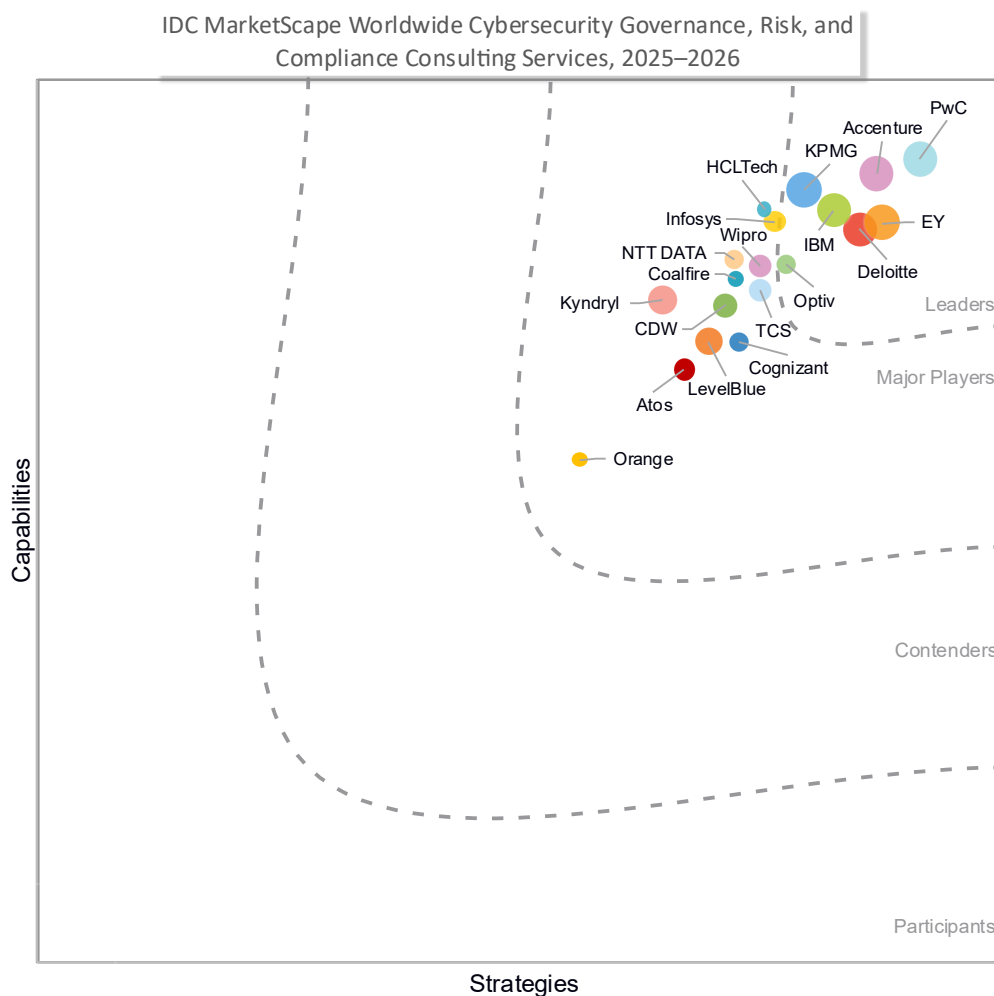


IDC MarketScape: Worldwide Cybersecurity Governance, Risk, and Compliance Consulting Services 2025–2026 Vendor Assessment

Philip D. Harris, CISSP, CCSK
THIS EXCERPT FEATURES EY

IDC MARKETSCAPE FIGURE

Figure 1: IDC MarketScape: Worldwide Cybersecurity Governance, Risk, and Compliance Consulting Services Vendor Assessment



Source: IDC, 2025

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 Cybersecurity Governance, Risk, and Compliance Consulting Services 2025–2026 Vendor Assessment (Doc # US53936925).

IDC OPINION

Cybersecurity risk and compliance leaders must often resolve a myriad of known issues, such as bad audits, breaches, increased quantity and sophistication of cyberattacks, and well-meaning but often erroneous guidance from the board or senior management. Equally bad is the problem of not knowing what you do not know. A qualified cybersecurity governance, risk, and compliance (GRC) service provider can be instrumental in helping an organization identify the source of problems or challenges, define it in meaningful terms that align with the business and overall corporate needs, and establish a plan of action in the form of a road map to address it.

