IDC MarketScape

IDC MarketScape: Worldwide Enterprise Governance, Risk, and Compliance Services 2025–2026 Vendor Assessment

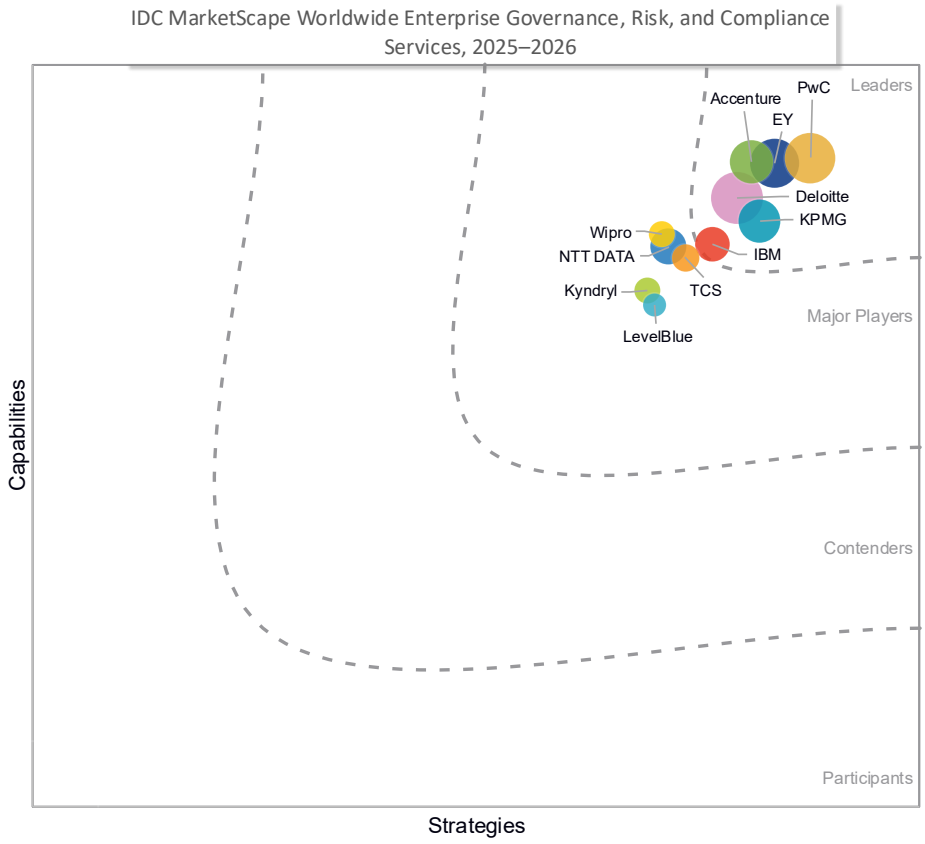
Bill Latshaw

THIS EXCERPT FEATURES PWC AS A LEADER

IDC MARKETSCAPE FIGURE

FIGURE 1

IDC MarketScape Worldwide Enterprise Governance, Risk, and Compliance Services Vendor Assessment



Source: IDC, 2025

December 2025, IDC #US53683125e

Please see the Appendix for detailed methodology, market definition, and scoring criteria.

ABOUT THIS EXCERPT

The content for this excerpt was taken directly from IDC MarketScape: Worldwide Enterprise Governance, Risk, and Compliance Services 2025–2026 Vendor Assessment (Doc # US53683125).

IDC OPINION

This IDC MarketScape examines the evolution of enterprise governance, risk, and compliance (GRC) as organizations recalibrate from static control functions to an agile, business-run operating model for resilience. Resilience is no longer synonymous with basic backup and business continuity; it includes the enterprise's ability to anticipate, absorb, and adapt to disruption, with cybersecurity now sitting at the center of that mission. Modern resilience must be holistic and continuous, cutting across the value chain and being powered by integrated security practices rather than siloed efforts. For technology buyers, that means aligning people, processes, data, and platforms with a common GRC operating model that supports rapid decision-making, transparent accountability, and trusted reporting. The IDC MarketScape that follows was designed to support your decision when choosing a provider that suits your needs and context.

