MARKET PERSPECTIVE

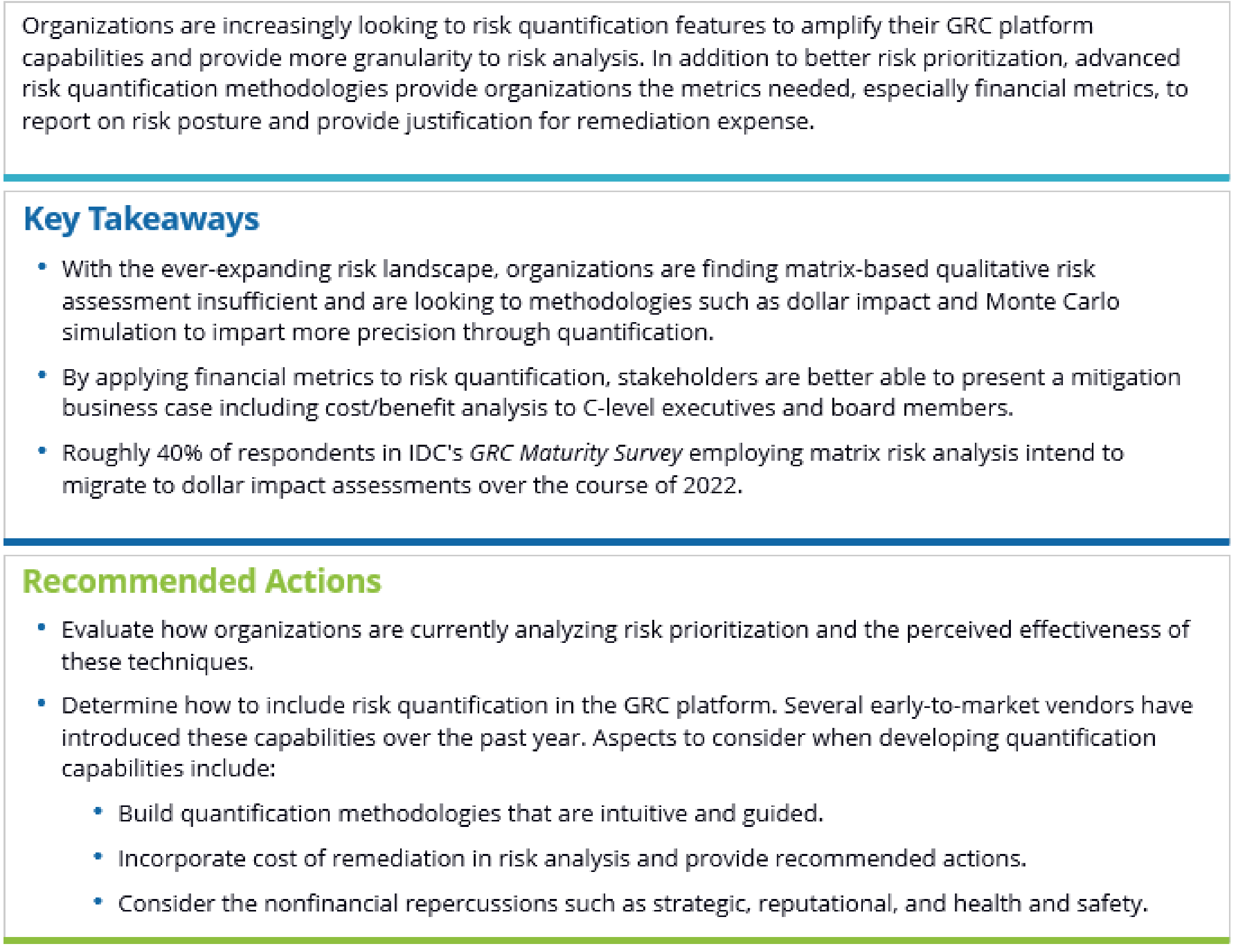
How to Increase the Value of Your GRC Platform with Risk Identification and Quantification

Amy Cravens

EXECUTIVE SNAPSHOT

FIGURE 1

Executive Snapshot: How to Increase the Value of Your GRC Platform with Risk Quantification



Organizations are increasingly looking to risk quantification features to amplify their GRC platform capabilities and provide more granularity to risk analysis. In addition to better risk prioritization, advanced risk quantification methodologies provide organizations the metrics needed, especially financial metrics, to report on risk posture and provide justification for remediation expense.

Key Takeaways

- With the ever-expanding risk landscape, organizations are finding matrix-based qualitative risk assessment insufficient and are looking to methodologies such as dollar impact and Monte Carlo simulation to impart more precision through quantification.
- By applying financial metrics to risk quantification, stakeholders are better able to present a mitigation business case including cost/benefit analysis to C-level executives and board members.
- Roughly 40% of respondents in IDC's *GRC Maturity Survey* employing matrix risk analysis intend to migrate to dollar impact assessments over the course of 2022.

Recommended Actions

- Evaluate how organizations are currently analyzing risk prioritization and the perceived effectiveness of these techniques.
- Determine how to include risk quantification in the GRC platform. Several early-to-market vendors have introduced these capabilities over the past year. Aspects to consider when developing quantification capabilities include:
  - Build quantification methodologies that are intuitive and guided.
  - Incorporate cost of remediation in risk analysis and provide recommended actions.
  - Consider the nonfinancial repercussions such as strategic, reputational, and health and safety.

