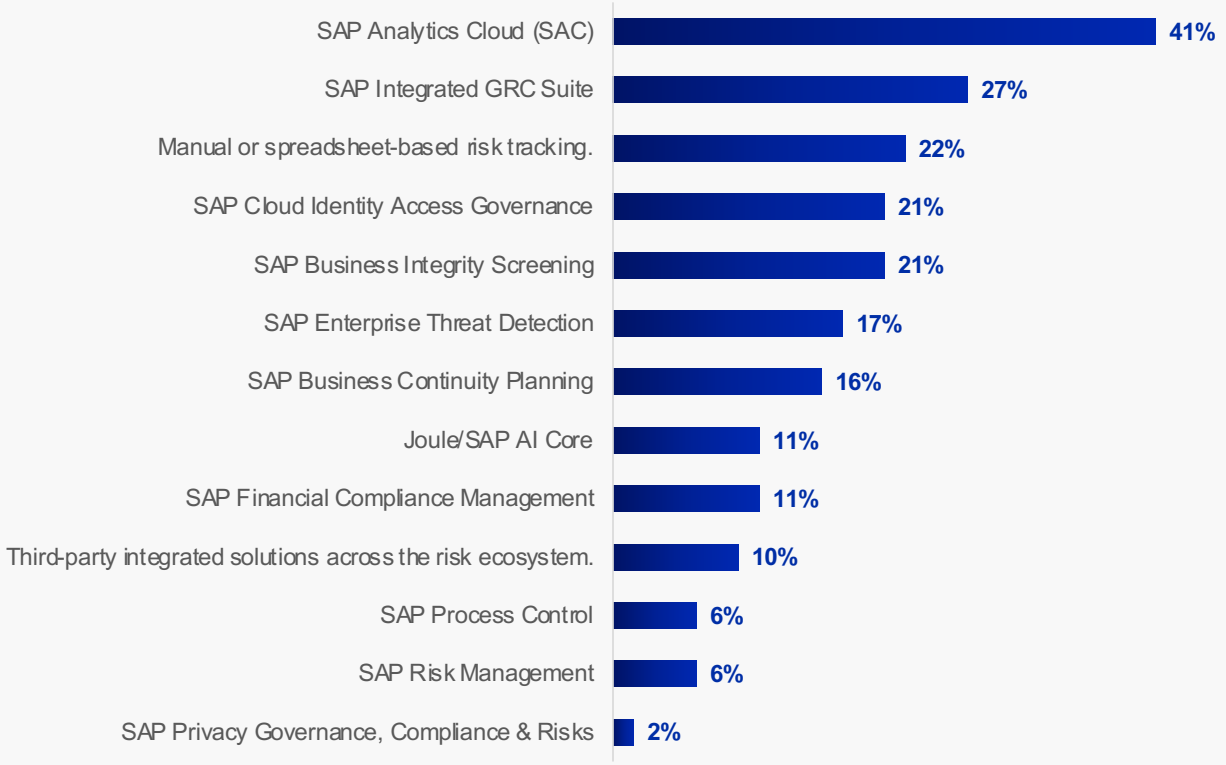
Most Important Business Requirements to Successfully Execute GRC Strategy

10

GRC Solutions

SAP Analytics Cloud leads the list of SAP solutions that are used to monitor, assess, or report on GRC or risk at 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%, 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.