The threat landscape reinforces this shift. Publicly disclosed software vulnerabilities have climbed steadily, with 2025 setting a new high, expanding the attack surface faster than many organizations can patch. Data exposure has been the leading breach outcome, with billions of records affected. Companies cite breach tactics, malicious hacking, supply chain compromise, and ransomware as underscoring the need for data-centric controls and integrated defenses. Breach costs vary widely by region but remain important to organizations everywhere. The takeaway for buyers is that resilience by design that runs on tightly integrated systems, secure dataflows, and unified oversight can reduce exposure and improve planning confidence.

Common buyer concerns center on operating model maturity and tool fragmentation. A resilient GRC function requires a clear taxonomy, harmonized policies and controls, and the three lines of defense based on shared data and consistent methods. Robust frameworks for corporate governance, enterprise risk management, and compliance that are supported by cross-cutting enablers in technology, data, organization design, and culture can provide scale and auditability. Buyers are pressing for platform-enabled GRC so that policy, risk, control testing, and reporting operate as one system of work, augmented by analytics and automation to reduce manual effort and cycle times.

Integrated GRC frameworks that prioritize common language, unified data models, and process automation are emerging as best practice foundations for durable change.

Looking ahead, we expect enterprise GRC to converge with cyber-resilience as a single, programmatic capability. Buyers should plan for an integrated, platform-first approach that unifies preparation, detection/response, and recovery with a single command-and-control view, enabled by the adoption of zero trust principles, strong encryption, and immutable backup. At the same time, being able to codify incident response and crisis communications so the organization can restore a minimum viable company quickly and emerge stronger is vital.

AI will be a force multiplier relying on machine learning to accelerate analysis, generative AI to recommend remediation, and agentic AI to automate routine tasks. IT also requires the talent to manage and introduce governance duties around privacy, provenance, explainability, and regulatory compliance. Board-level accountability will deepen with CEOs, CISOs/CIOs, CROs, and CFOs being jointly responsible for continuity targets and recovery timelines. The future state for GRC is continuous, data-driven, AI-enabled, and designed to be inseparable from how the business operates.

IDC MARKETSCAPE VENDOR INCLUSION CRITERIA

Using the IDC MarketScape model, IDC studied vendors that provide enterprise GRC services around the world. The vendors included in the study had to meet certain criteria to qualify for this vendor assessment:

- **Geographic presence:** Each vendor is required to operate GRCs or strategize on their design in more than one region.
- **Sales presence:** Each vendor has a sales force across one or more regions.
- **Customer base:** Each vendor has 100+ customers.
- **GRCS capability:** Each vendor possesses a GRC service that has trained professional enterprise GRC staff with expertise in governance, risk management, compliance, and cybersecurity.

ADVICE FOR TECHNOLOGY BUYERS

Anchor your enterprise GRC road map in an integrated resilience operating model. Unify preparation, detection/response, and recovery in a platform-first architecture with a single command-and-control view so teams can act swiftly and coherently when disruption hits. Align people, processes, and controls to that flow. Start with data and critical assets: Inventory and classify, enforce least-privilege access with MFA, apply encryption, and maintain immutable backups. Extend zero trust across your network

and cloud and continuously model threats and remediate vulnerabilities, an imperative as publicly disclosed CVEs keep climbing.

Operationalize AI with guardrails. Use machine learning and generative and agentic AI to accelerate analysis, reduce toil, and recommend remediation while instituting policies for privacy, provenance, explainability, and compliance. Build outcome metrics so you can prove value and course-correct. Make resilience a C-suite program by setting explicit continuity targets and decision rights, rehearsing crisis communications, and planning to restore a minimum viable company quickly after an incident.

Close structural risk gaps with automation and integration. Most breaches involve data exposure, and time to detect and contain remains high; instrument telemetry, automate evidence collection and response, and address third-party exposure as a first-order risk. Finally, measure what you manage by adopting resilience-by-design patterns that reduce data exposure and integrate systems across lines of business so leaders can trust the data they plan with and communicate confidently to stakeholders.