Source: IDC, 2022

June 2022, IDC #US49117622

NEW MARKET DEVELOPMENTS AND DYNAMICS

Risk quantification is a core component of governance, risk, and compliance (GRC) platforms that enables organizations to rank and prioritize risk. With the ever-expanding risk landscape, it is becoming increasingly important for organizations to effectively evaluate risk in order to see through the weeds and identify critical factors. Quantification provides a consistent way to evaluate relative risk based on the probability of occurrence and the potential impact to the organization. Risk quantification offers four critical capabilities for organizations:

- **Structured approach:** Risk identification and quantification processes provide organizations with a framework for consistent risk evaluation that lends to more meaningful analysis.
- **Risk prioritization:** Through the structured approach, risk is better identified, and in applying quantifiers, organizations can better assess their risk posture. By enabling a real-time, analysis-driven perspective of key organizational risk, companies are better able to mitigate against it.
- **Strategic response:** Risk quantification can in turn fuel an organization's strategic response to risk. Quantitative analysis is also valuable in helping organizations put a dollar value to risk, which fuels strategic decision making and provides guidance as to the appropriate risk remediation efforts based on the organization's risk appetite and risk exposure. Furthermore, by understanding the potential cost of risk to an organization and based on its risk appetite, the appropriate level of mitigation or insurance coverage can be determined.
- **Driving action:** Framing risk in monetary terms also allows for better business case presentation to C-level executives and boards in request for remediation efforts.

Risk Identification and Quantification Methodologies

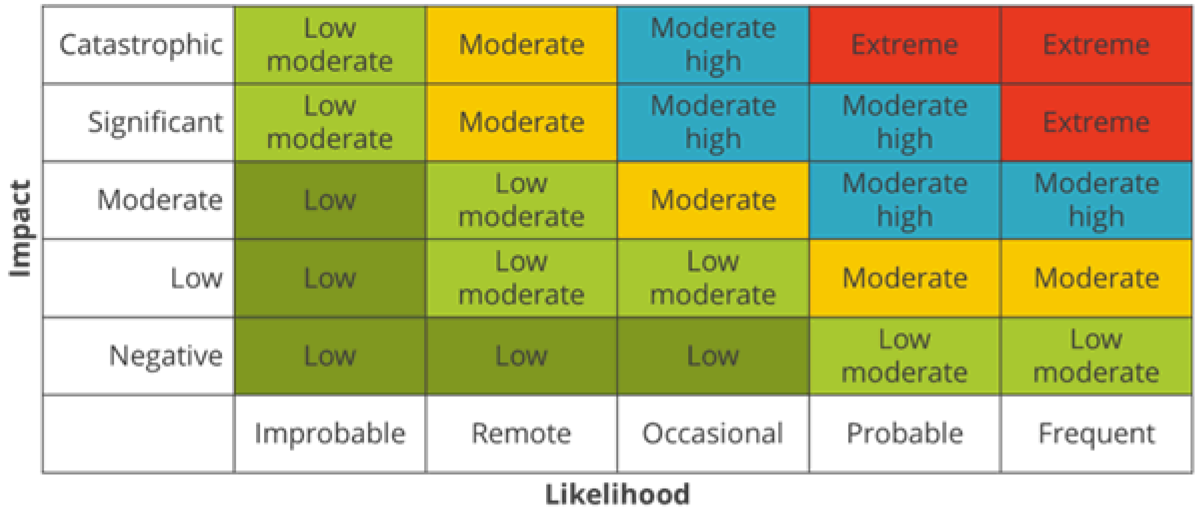
There are both qualitative and quantitative methodologies for risk analysis. The most common qualitative method is a matrix or heatmap, while quantitative methods include bowtie, FAIR, and Monte Carlo analysis.

Matrix/Heatmap

Matrix or heatmaps are the standard type of risk measurement used in GRC platforms and apply a numerical or color-based code to various risks based on projected likelihood of occurrence and potential impact on the organization. Occurrence and impact are given qualified, rather than quantified, ranges, as shown in Figure 2. A matrix or heatmap approach is a good tool to quickly visualize an organization's risk landscape; a dashboard filled with green suggests a risk-protected organization, while one primarily populated with red indicates an organization at significant risk. In addition to visualizing risk, these tools also help organizations loosely prioritize which risks are the most significant so that remediation efforts can be better focused. An organization can target red/level 5 risks to be the most important to address to reduce the organization's risk level.

FIGURE 2

Risk Matrix Example



Impact					
Catastrophic	Low moderate	Moderate	Moderate high	Extreme	Extreme
Significant	Low moderate	Moderate	Moderate high	Moderate high	Extreme
Moderate	Low	Low moderate	Moderate	Moderate high	Moderate high
Low	Low	Low moderate	Low moderate	Moderate	Moderate
Negative	Low	Low	Low	Low moderate	Low moderate
	Improbable	Remote	Occasional	Probable	Frequent

Source: IDC, 2022

The challenge with matrix-based risk scoring is that they lack precision. Multiple risks can have the same rating but have a very different risk potential. For example, a probable risk that would have significant impact is ranked the same as a probable risk that only has moderate impact. Both risks, viewed on a heatmap, would appear to have the same risk potential, when, in actuality, the risk potential is much different.