SAP Solutions Used to Monitor, Assess, or Report on GRC or Risk

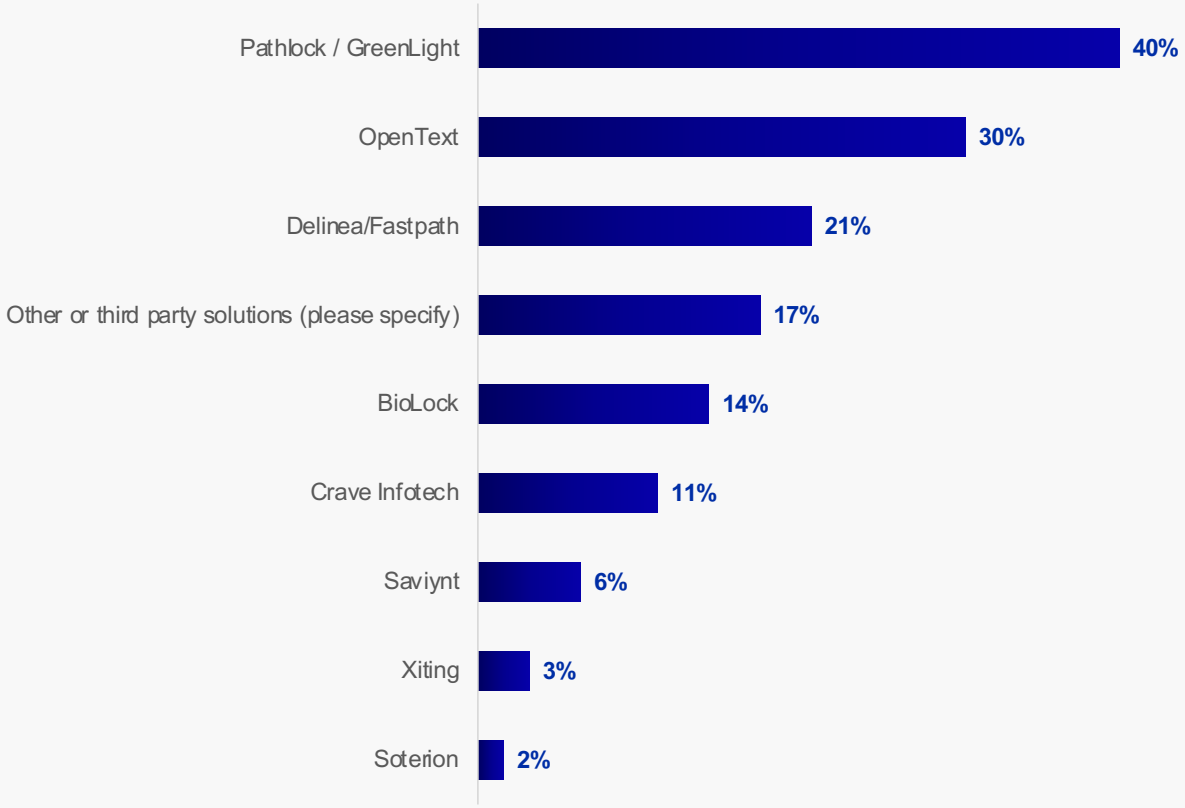


11

GRC Solutions

No single vendor commands true market dominance, and a substantial "Other" long tail (17%) alongside smaller niche players like BioLock, Crave Infotech, Xiting, and Soterion indicates the third-party market remains genuinely fragmented even as the underlying demand consolidates around a clear priority. The rapid rise in identity and access priority has not yet produced a corresponding wave of vendor consolidation or a clear market leader. Procurement and platform teams evaluating identity and access investments in 2027 should expect a genuinely competitive, fragmented selection process, and should weigh depth of SAP-native integration as heavily as brand recognition when comparing established access-governance specialists against newer identity security entrants seeking to expand from adjacent markets into the SAP ecosystem.

