IDC MarketScape

# IDC MarketScape: Worldwide Governance, Risk, and Compliance Software Vendor Assessment, 2025

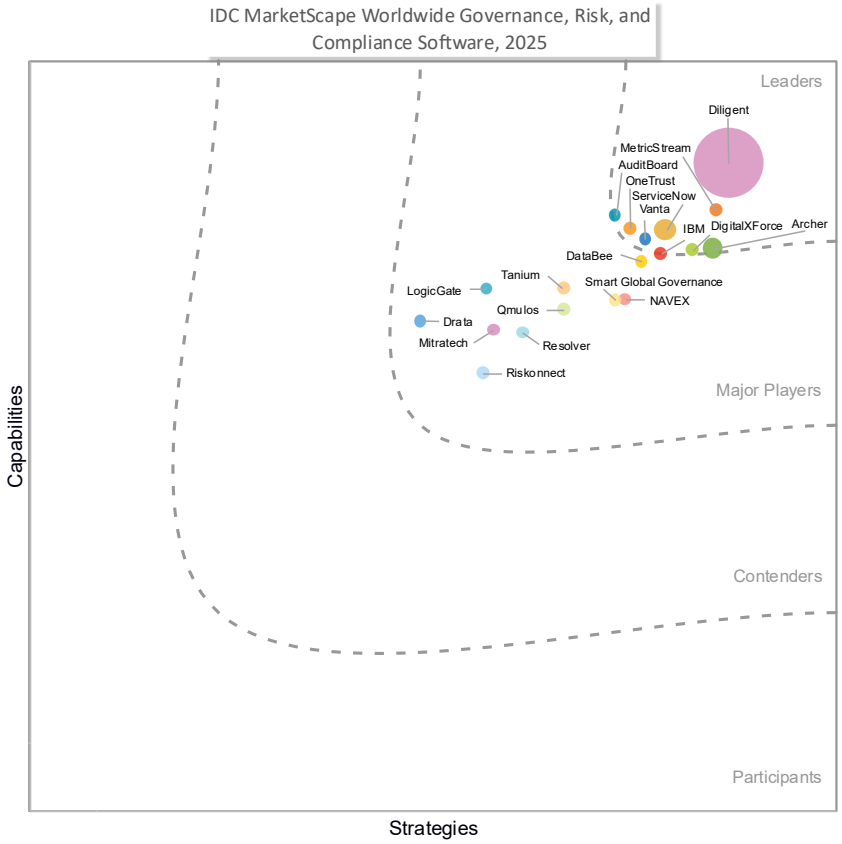
Philip D. Harris, CISSP, CCSK

**THIS EXCERPT FEATURES DATABEE AS A MAJOR PLAYER**

## IDC MARKETSCAPE FIGURE

### FIGURE 1

**IDC MarketScape Worldwide Governance, Risk, and Compliance Software Vendor Assessment**




Source: IDC, 2025

June 2025, IDC #US53615325e

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 Governance, Risk, and Compliance Software Vendor Assessment, 2025 (Doc # US53615325).

## IDC OPINION

The governance, risk, and compliance (GRC) marketplace for software continues to advance and provide various levels of value to organizations today. The increase in ransomware cyberattacks and regulatory requirements from the Securities and Exchange Commission and European governments to increase the accountability and responsibility of the senior executives and boards of directors have recently been fueling this process. These two groups have paid attention to their organizations' cybersecurity risk and compliance but not in such a way that they are provided with a complete and accurate view of these postures. These views have traditionally been only partial or incomplete views of the IT estate due to the manual nature of how risk and compliance are conducted today and have been conducted in the past. There has also been a lack of available cybersecurity solutions with the ability to constantly monitor the state of risk and compliance across the entire IT estate.

In addition, with the cybersecurity labor shortage, GRC vendors have been infusing automation, orchestration, machine learning (ML), and AI into their software platforms to accelerate productivity and reduce the overhead that is typical with GRC programs. A good example is GRC platforms that can continuously monitor IT estates, submit support tickets, and resolve risks and deficiencies in an accelerated fashion.

IDC believes GRC software is a crucial tool for any organization looking to manage its cybersecurity governance, risk, and compliance effectively and efficiently. GRC software can enhance efficiency through workflow and process automation, orchestration, ML, and AI across the various processes and methodologies required for risk management, compliance management, and governance. This can accelerate the productivity, accuracy, and timeliness of outcomes as well as provide executives and board members with the most current state of risk and compliance postures.

GRC software can help organizations:

- Identify potential risks and provide strategies for managing them. This can help organizations avoid costly mistakes and legal issues.