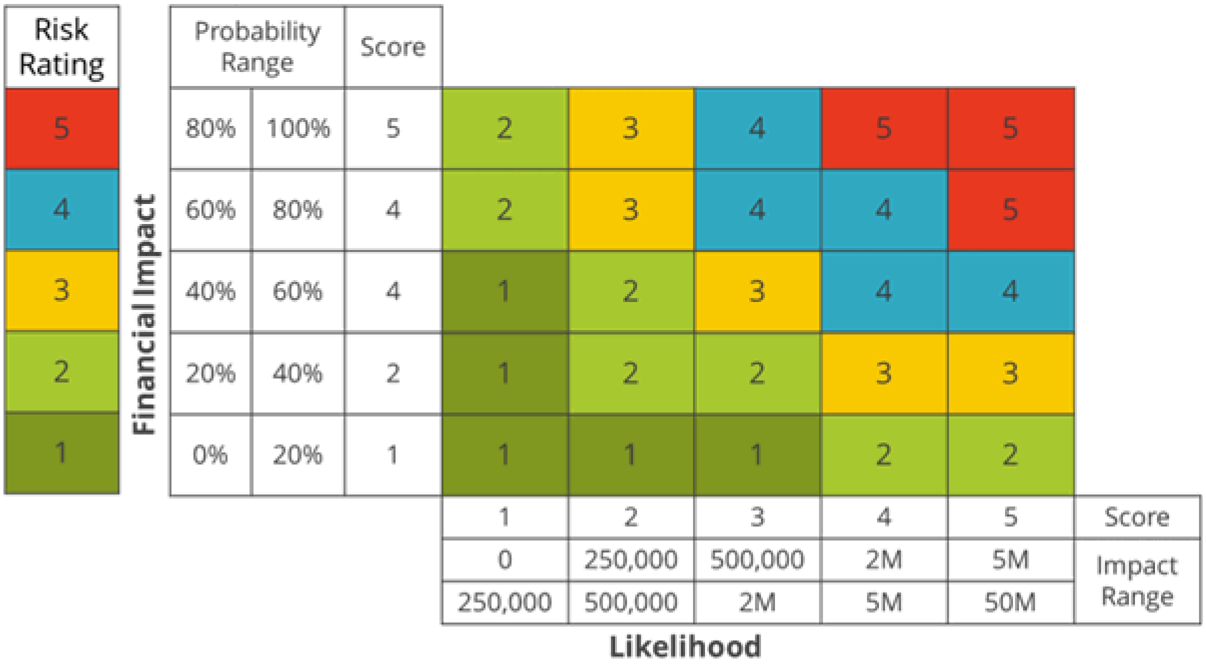
The heat matrix can be given more definition by adding quantifiable probability and impact ranges, as shown in Figure 3. This rudimentary dollar impact analysis essentially overlays a heatmap or matrix with quantifiable likelihood and impact assessments. It provides a range of the potential likelihood of an event transpiring as well as a range of the cost to the organization if the risk event occurs. By overlaying the qualitative heatmap with quantitative estimates, organizations are able to achieve more precise risk assessments and therefore are better able to prioritize remediation.

Ranges for likelihood and cost of a risk event should be fed by data collected across the organization and coalesced in the GRC platform. Overtime, as more data is aggregated, the ability to predict the rate of risk events will improve. This allows the organization to compare assumed likelihood and impact ranges with the historic data to evaluate the correctness of these assumptions. This enables improved estimations on risk potential, which in turn helps organizations better prioritize remediation spend. For instance, if an organization assumes that the risk potential for an event is 50%, but in the past years, the annual incidence is actually 10%, then the organization is likely overcompensating for this risk where the resources could be better attributed to prevention of a more elevated risk.

Dollar impact analysis is beneficial in making risk quantifiable which is impactful in prioritizing risk remediation as well as for reporting purposes. By framing risk in cost terminology, concerns can be better communicated to organizational decision makers including C-level executives and boards. Decision makers are better able to assess where risk investment should be concentrated as well as how impactful previous investments have been.

FIGURE 3

Probability/Impact Analysis Example



Risk Rating
5
4
3
2
1

Financial Impact

Probability Range		Score						
80%	100%	5	2	3	4	5	5	
60%	80%	4	2	3	4	4	5	
40%	60%	4	1	2	3	4	4	
20%	40%	2	1	2	2	3	3	
0%	20%	1	1	1	1	2	2	
			1	2	3	4	5	Score
			0	250,000	500,000	2M	5M	Impact Range
			250,000	500,000	2M	5M	50M	

Likelihood

Source: IDC, 2022

Dollar impact assessments can span a broad range in accuracy and tend to only be as good as the data feeding them. The closer an organization can accurately predict impact and likelihood, the more useful the metrics. When broad ranges are applied, there tends to be significant overlap in risk rating bands, where risks that appear to be lower priority may actually represent a greater risk to the organization. To better understand risk, organizations are applying advanced risk quantification techniques such as bowtie, FAIR, and Monte Carlo analysis.

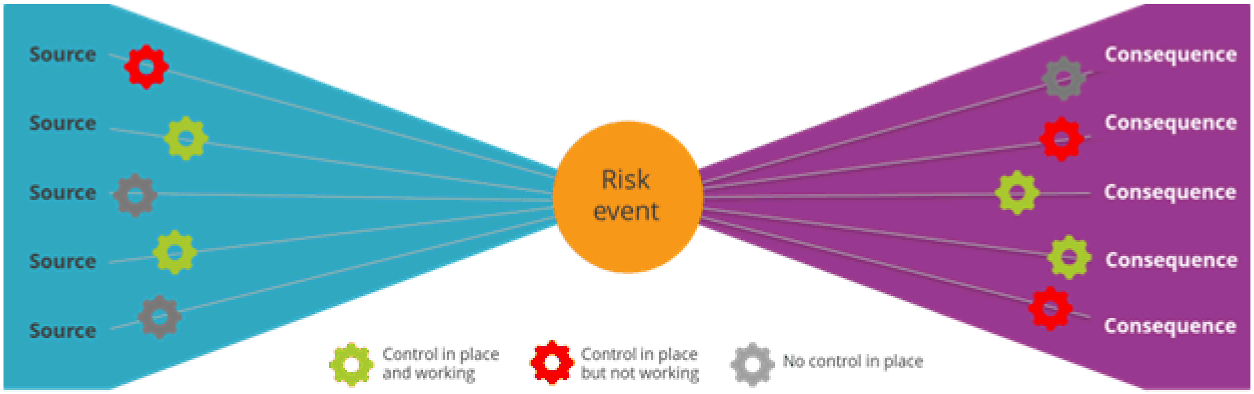
Bowtie

Bowtie risk analysis is a mapping process that enables organizations to track the cause and effects related to a potential risk event. This provides organizations with a clearer view of the multiple aspects that feed a risk event and the multiple consequences that are the result. For example, Figure 4 uses bowtie analysis to explore a risk event, including factors impacting the potential risk and potential repercussions of the event.