A cybersecurity GRC program enables a strategic approach to understanding the risk profile of an organization and managing risk and compliance effectively. It helps organizations:

- Conduct ongoing risk modeling exercises with management, both business and operational, to identify relevant threats to the organization and associated risks (known as the risk profile)
- Establish cybersecurity policies that effectively address the risk profile of the organization
- Prioritize and manage threats associated with the risk profile through policies
- Establish a blueprint and road map to identify and implement staffing, processes, and technical solutions that contribute to overall risk and compliance management
- Conduct risk assessment to ferret out hidden or unknown risks and conduct compliance assessments that ensure compliance with cybersecurity policies, regulations, industry standards, and cybersecurity frameworks

Cybersecurity GRC programs are primarily created to ensure that businesses can address critical threats in a timely manner. These programs also enable organizations to identify, categorize, prioritize, and mitigate risks and compliance issues specific to their business as well as to eliminate or reduce the risk of cyberattack threats based on their potential impact. These steps, if performed consistently and effectively, significantly increase the resilience of the business.

A cybersecurity GRC program can:

- Aid in developing effective cybersecurity policies and procedures
- Create executive, managerial, and operational reports that directly reflect the state of risk and compliance for the organization
- Assist decision-makers in identifying and tracking 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 cyberattack
- Assist the business with evaluating and prioritizing financial 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
- By infusing AI within GRC tools, an organization can enhance both productivity and outcomes, thereby increasing the ROI of the overall GRC program.

Organizations that lack adequate cybersecurity and corporate policies and visibility into cybersecurity risks and compliance issues within their IT estates are potentially unprepared; any type of attack could cause damage, disruption, and unauthorized access, which all impact reputation, brand, confidence from the board of directors as well as customers, and data. Implementing a cybersecurity GRC program will empower an organization to establish adequate cybersecurity and corporate policies. It also helps the business discover, anticipate, balance, monitor/track, and mitigate risks and compliance issues. Cybersecurity GRC service providers can be a catalyst for many organizations to begin the journey of creating and/or elevating such a program.

Before engaging with a cybersecurity GRC service provider, organizations should first determine their needs. For instance, decision-makers should consider the following questions:

- Do I need help documenting the right set of cybersecurity policies?
- Are these cybersecurity policies based upon a published cybersecurity framework?
- Do I need help to review my corporate policies to ensure these reflect all regulatory requirements my company is subject to?
- Is my organization compliant with all relevant cybersecurity regulations across various regions, countries, states, and/or provinces?
- Are there any other types of corporate requirements that must be applied to these policies?
- Do I want to build and run this program myself? Do I want a service provider to build the program and then I run it?

- Do I want a service provider to build and run the cybersecurity GRC program for me?
- Do I need as much automation as possible — is machine learning (ML), artificial intelligence (AI), and workflow management critical to my success?

Whether you are a cybersecurity GRC service provider that engages with organizations to create and implement a program or are hired to manage and execute it, utilizing a sound framework will be necessary to achieve a clear picture of cybersecurity risks and what is needed to remediate them. The benefits of establishing a cybersecurity GRC program include:

- Enabling an organization to constantly review, update, and approve policies
- Enabling effective strategic planning
- Increasing knowledge and understanding of exposure to risk and emphasizing that unacceptable risks are identified and addressed properly
- Enabling the CISO to paint a picture in business terms that will empower both the board of directors and the C-suite to make risk decisions regarding acceptance, avoidance, or mitigation
- Helping ensure that money and effort are not wasted on risks that are not significant
- Providing senior management with visibility into the organizational risk profile and risk treatment priorities to support their ability to make strategic decisions
- Reducing risks of litigation because of inadequate controls, processes, and contingency plans
- Establishing a systematic, well-informed, and thorough method of decision-making
- Reducing disruptions and avoiding rework by ensuring all staff have a better understanding of the process
- Setting the scene for continual risk reduction and security posture improvement within the organization
- Increasing business resilience against disruption and/or cyberattack that can impact revenue generation

IDC MARKETSCAPE VENDOR INCLUSION CRITERIA

Using the IDC MarketScape model, IDC studied vendors that provide cybersecurity GRC services worldwide. 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 GRC services in more than one region.
- **Sales presence.** Each vendor has a sales force across one or more regions.

- **Customer base.** Each vendor has more than 100 customers.
- **GRC service capability.** Each vendor offers a GRC service that has trained professional cybersecurity staff with expertise in cybersecurity risk management.

ADVICE FOR TECHNOLOGY BUYERS

Technology buyers should consider several factors when looking at cybersecurity GRC services, but they must first answer some key questions: Do I want to build and run this service myself? Do I want a service provider to build the service and then I run it? Or do I want a service provider to build and run the cybersecurity GRC service?

After choosing their preferred approach, they can consider the following for choosing a service provider:

- Understand the service provider's distinctive service capabilities. For instance, consider the number of years it has been performing such work as well as the customers you can speak with for testimonials.
- Determine whether the service provider is interested in understanding the problem to solve and working with you to refine it or it is just giving you a rundown of its services in the hope that you will just buy.
- Understand the differences in services between service providers in the field. Identify what they really bring to the table.
- Determine if the service provider has demonstrable knowledge and skill in the particular area of competence.
- Get clarity on the limits of the service provider's knowledge and skill in this area.
- Determine if the service provider's reach enables it to consistently address your needs on a global scale.
- Identify use cases that the service provider has addressed based on its successful projects. If the service provider is willing, have them describe instances where a project did not result in complete satisfaction.