- Ensure they are compliant with various laws, regulations, industry standards, and corporate policies. This can reduce the risk of fines and penalties and damage the organization's reputation and brand.
- Keep up with changes in worldwide and local laws, regulations, and industry standards. This also extends to the various industry standards bodies, such as ISO and NIST. This can help ensure that the organization remains compliant even as laws, regulations, and standards evolve.
- Generate reports that provide insights into an organization's governance, risk, and compliance status and posture. The underlying goal is to help executives, board members, and decision-makers make informed decisions as to whether to accept or avoid risks or compliance deficiencies.
- Establish a single repository of truth for all risks and deficiencies identified throughout the IT estate.
- Collect contextual intelligence about the state of various aspects of the IT estate. This will provide insights into areas of improvement, helping organizations continuously improve their governance, risk management, and compliance processes.
- Leverage new, enhanced, and powerful tools, such as AI integrated in the GRC platform to further accelerate all aspects of GRC, including policy, regulation, and industry standards normalization and currency, bringing context to the intelligence that GRC platforms gather and will contribute to highly effective asset management, data ownership, and data classification.
- Manage the potential risks from engaging with and/or acquiring third- to nth-party solutions, suppliers, and supply chains that have access to sensitive organization assets, data, strategies, and so forth.

Ultimately, GRC software helps organizations by providing platforms for the governance of the overall program, risk and compliance assessments, risk and deficiency remediation, and reporting across the IT estate, third parties, and supply chains. Many of the traditional GRC tasks, methods, and processes are no longer manual and leverage automation, orchestration, ML, and AI. This will reduce human bias and subjectivity, accelerate processes and outcomes, significantly improve accuracy, and ensure risks and deficiencies are managed to conclusion. With the collection of contextual intelligence, GRC dashboards and reporting capabilities can provide insights into the actual state of risk and compliance postures, highlight areas of improvement, and, in some cases, offer cyber-risk quantification (CRQ) to provide executives and board members with the monetary impact of accepting or avoiding risks and compliance deficiencies.

The Market Definition section in the Appendix provides a description of what IDC believes is the minimum set of capabilities a GRCS software provider should offer.

IDC encourages buyers to evaluate GRCS software providers based on the outcomes they want to achieve related to day-to-day identification, treatment, and closure of risks.

## IDC MARKETSCAPE VENDOR INCLUSION CRITERIA

Using the IDC MarketScape model, IDC studied vendors that provide GRCS throughout 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 in more than one region throughout the world.
- **Sales presence:** Each vendor has a sales force across one or more regions throughout the world.
- **Customer base:** Each vendor has 100+ customers.
- **GRCS capability:** Each vendor possesses a GRCS service that has trained professional cybersecurity staff with expertise in cybersecurity risk management.

## ADVICE FOR TECHNOLOGY BUYERS

GRC software offers various features and capabilities based on organizational priorities and requirements. The following are critical factors to consider:

- **Automation, orchestration, ML, and AI:** Advanced features are now available in GRC platforms. These features can dramatically ease any GRC program and make it efficient when implemented properly. These days, cybersecurity organizations must do more with less and have a GRC platform that can automate procedures, processes, and methodologies that once were manual and orchestrate entire risk and compliance management activities. Infusing AI and ML brings tremendous benefits in preparing outputs that are almost complete but require an analyst to validate and confirm the results before presenting them to management.
- **User experience:** GRC platforms offer simplified interfaces that accelerate the user experience while not sacrificing accuracy and efficiency. Ensure that the use cases document the ways the GRC platform is to be used. Even a few GRC platforms have dramatically simplified and clarified the leveraging of CRQ.
- **Security:** Governance, risk, and compliance management are critical aspects of any organization. The GRC platform's access control and confidentiality are essential to ensuring sensitive information is protected from theft, unauthorized modification, unauthorized access, and disruption.

- **Integration:** GRC platforms offer extensive portfolios of connectors to a wide variety of systems, databases, and applications for the purpose of gathering risk and compliance information. GRC platforms are now creating intelligence fabrics with contextual intelligence designed to add value through data classification, data and asset ownership, and the sensitivity of the information in the context of the systems storing the data.
- **Customization:** Deploying new GRC software should align with your enterprise's unique requirements. Recognize that organizations within the same industry may have different objectives and choose a solution that offers full customization capabilities to address your company's specific needs.
- **Cost:** While governance, risk management, and compliance are non-negotiable priorities, considering factors such as total cost of ownership and ROI is essential when choosing a new GRC solution. Provide robust support for your GRC strategy while maintaining favorable costs, allowing you to maximize profits for your shareholders.
- **Reputation:** Evaluating the reputation of software vendors is equally crucial. As the demand for GRC solutions grows due to stricter compliance regulations, new vendors enter the market regularly. Assess a vendor's reputation based on the vendor's experience in providing GRC solutions, client base, and reviews. This insight will help you set realistic expectations.
- **Scalability:** The GRC software you select should accommodate organizational growth. As your business expands, compliance requirements and data handling increase. Ensure your GRC tool can meet these future needs and adapt flexibly to changes in your GRC strategy.