Organizations can also visualize the control frameworks that are, or could be, implemented to minimize risk events and their consequences. Organizations can view controls on both sides of the risk event, either to prevent the risk from occurring or to prevent repercussions. Controls on the left side of the bowtie are preventative, put in place to keep the risk from occurring, while controls on the right side are reactive, put in place to minimize the damage if the risk event occurs. Further insight into the risk landscape can be added by layering control status (implemented/effective = green, implemented/not effective = red, and not implemented = grey) to better illuminate where additional investment may be needed.

FIGURE 4

Bowtie Analysis Example



Source: IDC, 2022

Bowtie analysis can be attributed to common events to further explain how the model functions. To better illustrate, consider the example of a car accident as a risk event. The sources of risk may be road conditions, traffic, driver distraction, and so forth. The consequence may be injury, damaged car, legal, and so forth. The controls on the left side (gear figures in Figure 4) might be snow tires or rerouting — mitigation efforts that will reduce the chance of the incident occurring. On the right side, controls would include wearing a seat belt or having insurance — mitigation efforts that would reduce the significance of the consequence if the risk event occurs.

The benefit of bowtie analysis is that it allows for a universal view of the potential implications of an event. The model can factor in strategic, health and safety, environmental, and reputational repercussions in addition to financial impacts. With the interconnected nature of the modern risk landscape and the significance of nonfinancial repercussions to an organization in today's trust environments, being able to capture this unified view of risk and its repercussions has significant value.

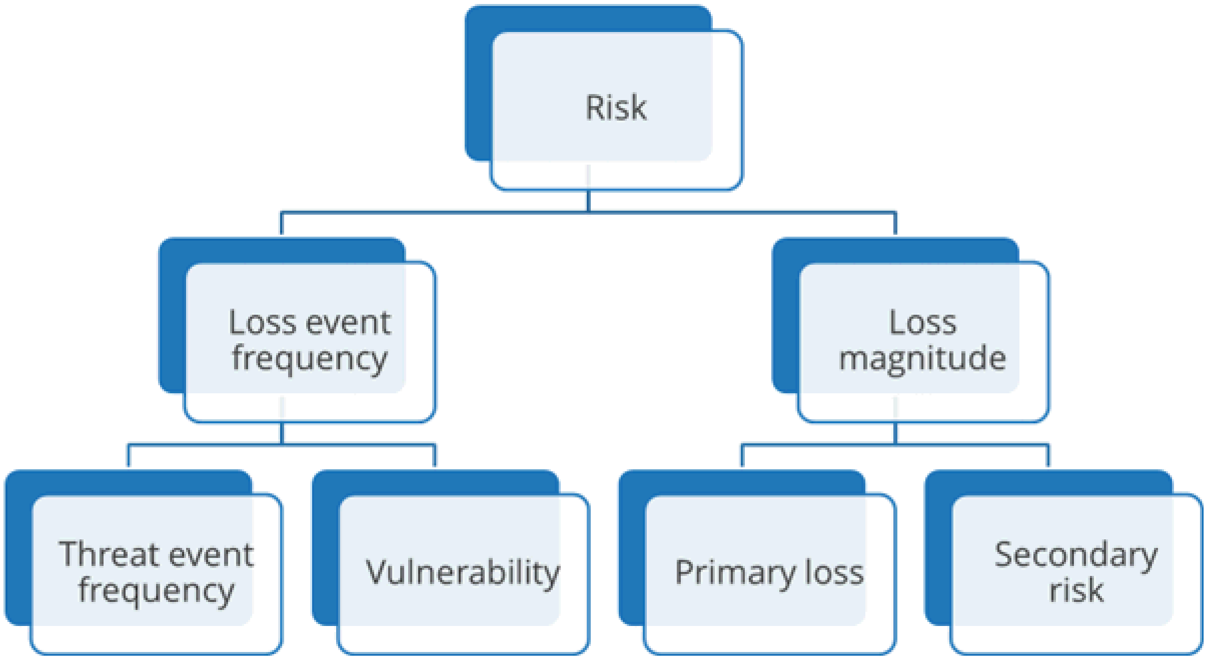
FAIR

FAIR (Factor Analysis of Information Risk) is a method similar to bowtie analysis used to codify and monetize risk and aid in establishing accurate probabilities for the frequency and magnitude of a risk event (see Figure 5). Like bowtie analysis, FAIR identifies the contributing components of risk and their relationship to one another. The relationships between each element of risk can be measured mathematically and assigned dollar values, so that ultimately risk can be calculated as financial loss potential. There are multiple components in a FAIR analysis:

- Asset: Consider relevant assets that may be impacted such as a customer information database or an ecommerce application.
- Threat: Identify the probable threats (insiders, criminal hackers).
- Effect: Determine how the threat would impact the business (reputation, operations, financial) and how the loss would take place.
- Risk: What is the probable frequency and probable magnitude of future loss?

FIGURE 5

FAIR Analysis Model



Source: IDC, 2022

An organization can use FAIR in conjunction with bowtie analysis. To effectively quantify cyber-risk, two models are needed: a model such as bow-tie to clearly define the risk scenario and a risk analysis model such as FAIR to quantify the cyberloss exposure. The NIST has also supported FAIR risk analysis in conjunction with its cybersecurity framework (CSF) for risk identification and quantification.