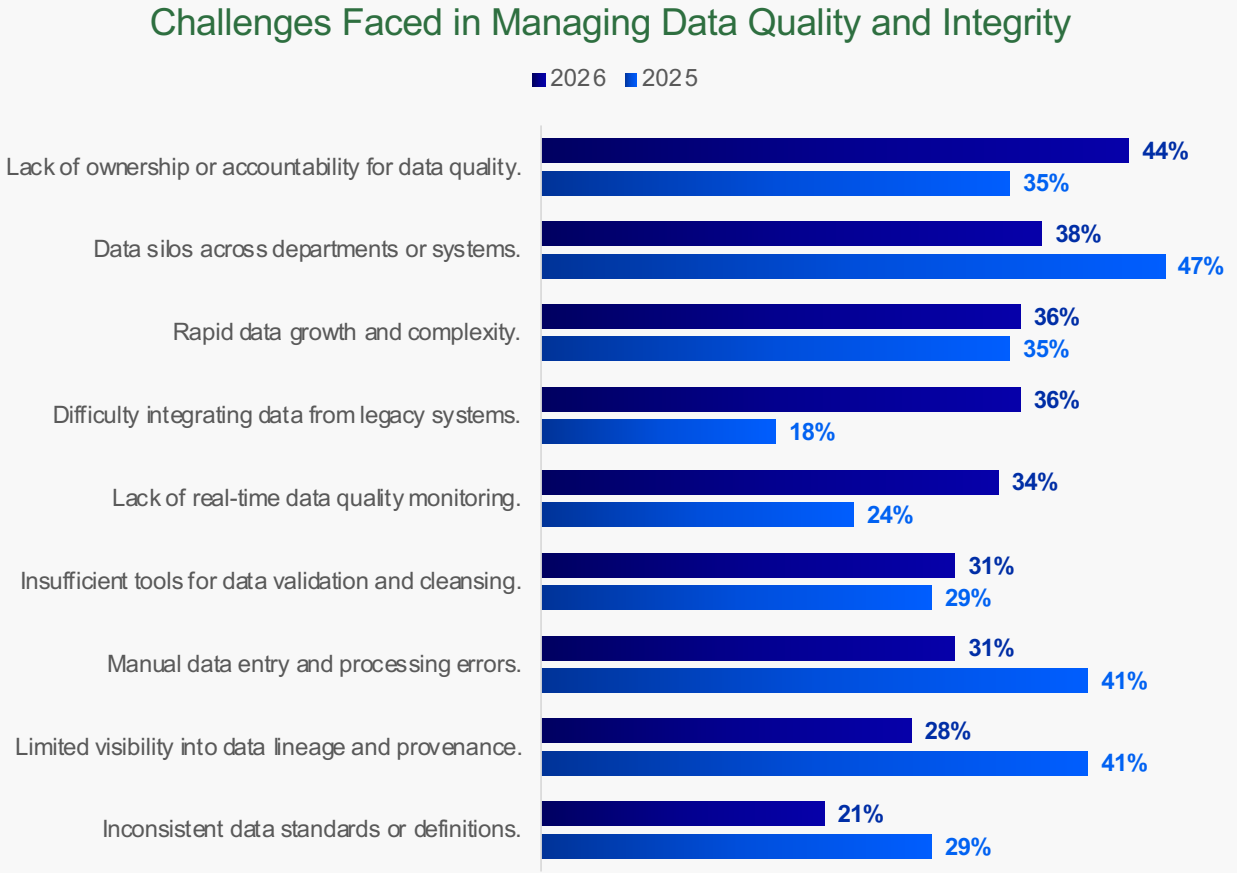
Third-Party GRC Solutions in Use



12

Data Quality and Integrity

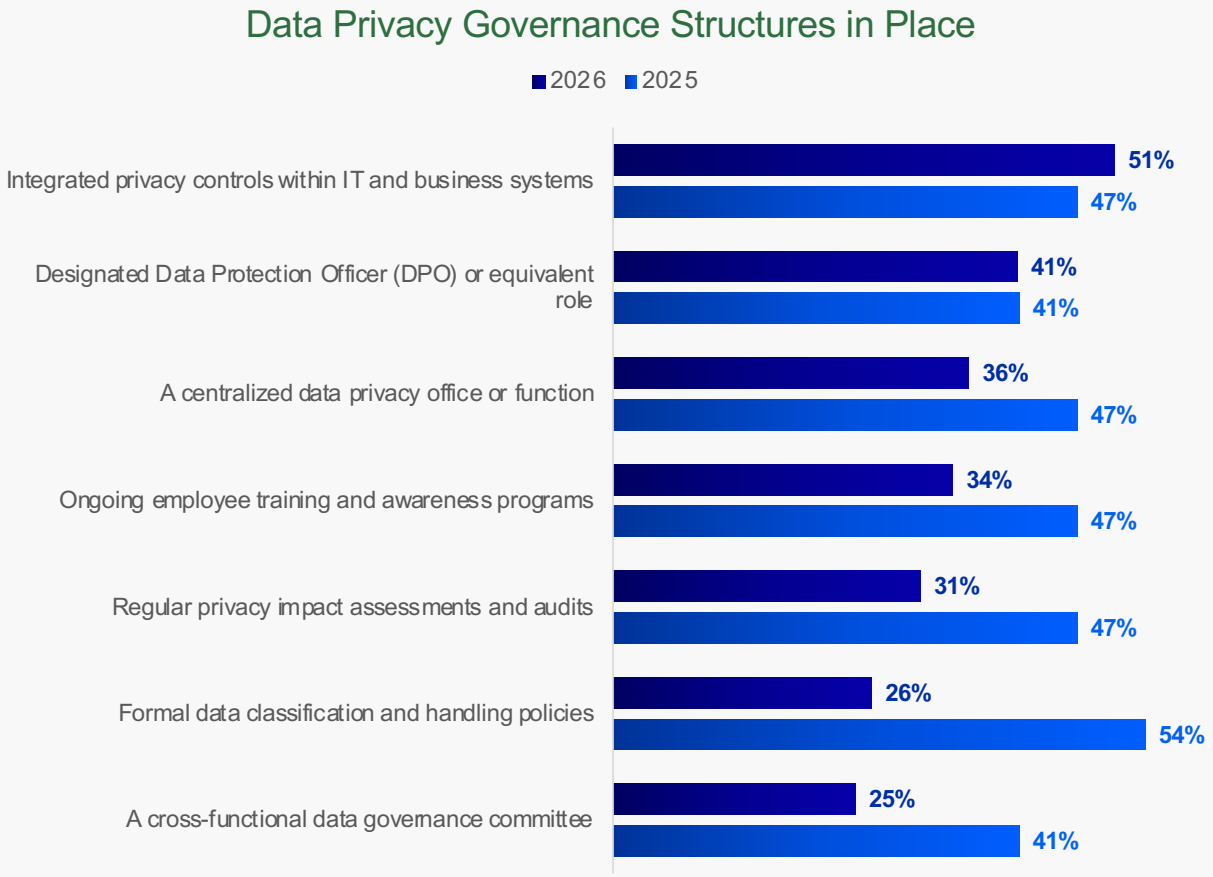
Tactical, easier-to-fix data problems are receding, while the structural, harder-to-fix ones are intensifying. Issues that respond well to better tooling and tighter integration, inconsistent data standards, manual entry errors, siloed departmental data, and limited lineage visibility, all declined meaningfully in 2026, which tracks with the integration inflection point and the surge in security and access technology adoption. Organizations that have connected their systems and modernized their controls are seeing fewer of these baseline hygiene complaints. But the challenges that developed instead are organizational rather than technical. This is demonstrated in the lack of ownership or accountability for data quality now being the single most-cited challenge. This grew just as eroding formal privacy and governance structures would predict, fewer organizations maintain the committees, assessments, and documented policies that used to assign clear ownership over data, so accountability gaps are surfacing even as the underlying pipes get better connected.