VENDOR SUMMARY PROFILE

This section briefly explains IDC's key observations resulting in a vendor's position in the IDC MarketScape. While every vendor is evaluated against each of the criteria outlined in the Appendix, the description here provides a summary of each vendor's strengths and challenges.

PwC

According to IDC analysis and buyer perception, PwC is positioned in the Leaders category in this 2025–2026 IDC MarketScape for worldwide enterprise governance, risk, and compliance services vendor assessment.

PwC positions enterprise GRC as both a transformation and an operational play by combining strategy and regulatory advisory to determine the best way forward. From there, designs move into solution build and platform implementation, standing up enabled AI-enabled workflows, testing cadence, and reporting. When ongoing support is needed, PwC provides managed services for regulatory testing and monitoring, policy compliance, risk and issue management, and reporting, delivered as a co-source or fully operated models. That means a single team can help redesign risk governance and provide the people, AL-enabled GRC tooling, and SLAs to keep controls moving while change is made concrete.

PwC offers operational, regulatory, and policy/control compliance testing with defined methodologies, workpapers, and cadence, plus enterprise testing managed services to standardize AI-enabled GRC tooling, evidence, and throughput across business and IT

change. Those capabilities sit next to broader cyber, risk, and regulatory consulting that connects operational security, business, and compliance risks. This helps clients stabilize control execution while larger design work proceeds, creating a more horizontal view of risk across the organization.

PwC's enterprise GRC offerings are organized around AI-based offerings Advise, Solution, and Operate, which bring together strategy, engineering, operations, and managed services to help clients manage enterprise risks, navigate complex regulations, and build resilient control environments that are tech forward and AI enabled. PwC's AI-enabled IRM approach uses advanced analytics and machine learning to support forward-looking risk signals and decisions.

PwC's GRC offering is built for a blend of execution and change. It is designed to scale and provide repeatability in control operations, helping organizations that have chronic capacity gaps or a fragmented control environment and documentation. The firm's managed services operate alongside its advisory teams, making handoffs lighter, which can enable accelerated time to steady state control performance.

Strengths

PwC positions enterprise GRC as an integrated risk management (IRM) program that connects people, process, data, and technology around a common operating model with shared taxonomies and architecture. By doing so, governance becomes the framework through which the business operates. It helps clients envision, launch, and optimize IRM while standardizing policy, controls, and reporting. PwC also brings platform enablement, configuring enterprise GRC and model-risk solutions on Archer, MetricStream, ServiceNow, and other ecosystems. For buyers focused on outcomes, PwC can operate GRC as a managed service — governing policies and procedures, managing multi-framework control sets, and producing executive-grade metrics and evidence. Acceleration tools such as Risk Link (integrated risk intelligence) and Third Party Tracker help connect regulations to controls and streamline third-party oversight. PwC's resilience practice integrates business continuity, incident response, and cyber/operational resilience into an end-to-end program.

Challenges

PwC underscores the reality for technology buyers regarding the continuously shifting risk and regulatory landscape and the need for controls to be mapped across multiple frameworks and jurisdictions while remaining auditable and efficient. Many organizations still run fragmented risk processes and tools, making it hard to align policy, controls, and evidence to a common taxonomy and single operating model. Third-party risk is intensifying as regimes such as DORA raise the bar for ongoing monitoring and contract governance across extended supplier networks. PwC sees AI-

driven innovation demand governance for model risk, data quality, privacy, and responsible AI practices with roles, standards, inventories, and monitoring included. PwC's approach may be somewhat method-heavy for smaller clients, but they partner well with them to meet this need.

Consider PwC When

PwC is a good choice for companies that want to stand up or modernize an integrated GRC/IRM program by defining a target operating model, harmonizing taxonomies and processes, and implementing the technology to make it real. It is suitable for organizations that prefer outcomes and ongoing capacity via managed services that run risk, compliance, internal audit, and cyberoperations with repeatable, scalable playbooks and reporting. If third-party risk is central, whether to meet DORA or to industrialize onboarding, due diligence, and continuous monitoring due to an organization's need for TPRM services and products to accelerate the journey, PwC meets this need. PwC's focus on AI is helpful to organizations with AI on their road maps and is a good choice where resilience is a priority and an organization aims to integrate business continuity, incident management, and operational resilience into a cohesive enterprise program.