Governance, risk management, and compliance management are critical activities of any business and must be prioritized. Regulations and laws are now making it crucial for executives and board members to have their fingers on the pulse of the ongoing risk and compliance posture. Without a proper GRC strategy, organizations can encounter significant challenges that go unnoticed, unmonitored, and unmitigated. Implementing GRC software can streamline this strategy, making internal resources and staff more effective and efficient through powerful workflows, user-friendly features, and the ongoing trackability of risks and deficiencies. This can also have an impact on the resilience of an organization to withstand cyberattacks.

## 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.

## DataBee

DataBee, a Comcast company, is positioned in the Major Players category in the 2025 IDC MarketScape for worldwide governance, risk, and compliance software.

Quick facts about DataBee include:

- **Year founded:** 2022
- **Number of Employees:** ~120
- **Regional presence:** The United States, Canada, the United Kingdom, the Netherlands, Germany, India
- **Products:** The DataBee security, risk, and compliance data fabric platform

To date, four product modules run on the platform:

- DataBee for Vulnerability and Asset Exposure Management
- DataBee for Security Threats
- DataBee for PCI-DSS 4.0 Preparedness
- DataBee for Continuous Compliance and Risk Management (CCRM)
- DataBee BeeKeeper generative AI chatbot

DataBee, which Comcast founded and fund, offers the DataBee cloud-native security, risk, and compliance data fabric platform. This platform provides connected data and deep insights into security and GRC teams, enabling them to address security and compliance gaps more efficiently and cost-effectively. DataBee automates data engineering by ingesting data from various sources, standardizing and normalizing it into the Open Cybersecurity Schema Framework, and transferring a clean data set to the customer's data lake or any Iceberg-compatible storage destination. It employs patent-pending entity resolution techniques to unify device and user identifiers, enhancing the value extracted from disparate tools and providing actionable security and compliance insights.

In addition to the DataBee platform, customers can purchase specific solutions such as DataBee for Vulnerability and Asset Exposure Management, Security Threats, PCI-DSS 4.0 Preparedness, and CCRM. Recently, DataBee introduced DataBee BeeKeeper, a generative AI-based chatbot that automates asset and application validation by engaging potential owners via Microsoft Teams. This innovation streamlines asset and application discovery, inventory, and management, contributing to improved security and compliance outcomes. DataBee primarily targets large enterprises and federal organizations in heavily regulated industries, including financial services, government, insurance, pharmaceuticals, energy and utilities, manufacturing, transportation, and retail.

While DataBee in and of itself is not a GRC platform in the traditional sense, it offers a means to prioritize and manage a cross-organizational integrated GRC program using a powerful intelligence fabric, AI, ML, and workflows. DataBee offers a data-driven means to manage, measure, and calibrate risk and compliance through the collection of intelligence from throughout the IT estate. Using this intelligence, DataBee dashboards and reporting are centralized and can empower analysts and management across the enterprise to carefully monitor and maintain an ongoing GRC program to ensure compliance with corporate cybersecurity policies, industry standards, and regulatory requirements.

## Strengths

DataBee was designed to be data-driven, and using AI and workflows can bring powerful results to the company's customers. DataBee offers capabilities such as contextual intelligence from throughout the IT estate that creates impactful insights, aids executives in objective decision-making, and shows the risk posture of an organization, which is critical for cybersecurity leaders.

DataBee is flipping the tables on managing cybersecurity and GRC programs by retraining the CISO and other executives to become data-driven instead of being "interrupt-driven" (reactive). DataBee has realized from its internal practices at Comcast that cybersecurity intelligence gathering is no longer a luxury but a critical need for data-driven cybersecurity leaders to be successful.

## Challenges

DataBee is a new capability introduced to the marketplace in the past couple of years and, hence, does not yet have wide market recognition. While this appears to be a stealthy introduction to the marketplace, DataBee must be prepared to turn on its marketing engine.

## Consider DataBee When

Large enterprises with mature risk and GRC management programs that potentially have more than one GRC platform currently being leveraged should consider DataBee. Organizations will find the ROI, accelerated results, and data-driven approach to be powerful for consolidating GRC and risk management platforms in favor of a nimbler intelligence fabric.

## 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 and/or 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 to provide an accurate and consistent assessment of each vendor's characteristics, behavior, and capability.