13

Data Privacy

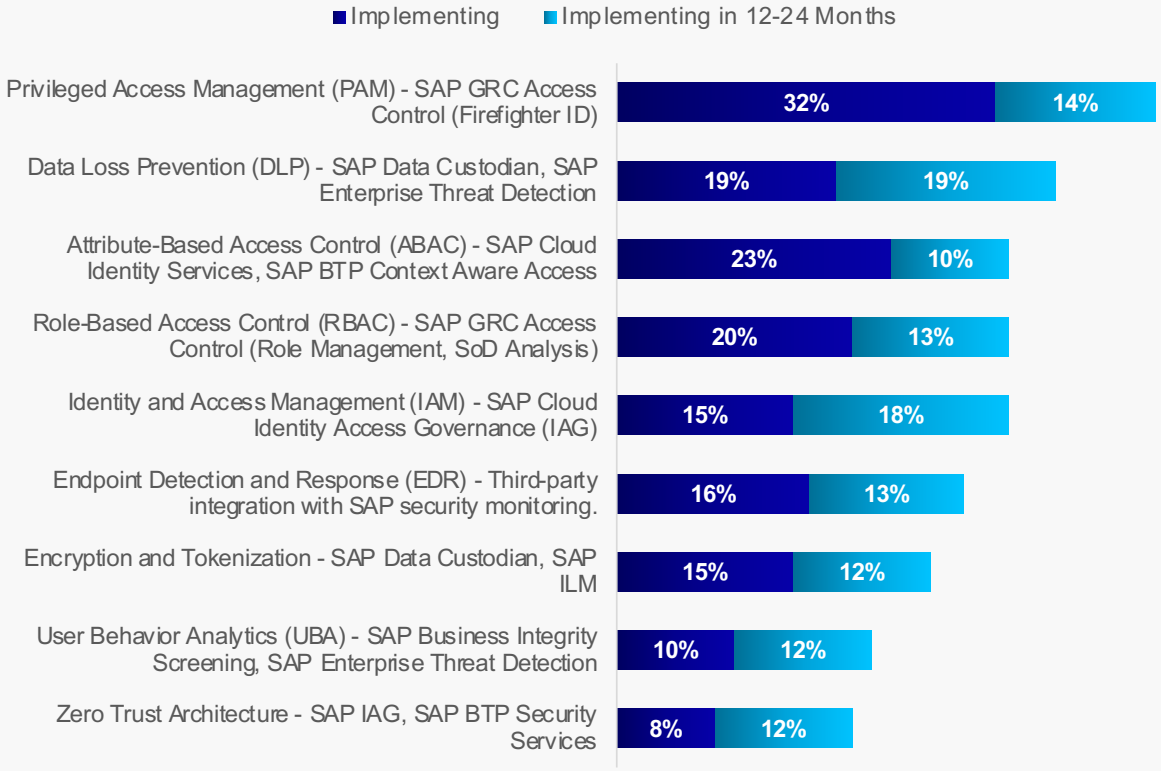
Organizations are increasingly trusting technology to carry the compliance burden that committees, policies, and training programs used to carry, and they are dismantling that human infrastructure faster than the technical layer can realistically absorb its function. However, respondent organizations are retaining the single accountable person a regulation may require while quietly removing the cross-functional committee, the classification policies, the impact assessments, and the training programs that person previously depended on for support, escalation, and audit trail. As organizations accelerate platform modernization and lean on embedded technical controls, they are simultaneously removing the formal oversight mechanisms that would normally catch a privacy gap before it becomes a regulatory finding. This means the risk is not that privacy compliance fails today, but that it fails silently during the next transformation event, with no committee, policy, or audit process left standing to catch it in time.



GRC Technologies

The technology adoption surge is still in its early phases rather than approaching a plateau, and it resolves an apparent contradiction in the current use figures. Privileged Access Management showed the only decline in current usage among the access and security categories, but it also carries the single largest active implementation share of any technology in this dataset, which strongly suggests that dip was not abandonment but organizations actively replacing or upgrading their PAM capability rather than walking away from it. In addition, this year's budget increases are being deployed as a broad, simultaneous build-out across the entire identity and access technology stack rather than a narrow bet on one or two tools, and organizations that have not yet begun implementing multiple categories in parallel should expect to fall further behind a peer group that is already executing on a multi-year roadmap, not just a single-year initiative.