VENDOR SUMMARY PROFILES

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.

EY

EY is positioned in the Leaders category in the 2025–2026 IDC MarketScape for worldwide cybersecurity governance, risk, and compliance consulting services.

EY (formerly Ernst & Young) is a multinational professional services network and one of the so-called "Big Four" firms, operating in over 150 countries through a network of member firms. Known for its audit, tax, advisory, and consulting services, EY leverages deep domain expertise across industries to support clients in navigating complex regulatory, operational, and technological challenges. Its cybersecurity practice, embedded within its broader risk advisory and technology consulting services, helps organizations build resilience, manage cyber-risk, and comply with evolving regulatory and business imperatives across global jurisdictions.

In the cybersecurity GRC arena, EY distinguishes itself by offering integrated services that link strategic governance, risk quantification, and compliance assurance into a unified program. Its "Cyber Risk, Compliance & Resilience" capability enables clients to assess their cyber posture, determine where investments are required, and implement structured decision-making tied to financial and operational impact. The firm emphasizes that beyond simply meeting regulatory requirements, organizations should embed cyber-risk management into broader business strategy and governance frameworks, transforming GRC from a static obligation into a dynamic enabler of trust and business continuity.

Another area of differentiation for EY lies in its technology-risk and assurance capabilities, which extend its GRC offering into areas such as regulatory readiness, framework alignment, and simulation-based testing. For instance, its Technology Risk Cybersecurity Assurance team provides independent assessments of cyber programs, regulatory readiness (e.g., NIST, ISO frameworks), and incident response simulations, enabling boards and executives to evaluate the effectiveness of controls and their alignment with financial and operational risk profiles. By combining advisory design with assurance, testing, and remediation workflows, EY positions itself as a full-life-cycle GRC partner rather than simply a compliance advisor.

Finally, EY's global scale, industry-specialist teams, and managed services capabilities further enhance its GRC portfolio in the cybersecurity space. Its global footprint and cross-industry experience allow it to support clients in regulated sectors such as financial services, government, healthcare, and energy, where cyber-governance, risk, and compliance obligations are especially acute. Additionally, its managed cybersecurity services help organizations shift from reactive controls to proactive, insight-driven programs, creating cost-effective, resilient cyber functions that integrate governance and compliance into operational delivery. In summary, for enterprises seeking a service provider that can integrate GRC into a broader cyber-resilience and transformation agenda with both advisory and operational depth, EY offers a compelling and differentiated option in the cybersecurity GRC market.

Strengths

- **Focus on cybersecurity risk, compliance, and resilience services:** EY is focused on enhancing its clients' operational spectrum while maximizing engagement value.
- **Operational improvements in the client's cyber GRC estate:** EY services are focused on becoming adept at anticipating changes within client needs, measuring client success and satisfaction, meeting project schedules and goals, and fostering an integrated client team that actively listens to and challenges clients through proactive engagement frameworks and predictive analytics. These services also help organizations establish clearly defined success metrics or KPIs related to risk reduction, compliance adherence, and overall client satisfaction metrics.
- **Enhanced focus on proactive incident response models:** EY emphasizes training, communications, and role clarity in its services. It also offers customizable retainer models for ongoing service engagements, with a focus on rapid recovery to provide minimal service disruptions. EY's Cyber GRC teams also work across cyber forensics, cyber-risk management, and cyber assurance and digital risk capabilities.

Challenges

- **Independence constraints in certain services:** EY's assurance heritage means that independence rules may limit some advisory engagements, particularly where audit or assurance overlap. This can restrict flexibility when clients want integrated strategy, implementation, and audit services from the same provider. It may also make vendor selection more complex.
- **Traditional advisory model amid fast-moving regulation:** Since regulations (AI, data privacy, continuous monitoring) evolve rapidly, EY must adapt its advisory and service delivery model accordingly. Some clients may perceive EY's approach as more traditional and less agile for newer GRC paradigms. Staying ahead of emerging frameworks is an ongoing challenge.

Consider EY When

- **A partner that employs adaptive cyber-resilience:** EY could prove to be an ideal partner if you need cross-functional incident response teams. EY's teams include cybersecurity experts, forensic analysts, and crisis communicators, ensuring a collaborative approach in addressing a wide range of clients' needs and requirements.
- **Enhanced executive-level engagement:** Consider working with EY if you need strong relationship ties to both regulators and senior boards/C-suites, which enable it to meet the unique needs of global enterprise clients, no matter the jurisdiction.