Monte Carlo

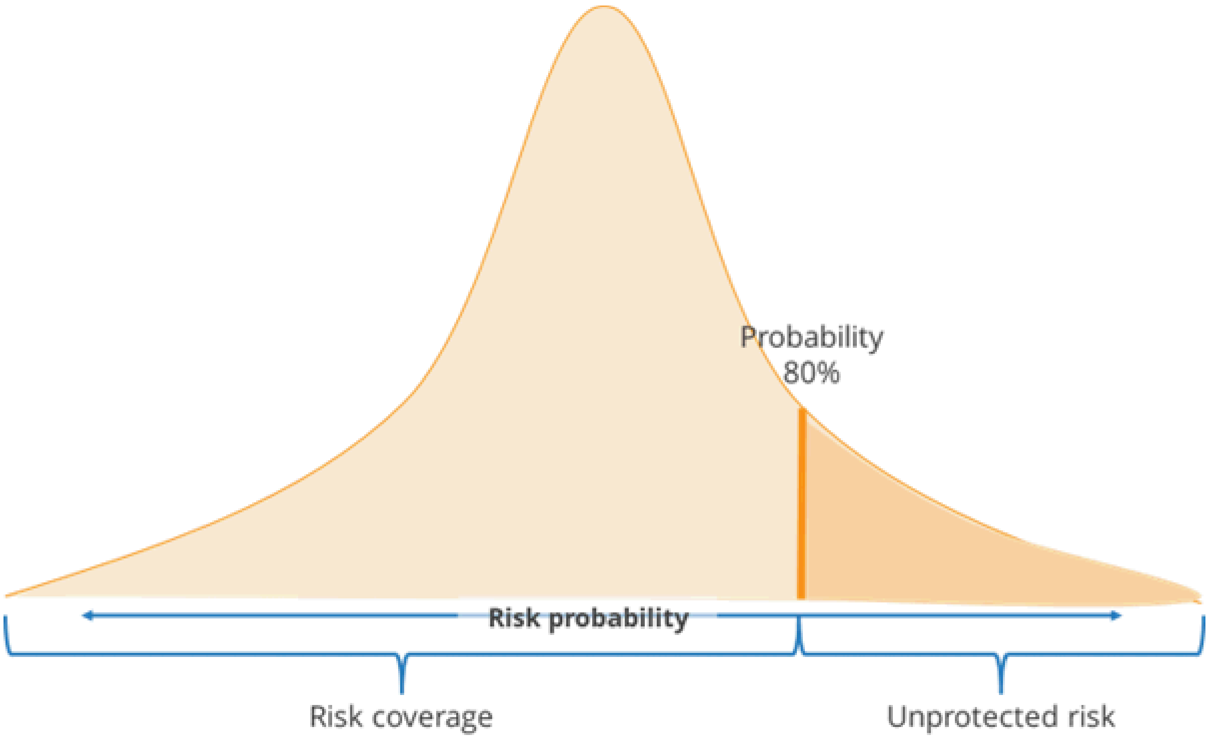
Monte Carlo is a computer simulation technique that presents probability distributions of possible outcomes based on an action (see Figure 6). The model runs thousands of randomly generated scenarios to discover the probability of any risk event occurring. Creating the probability distributions of the outcomes allows the decision maker to quantitatively assess the level of risk that comes with taking a particular decision and, as a result, select the decision that provides the best balance of benefit against risk.

From a risk management perspective, the Monte Carlo simulation provides a statistical method for determining the likelihood of multiple possible outcomes to any particular risk event based on repeated random sampling. By doing so, organizations can obtain a better understanding of the range and probability of possible financial repercussions. Based on the determined analysis, organizations can then assess whether existing controls are insufficient, at target, or overcompensating for the risk.

Looking at a risk analysis example, suppose the range of potential financial impact from the risk event ranges from $100,000 to $500,000. If the control in place is costing the organization less than the lower end of this range, the investment is likely merited given the potential high end of the financial risk potential. However, if, for instance, the organization is paying an insurance rate to cover this risk at the upper end of the impact potential ($450,000–500,000), then given the low probability of this level of implication, the organization could lower its risk premium and invest in mitigation for other risk areas.

FIGURE 6

Monte Carlo Risk Analysis



Source: IDC, 2022

Benefits of Advanced Risk Quantification

Qualitative risk identification is standard in most GRC platforms and has been effective in establishing risk analysis as a key component of a GRC strategy. However, qualitative risk analysis is limited in its capabilities to accurately assess enterprisewide risk with quantitative methods, providing a much more accurate risk assessment. By adding specific metric parameters, quantitative risk analysis provides a more precise and consistent evaluation of risk. When an organization applies metrics to measure the potential of a risk event and the impact to the organization, a more accurate assessment and response can be determined.

Qualitative risk heatmaps have the potential for significant risk misrepresentation, with green, yellow, and red scoring bands overlapping, making an accurate risk assessment difficult. For instance, while risk A might rank as a higher priority than another risk B, the actual potential damage to the organization is greater with risk B. The nebulous risk categorization in a heatmap approach to risk analysis prohibits an organization from accurately ranking top risks.

By giving risk a numerical value, organizations can compare risk across the organization, comparing apples to apples, providing a uniform view across disparate categories of risk. The ability to compare the impact of an ESG risk versus an operational risk or security risk for instance will provide much greater clarity in the organizations' risk landscape. Finally, by employing consistent metrics, a risk can be viewed in aggregate, adding the risk across all risk types and determining if it is acceptable. If risk is viewed in isolation, the true impact is missed, but if the strategic, financial, health and safety, environmental, and reputational risk can be viewed in aggregate, a much clearer assessment of impact can be determined.

Quantitative risk assessment also allows organizations retrospectively to evaluate the accuracy of their assessments and to improve estimates overtime. For instance, if an organization is anticipating a 10% chance for a risk to occur and the actual occurrence is 1%, then the organization can lower the risk occurrence estimate, which then translates to a lower remediation investment and a better allotment of resources.