Technologies or Frameworks Being Implemented to Protect Data, Govern Access, and Minimize Insider Threats

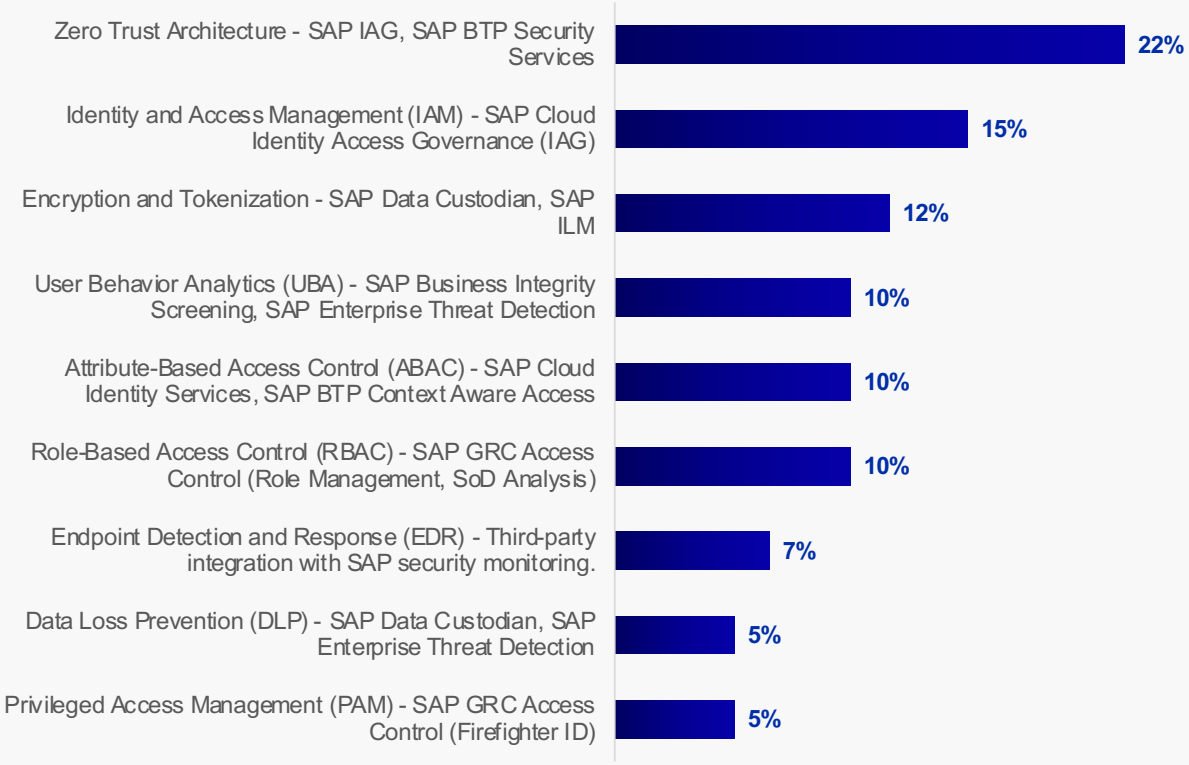


GRC Technologies

Zero Trust Architecture is transitioning from a niche architectural concept into the default reference model that other categories are increasingly being built underneath. This means conversations inside SAP customer organizations are shifting from whether to adopt a Zero Trust posture to how quickly they can operationalize one. Identity and Access Management shows a similar pattern with 15% evaluating on top of its own deep pipeline, reinforcing that identity remains the strategic center of gravity for this entire technology wave.

Zero Trust and identity management represent the technologies still being actively shaped and decided across the SAP customer base, making the next 12 to 24 months a critical window for vendors and internal architects to influence how those frameworks get defined, while PAM and DLP should be treated as a largely settled market where the remaining opportunity lies in deepening existing deployments rather than winning new evaluations.

Technologies or Frameworks Being Evaluated to Protect Data, Govern Access, and Minimize Insider Threats



DART
MODEL FRAMEWORK

GRC and Risk Intelligence for SAP

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%)

THANK YOU

Robert Holland
Chief Research Officer
robert.holland@sapinsider.org

SAP insider.org
PO Box 982Hampstead, NH 03841