- **Cyber is embedded as a board-level imperative in strategy, risk, compliance, and resilience.** Consider EY as a partner if you want people, process, and tech to move together. EY emphasizes enablement, communication, and adoption that help sustain improvements beyond go live.

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.

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 market share of each individual vendor within the specific market segment being assessed.

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

According to the 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 governance, risk, and compliance market relates to this definition. GRC includes both 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 personal data, they increasingly become aware of challenges involving the privacy and security of that data. Services that help organizations secure the privacy of data, address the threat of cyberattacks, and deal with the growing number of privacy-focused regulations are imperative. Technology suppliers and service providers have a unique visibility as well as trust with enterprise clients to develop collaboration across departments and roles. This collaboration ensures 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 security governance, risk, and compliance 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 encompasses adhering to all necessary regulatory and legal requirements, as well as managing any changes to the regulatory environment and its impact on the enterprise. This segment includes regulatory compliance management and regulatory change management.
- **Audit and regulatory management.** Audit management solutions help organizations plan, manage, and analyze processes (both 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. This also enables organizations to 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.
- **Third-party risk management.** TPRM services are designed to help organizations identify, assess, mitigate, and monitor risks associated with third-party engagements and/or acquisitions. These services span advisory and consulting to fully outsourced managed services, offering scalable solutions tailored to the complexity and maturity of an organization's cybersecurity risk posture and cybersecurity compliance needs.

The worldwide GRC market is made up of professional security services (PSS), which include consulting and integration security services; software, software as a service (SaaS), and managed security services (MSS), consisting of legacy customer premises equipment (CPE), traditional hosted, cloud hosted, or as a service; and education and deployment. The sections that follow include a breakdown of these categories.

Professional Services

Professional services include consulting, design, implementation, and engineering services to support the creation and implementation of GRC programs and software solutions. In addition, advisory services consist of executive guidance: strategy, road maps, mentorship, board training, virtual executive services, and program management.

Managed Services

This category includes services that establish responsibilities, processes, practices, methodologies, and tools to create the cyber-risk vision and strategy. These services involve:

- Risk definition and appetite, plans, road map, and budget
- Policies and procedures required to comply with relevant cybersecurity and privacy laws, policies, rules, and regulations
- Metrics that show risk and compliance posture, residual risks, financial impacts, and ROI
- Due diligence activities and assessments to identify, assess (qualitative, quantitative, and maturity), categorize, catalog, test, and monitor aspects of

the enterprise related to risk, compliance, privacy, third parties, and supply chain, as well as audit readiness

- Activities on selecting, implementing, integrating, migrating, managing, operating, and maintaining solutions that provide automation, orchestration, machine learning, and AI

Education and Deployment

This category includes skill and awareness training and education, program and solution deployment, and configuration services. GRC providers often incorporate these services into the overall solution. Skill training can cover various areas of GRC, such as governance management, risk management, and compliance management, and is typically designed for staff who perform these functions. Awareness training is designed to raise awareness among all employees of their responsibilities for GRC.

LEARN MORE

Related Research

- *Worldwide Security Governance, Risk, and Compliance Services and Software Forecast, 2025–2029* (IDC #US53611425, June 2025)
- *Worldwide Security Governance, Risk, and Compliance Services Forecast, 2025–2029* (IDC #US53611525, June 2025)
- *IDC's Worldwide Security Services Taxonomy, 2025* (IDC #US53294625, April 2025)
- *Cybersecurity Metrics – A Data-Driven Framework for the Future* (IDC #US52699424, November 2024)
- *Continuous Compliance Management Increases Resilience to Cyberattack* (IDC #US52638324, October 2024)
- *Choosing the Right Security Framework* (IDC #US49291622, July 2022)

Synopsis

This IDC study explores the services underpinnings required to enable a successful and fully implemented cybersecurity GRC program that can be managed either by the end customer or by the service provider that built it. This study also raises questions that buyers and vendors in this space can use as a guide to make informed decisions and achieve desired outcomes. The discipline and design of cybersecurity GRC services can provide a framework for orienting organizations from optimizing standard checkbox outcomes to optimizing a value-added program that effectively manages cybersecurity risks. This framework should also provide a prescriptive life-cycle approach that drives commitment and support from senior executives, board members, and various stakeholders in between.

"A well-defined cybersecurity GRC program is critical in today's ever-changing and growing threat landscape," said Phil Harris, research director, IDC's GRC Services and Software program. "Attackers are in the business for the long haul, extracting as much valuable data or intelligence while undetected to reap as many benefits as possible. A practical and pragmatic way to combat this is to adopt an ongoing methodical approach to assessing the depth and breadth of cybersecurity controls and the maturity to cull new or not-so-obvious vulnerabilities and exposures that attackers exploit. This is an ongoing race, and organizations with strong cybersecurity GRC programs will be better prepared to withstand evolving attacks."

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.