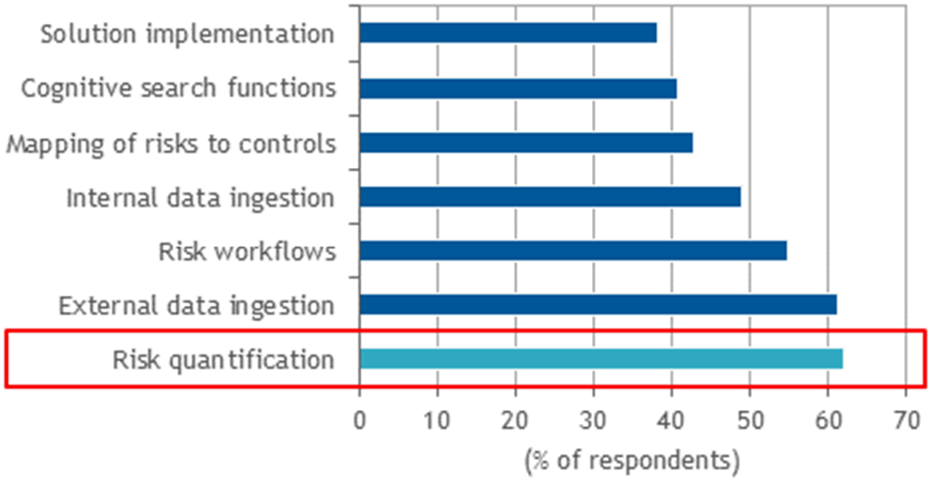
Ultimately, better risk quantification improves an organization's trust perception. By exhibiting strength in identifying risks, there will be greater trust in an organization's ability to remediate against risk. If an organization can accurately assess what the top risks are, they can demonstrate how those risks are being remediated through improved controls and changed behaviors. Transparency of risk and remediation improves organizational trust with all stakeholders including consumers, investors, partners, and internal stakeholders.

Demand for Advanced Risk Quantification

Risk quantification is one of the leading categories that organizations are seeking more support capability for from the GRC platform. According to IDC's November 2021 *GRC Maturity Survey,* risk quantification was the leading area to potentially benefit from automation to alleviate manual workload, error, and lack of skills (see Figure 7). Organizations are seeking ways to better understand their risk posture, across the entire landscape of risk, and have identified quantification tools as a critical capability in achieving that goal.

FIGURE 7

Top Areas for Automation



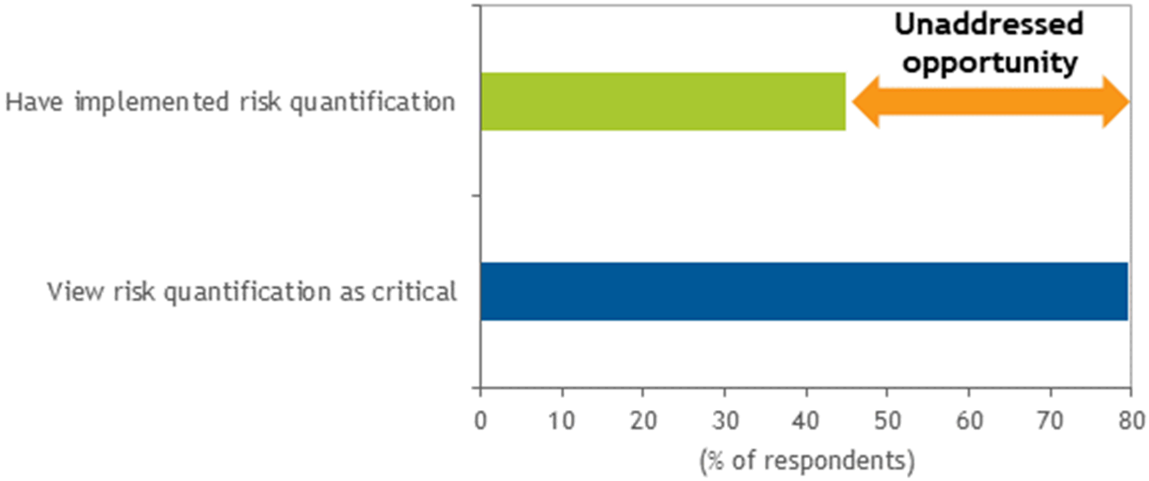
n = 206

Source: IDC's *GRC Maturity Survey,* November 2021

Currently, less than half of respondent organizations are utilizing risk quantification features built into their GRC platforms (see Figure 8). Compared with other advanced GRC features such as AI/chatbot support and API integration, adoption rates of risk quantification have a considerably higher use rate, which speaks both to the demand for this capability and the potentially simpler implementation. While heatmaps or risk matrixes are the most prevalent tool used for risk prioritization, this will transition significantly over the next several years.

FIGURE 8

Perceived Importance of Risk Quantification Versus Implementation



n = 206

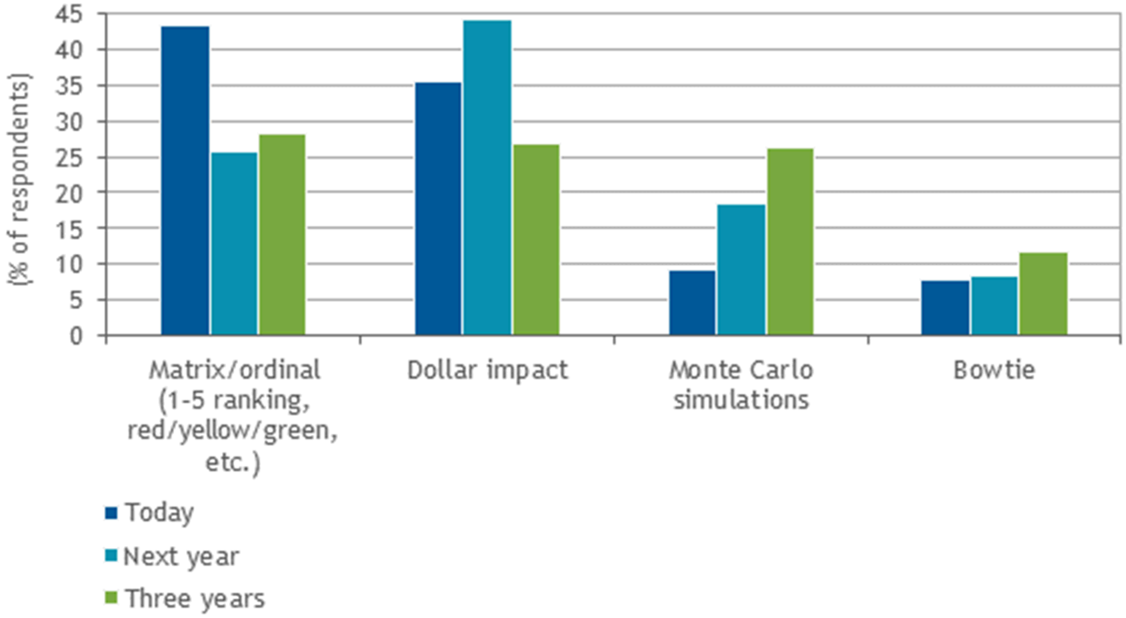
Source: IDC's *GRC Maturity Survey,* November 2021