# Market Definition

GRC software is a type of enterprise software that helps organizations manage their GRC processes and methodologies. GRC software provides a unified platform for managing these three critical aspects of an organization's cybersecurity programs. The following is a breakdown of what each component means:

- **Governance** refers to the processes, procedures, and policies that ensure an organization is controlled and directed in a manner that aligns with its strategic goals. It includes areas such as executive management, the board of directors, internal controls, risk management, and compliance.
- **Risk** refers to the potential for loss or harm that could impact an organization. Risks can come from various sources, including operational, financial, strategic, reputational, and compliance risks. Risk management involves identifying, assessing, and mitigating these risks.
- **Compliance** refers to the process of ensuring that an organization complies with laws, regulations, and standards that apply to its operations. Compliance management involves activities such as monitoring, reporting, and auditing to ensure compliance.

GRC software helps organizations manage these three aspects by providing platforms for the governance of the overall program, risk and compliance assessments, risk and deficiency remediation, and reporting across the IT estate, third parties, and supply chains. Many of the traditional GRC tasks, methods, and processes are no longer manual and are leveraging automation, orchestration, ML, and AI. This will reduce human bias and subjectivity, accelerate processes and outcomes, significantly improve accuracy, and ensure risks and deficiencies are managed to conclusion. With the collection of contextual intelligence, GRC dashboards and reporting capabilities can provide insights into the actual state of risk and compliance postures, highlight areas of improvement, and, in some cases, offer CRQ to provide executives and board members with the monetary impact of accepting or avoiding risks and compliance deficiencies.

GRC software can help organizations:

- Identify potential risks and provide strategies for managing them. This can help organizations avoid costly mistakes and legal issues.
- Ensure they are compliant with various laws, regulations, industry standards, and corporate policies. This can reduce the risk of fines and penalties and damage the organization's reputation and brand.
- Keep up with changes in worldwide and local laws, regulations, and industry standards. This also extends to the various industry standards bodies, such as ISO or NIST. This can help ensure that the organization remains compliant even as laws, regulations, and standards evolve.
- Generate reports that provide insights into an organization's governance, risk, and compliance status and posture. The underlying goal is to help executives, board members, and decision-makers make informed decisions as to whether to accept or avoid risks or compliance deficiencies.

- Establish a single repository of truth for all risks and deficiencies identified throughout the IT estate.
- Collect contextual intelligence about the state of various aspects of the IT estate. This will provide insights into areas of improvement, helping organizations continuously improve their governance, risk management, and compliance processes.
- Leverage new, enhanced, and powerful tools such as AI integrated in the GRC platform to further accelerate all aspects of GRC, including policy, regulation, and industry standards normalization and currency, bringing context to the intelligence that GRC platforms have gathered and that will contribute to highly effective asset management, data ownership, and data classification.
- Manage the potential risks from engaging with and/or acquiring third- to nth-party solutions, suppliers, and supply chains that have access to sensitive organization assets, data, strategies, and so forth.

## LEARN MORE

## Related Research

- *Worldwide Security Governance, Risk, and Compliance Services and Software Forecast, 2024–2028* (IDC #US51935324, March 2024)
- *Worldwide Security Governance, Risk, and Compliance Software Forecast, 2024–2028* (IDC #US51935824, March 2024)
- *IDC's Worldwide Security Products Taxonomy, 2024* (IDC #US51825024, February 2024)
- *IDC's Worldwide Security Services Taxonomy, 2023* (IDC #US50332523, March 2023)
- *IDC's Worldwide Governance, Risk, and Compliance Software Taxonomy, 2021* (IDC #US47611921, April 2021)

## Synopsis

This IDC study explores the services underpinnings required to enable successful and fully implemented GRC software that can be managed either by the end customer or by a managed security services provider. The discipline and design of GRC software can provide a path forward for ensuring an organization is responsible for managing all risk and compliance issues as expeditiously as possible. Management and executives can understand which critical issues require action for mitigation. By leveraging AI going forward, software providers are finding ways to alleviate the cumbersomeness and laboriousness of having to manage GRC programs.

"GRC software has come into its own with regard to capabilities and features that empower, accelerate, and enable end users to be highly effective in managing issues and aiding management to take appropriate steps to mitigating risks and compliance issues to increase business resilience to cyberdisruptions," says Phil Harris, research director, IDC's GRC Services. "Attackers are in their business for the long game, where they can exploit vulnerabilities (risk and compliance) that go unmanaged to extract as much valuable data or intelligence over an extended period of time undetected to reap as much money as possible. GRC software is a critical capability for any organization to mitigate risks and compliance issues to reduce the risk of cyberevents. Organizations also have critical compliance requirements that are intended to protect the very information that cyberattackers seek to steal. This is an ongoing race, and organizations with strong GRC programs backed by powerful GRC software will be better prepared to withstand ongoing attacks and reduce the risk of running afoul of regulators."

## 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 report sales at +1.508.988.7988 or www.idc.com/?modal=contact_repsales for information on applying the price of this document toward the purchase of an IDC service or for information on additional copies or web rights.

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