APPENDIX

Reading an IDC MarketScape Graph

For the purposes of this analysis, IDC divided potential key measures for success into two primary categories: capabilities and strategies. Based on the importance of making enterprise GRC actionable, capabilities were weighted at 60%, with strategy at 40%.

Positioning on the y-axis reflects the vendor's current capabilities and menu of services and how well aligned the vendor is to customer needs. The capabilities category focuses on the capabilities of the company and product today, here and now. Under this category, IDC analysts will look at how well a vendor is building/delivering capabilities that enable it to execute its chosen strategy in the market.

Positioning on the x-axis, or strategies axis, indicates how well the vendor's future strategy aligns with what customers will require in three to five years. The strategies category focuses on high-level decisions and underlying assumptions about offerings, customer segments, and business and go-to-market plans for the next three to five years.

The size of the individual vendor markers in the IDC MarketScape represents the estimated market share of each individual vendor within the specific market segment being assessed. The IDC MarketScape research for worldwide GRC was performed at

the same time as the cybersecurity GRC studies. While there is overlap in these IDC MarketScape documents, our sizing was specific to the respective segment within the overall GRC services market.

IDC MarketScape Methodology

IDC MarketScape criteria selection, weightings, and vendor scores represent well-researched IDC judgment about the market and specific vendors. IDC analysts tailor the range of standard characteristics by which vendors are measured through structured discussions, surveys, and interviews with market leaders, participants, and end users. Market weightings are based on user interviews, buyer surveys, and the input of IDC experts in each market. IDC analysts base individual vendor scores, and ultimately vendor positions on the IDC MarketScape, on detailed surveys and interviews with the vendors, publicly available information, and end-user experiences in an effort to provide an accurate and consistent assessment of each vendor's characteristics, behavior, and capability.

Market Definition

The IDC enterprise GRC services market helps organizations develop a strategic approach to prioritizing and managing business and/or cyberthreats to an organization. A GRC program is created to ensure the most critical business and/or cyberthreats are handled in a timely manner. Organizations must establish and implement a GRC program to identify, categorize, prioritize, and mitigate risks specific to their business and to eliminate or reduce the risk of business disruptions and/or cyberattack threats based on the potential impact each threat poses.

A GRC program can:

- Assist decision-makers with the threats and exposures associated with people, process, and technology on a day-to-day operational level.
- Assist the business with establishing the likelihood and potential impact of any business disruption and/or cyberattack.
- Assist the business with evaluating and prioritizing any financial budget impacts and ensure money, time, and resources are expended in the right places.
- Assist in preventing or reducing the impact of risks identified in assessments.

According to OCEG, "Governance, risk, and compliance (GRC) is the integrated collection of capabilities that enable an organization to reliably achieve (business) objectives (governance) while addressing uncertainty (risk management) and acting with integrity (compliance). It encompasses governance, assurance, and management of performance, risk, and compliance."

IDC's enterprise governance, risk, and compliance market relates to the governance, risk, and compliance definition mentioned previously. GRC is inclusive of services and software that assist organizations with tasks and initiatives to:

- Enhance performance, create greater efficiencies, and reduce risk.
- Establish and monitor enterprise and IT governance, programs that address several types of risk management and mitigation, and compliance with global laws and regulations, industry standards, and company policies.
- Aggregate the tools required to help an enterprise identify, track, and analyze enterprise, business, and technology risks and monitor and manage corporate and IT governance and compliance.

As organizations handle, collect, analyze, or share any personal data, there is an awareness of the challenges facing the privacy and security of that data. Services to aid and guide organizations concerned with the privacy of their data and the threat of cyberattacks and to deal with the growing number of privacy-focused regulations are imperative. Technology suppliers and service providers have unique visibility and trust with enterprise clients to develop collaboration across departments and roles to ensure risk and compliance efforts are focused on common enterprise goals, provide a common language as a baseline for communicating these goals, and minimize redundant work efforts.