With the growing risk landscape and the need for more granularity in risk assessment, organizations are planning to upscale their risk quantification practices. There will be a shift over the next three years in how organizations quantify risk. Roughly 40% of those companies using heatmap or matrix risk analysis will adopt a more advanced risk quantification methodology over the course of 2022. In the short term, migration will be relatively evenly divided between use of dollar impact analysis and Monte Carlo simulations. With over one-third of respondents already using dollar impact analysis, over the next year, it will become the primary mode of risk analysis, displacing matrix analysis.

Past 2022, however, respondents indicated a strong shift to Monte Carlo simulations. Again, roughly 40% of respondents intend to evolve their risk quantification programs over the 2023–2024 time frame, transitioning from a dollar impact approach to Monte Carlo simulations. Respondents indicated usage of bowtie analysis is also expected to increase but at a much slower rate (although bowtie analysis is sometimes invisibly integrated into the GRC solution and may be driving risk analysis without the user actively engaging in the analysis) (see Figure 9).

FIGURE 9

Migration of Risk Quantification Strategies Over a Three-Year Period



n = 206

Source: IDC's *GRC Maturity Survey,* November 2021

The migration to advanced risk quantification will look differently for different organizations based on their GRC maturity. More mature GRC organizations, defined by their adoption of point-specific GRC solutions and integration of risk management in organizational governance and strategy, will exhibit less of a migration away from matrix analysis, which will actually have fairly consistent adoption rates over the next three years, and more of a shift from dollar impact analysis to Monte Carlo simulation. Less mature organizations tend to be one or two years behind in this evolution, with a first phase transition from matrix to dollar impact in the coming year and a second phase from dollar impact to Monte Carlo in two or three years.

Innovation in Risk Quantification

Archer Insight

Archer is a market leader in integrated risk management solutions and, with a 20-year history, has led the market in introducing advanced quantification capabilities with the launch of Archer Insight in July 2021. With Insight, Archer is working to help clients prioritize risk management through heightened analytics, layering quantifiers to risk assessment and enabling the ability to report on potential dollar cost of various risks and make defensible business decisions.

Archer Insight is an embedded suite of risk quantification features that include multiple methods to apply quantitative metrics to the processes enabled by the platform. Archer Insight leverages multiple risk analysis techniques including bowtie analysis, Monte Carlo simulation, and risk aggregation and visualization capabilities. The solution applies quantitative analysis across a broad range of risk arenas

(IT/cybersecurity, enterprise, and operational) and risk impacts (financial, strategic, reputational, operational, environmental, and health/safety) to provide a more accurate assessment and ranking of organizational risk.

Archer Insight can be custom fit to the organization's needs and allows for a graduated approach to risk quantification. Users can elect simple (qualitative), standard, or strategic levels of quantification, all offering increasingly advanced analytical capabilities. All analysis is linked to bowtie analysis, which is performed intrinsically in the platform. Insight also enables users to drill down into risk based on the quantification analysis, pinpointing specific risks to identify where remediation efforts should be focused. Regardless of where the company is in its risk journey, Archer guides its clients through question/response-driven data input, making the complex an intuitive process.

MetricStream

MetricStream, a leading player in the GRC market with over 20 years of industry history, views risk quantification as an important tool in understanding and protecting against an organization's risk landscape. The company identifies risk quantification and its ability to put risk in monetary terms as a critical factor in developing the business case for prioritizing cyber-risk remediation and investments, and appropriately adjusting cyber-risk insurance based on this monetized risk assessment. Simple risk quantification was launched in the Enterprise version of MetricStream CyberGRC in August 2021 with the Brazos release and has undergone continuous development, with updated capabilities launched in the Colorado update (December 2021) as well as the Danube update (March 2022).

MetricStream's quantification supports multiple risk quantification models, including FAIR, to quantify enterprise and cyber-risk. Users can either leverage the embedded FAIR model and risk calculation formulas or can create their own models to best reflect the organization's risk priorities and tolerance. The platform also supports scenario-based simulations, including Monte Carlo simulation, to determine appropriate risk remediation given an organization's risk preferences.

The current risk quantification solution populates the analysis based on end-user assessments of risk and what maximum, minimum, and most likely results will be associated with a risk event. In addition, assessments will include a question/answer format to enable intuitive information collection. MetricStream believes that risk quantification will advance organizations to the highest maturity in risk management and enable companies to not only embrace but thrive on risk.

Mitratech

Alyne, a Mitratech company, is a Germany-based integrated GRC platform solution provider with a leading-edge risk identification and quantification framework. The Alyne risk analysis framework is a six-step process designed to systematically determine the prominent risks to an organization and to apply a cost analysis to those risks to better prioritize risk remediation. The process begins with defining the risk context: Often organizations haphazardly identify risks based on potential threats without applying context. The Alyne solution is grounded in a control framework, working from applied regulations to determine necessary controls to limit risk. These controls are the basis of the second phase, risk identification, where platform users are guided through a Risk Control Self-Assessment (RCSA) via an intuitive question-based risk review of each control. The platform then generates risk tree through an AI-driven analysis of the RCSA responses.

The next steps in the process are to qualify and manage risks. The risk trees are utilized to determine the deviation between the target and actual behavior; the larger the deviation, the more points that are applied. This potential impact is then assigned a probability, all of which occurs automatically through the Alyne platform. The platform also enables communication and collaboration across disparate teams in conducting the initial and ongoing risk analysis as well as in the remediation efforts.

The final phase of the Alyne risk analysis process is to quantify the risk and provide an aggregate organization risk view. The Alyne platform uses a guided risk calculator based on FAIR methodology (see description of FAIR provided previously). Based on inputted values of estimated maximum loss and historical lower and upper loss events, an expected loss projection is generated. Quantified individual risks can then be aggregated in a Monte Carlo simulation (see description provided previously), which, coupled with the organization's risk appetite, can determine the appropriate level of risk insurance or mitigation efforts that the organization should engage in.

SecurityScorecard

SecurityScorecard is an industry leader in cybersecurity ratings, providing actionable cyber-risk data and services throughout the customer life cycle. While perhaps best known for its cyber-risk ratings capabilities, SecurityScorecard launched a cyber-risk quantification capability in 2Q22 that will enable further insight into a company's risk position by translating cyber-risk into business context. The new solution, launched in partnership with RiskLens and ThreatConnect, is available to SecurityScorecard customers as an add-on to cyber-risk ratings.

The two partnerships that SecurityScorecard has engaged with for risk quantification allow customers to choose from multiple models, each grounded in SecurityScorecard's security posture data. While RiskLens and ThreatConnect both quantify risk into a universally understood financial metric, the approach is somewhat distinct. The Threatconnect RQ solution leverages industry frameworks such as CIS 18 and MITRE ATT&CK tactics to compute the most likely path an attacker will take, while RiskLens uses the FAIR analysis to quantify risk. Regardless of the model selected, users simply input industry sector and revenue for firmographic data, and based on the attack type selected, the models generate probability, predicted frequency, financial impact, and risk mitigation options.

The SecurityScorecard solution is unique from other solutions on the market, with principal differentiators being:

- **Dual model analysis:** The SecurityScorecard solution allows users to validate risk quantification outcomes through comparison across multiple models, providing flexibility in methodology as well as assurance in the output.
- **Depth of data:** SecurityScorecard, as an industry leader in cybersecurity ratings, has more than 60+ B vulnerabilities detected across 12+ M organizations continuously, providing a breadth of company security posture data availability that feeds the models that assumption-based models lack.
- **Actionability:** While the dollar metrics generated from risk quantification analysis is impactful, SecurityScorecard offers further support through recommended actions that aid the organization's leadership in investment and remediation decisions.

ADVICE FOR THE TECHNOLOGY SUPPLIER

As organizations are challenged with prioritizing an increasingly complex set of risk, GRC platform vendors can increase the solution value by overlaying advanced risk quantification capabilities. Risk quantification is an effective tool for translating risk into business terminology and thus can more effectively communicate risk needs to executive leadership. In considering risk quantification, evaluate the organization's risk landscape including new risk areas such as ESG and develop risk quantification techniques that will include nonfinancial risk measurement to account for other types of loss such as reputational or environmental impact. Furthermore, quantification methodologies should be guided and should incorporate cost of remediation in risk analysis. With a large share of organizations anticipating transitioning their risk quantification methodologies in the next one to three years, now is the time to begin introducing these capabilities.

LEARN MORE

Related Research

- *IDC Survey Spotlight: C-Level Heavily Involved in GRC Platform Selection* (IDC #US49034722, April 2022)
- *IDC Survey Spotlight: Organizations Seek Greater GRC Automation* (IDC #US49028922, April 2022)
- *Trust Events as GRC Implementation Instigators* (IDC #US48971122, April 2022)
- *Worldwide Environmental, Social, and Governance Risk Management Software Market Shares, 4Q21: Proliferation in the Vendor Landscape* (IDC #US48946322, April 2022)
- *Managing Environmental, Social, and Governance Risk to Support Business Resilience: GRC Response to Manage Emerging ESG Risk* (IDC #DR2022_T7_AC, March 2022)
- *GRC Maturity Profile* (IDC #US48812822, February 2022)
- *IDC Survey Spotlight: GRC Spending Growth Set to Continue in 2022* (IDC #US48742022, January 2022)
- *PRM (Political Risk Management): The Next Important Acronym in GRC?* (IDC #US48618621, January 2022)

Synopsis

This IDC Market Perspective explores different risk quantification methodologies as well as organizations' demand for quantification and their transition plans to more advanced strategies in the coming years. Advanced risk quantification is an emerging GRC platform feature that is highly beneficial in assessing risk.

"As organizations are faced with a growing risk landscape, risk quantification can amplify the benefits of a GRC platform by providing more pinpointed risk analysis," says Amy Cravens, research manager, Governance, Risk, and Compliance at IDC. "Most organizations anticipate upgrading their risk quantification capabilities in the next few years and will be seeking GRC platforms that have this capability."

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. IDC helps IT professionals, business executives, and the investment community make fact-based decisions on technology purchases and business strategy. More than 1,100 IDC analysts provide global, regional, and local expertise on technology and industry opportunities and trends in over 110 countries worldwide. For 50 years, IDC has provided strategic insights to help our clients achieve their key business objectives. IDC is a subsidiary of IDG, the world's leading technology media, research, and events company.

Global Headquarters

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

Copyright Notice

This IDC research document was published as part of an IDC continuous intelligence service, providing written research, analyst interactions, telebriefings, and conferences. 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/offices. Please contact the IDC Hotline at 800.343.4952, ext. 7988 (or +1.508.988.7988) or sales@idc.com 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.