The enterprise and cyberGRC market is a functional market within IDC's broader software taxonomy and includes the following segments:

- **Governance:** Corporate governance management applications support corporate board members, C-suite executive teams, and second-line-of-defense professionals in defining and implementing corporate policies. This segment includes applications for policy management and compliance management.
- **Risk management:** Risk management applications assist in identifying, analyzing, monitoring, and managing all types of risks threatening an organization, including IT risk, compliance risk, security risk, and third-party risk.
- **Compliance:** Compliance management addresses the adherence to all necessary regulatory and legal requirements in addition to managing any changes to the regulatory environment and their impact on the enterprise. This segment includes regulatory compliance management and regulatory change management.
- **Audit and regulatory management:** Audit management solutions provide the ability to help organizations plan, manage, and analyze processes (manual and automated). Numerous types of audits must be managed within an organization, including compliance audits, IT audits, security audits, and third-party audits

- **Business resiliency/continuity/recovery:** Business resiliency/continuity/recovery solutions identify exposure to internal and external threats and quickly adapt to disruptions while maintaining continuous business operations and safeguarding people, assets, and overall brand equity. They effectively deal with disruptive and unexpected events that threaten to harm the organization or its stakeholders. These solutions establish capabilities to enable the recovery or continuation of vital technology infrastructure and systems following a natural or human-induced disaster.
- **Geography:** These solutions establish capabilities to enable the recovery or continuation of vital technology infrastructure.

LEARN MORE

Related Research

- *Market Analysis Perspective: Worldwide and U.S. Business Consulting Services 2025* (IDC #US52405725, September 2025)
- *IDC MarketScape: Worldwide Enterprise Strategy Consulting Services 2025 Vendor Assessment* (IDC #US52035225, September 2025)
- *Worldwide and U.S. Business Consulting Services Forecast, 2025–2029* (IDC #US52964225, June 2025)
- *Worldwide Business Consulting Services Global Client Value Survey 2025* (IDC #US52964525, May 2025)
- *The Future of Business Consulting Services in an Agentic AI World* (IDC #US52405625, May 2025)
- *IDC Innovators: Business Consulting Services in the United States, 2025* (IDC #US53309225, April 2025)
- *What Is Work Today — And When Will We Stop Needing Humans to Do It?* (IDC #US51072724, March 2025)

Synopsis

This IDC study highlights the shift from static GRC controls to agile, integrated, and AI-enabled operating models. It evaluates vendors on their ability to deliver holistic resilience, unify risk and compliance, and leverage automation and analytics, guiding organizations to select partners that support rapid decision-making, transparency, and trusted reporting in a dynamic threat landscape.

"In a world where disruption is constant and cyberthreats multiply, organizations cannot remain reactive. Companies must make the choice to transform their enterprise GRC into a unified, AI-driven force for resilience, rapid decision-making, and trusted

accountability across their lines of business. The ever-changing and confused future demands nothing less." — Bill Latshaw, research director, Worldwide Business Consulting Services at IDC

ABOUT IDC

International Data Corporation (IDC) is the premier global provider of market intelligence, advisory services, and events for the information technology, telecommunications, and consumer technology markets. With more than 1,300 analysts worldwide, IDC offers global, regional, and local expertise on technology, IT benchmarking and sourcing, and industry opportunities and trends in over 110 countries. IDC's analysis and insight helps IT professionals, business executives, and the investment community to make fact-based technology decisions and to achieve their key business objectives. Founded in 1964, IDC is a wholly owned subsidiary of International Data Group (IDG, Inc.).

Global Headquarters

140 Kendrick Street
Building B
Needham, MA 02494
USA
508.872.8200
Twitter: @IDC
blogs.idc.com
www.idc.com

Copyright and Trademark Notice

This IDC research document was published as part of an IDC continuous intelligence service, providing written research, analyst interactions, and web conference and conference event proceedings. Visit www.idc.com to learn more about IDC subscription and consulting services. To view a list of IDC offices worldwide, visit www.idc.com/about/worldwideoffices. Please contact IDC at customerservice@idc.com for information on additional copies, web rights, or applying the price of this document toward the purchase of an IDC service.

Copyright 2025 IDC. Reproduction is forbidden unless authorized. All rights reserved.