E-BOOK

Governance, Risk, and Compliance The Definitive Guide

riskonnect.

Governance, risk, and compliance – popularly known as GRC – is a set of processes and procedures to help organizations achieve business objectives, address uncertainty, and act with integrity.

The basic purpose of GRC is to instill good business practices into everyday life. While not a new concept, GRC has grown in stature as risks have become more numerous, more complex, and more damaging.

GRC today spans multiple disciplines, including enterprise risk management, compliance, third-party risk management, internal audit, and more. While each discipline has its own priorities – and often its own way of doing things – GRC leaders are now recognizing the power of sharing data and intelligence to drive better results and build a stronger, more resilient organization.

This ebook will help you understand GRC and the value of an integrated approach so leaders can make smart, fast decisions to protect the organization.

TABLE OF CONTENTS

FORCES DRIVING AN INTEGRATED GRC PROGRAM

Today's risk landscape is more crowded, uncertain, and interconnected than ever. One risk – say a health and safety issue – can spill over to supply chain, business continuity, business relationships, IT security, workforce productivity, and more. At the same time, multiple forces are reshaping the risk terrain, including:

Rising pace and scope of regulatory compliance: Virtually every organization in every industry is facing an ever-growing and ever-changing number of regulations with which they must comply.

Accelerating digitization of risk management: The internet of things, third parties, blockchain ... every new point of access adds vulnerability and increases risk exponentially.

Growing importance of risk management in corporate strategy: Risk management is increasingly viewed not just as a tactical function, but as a valuable part of corporate strategy.

Evolving sophistication of analytics: Better analytics are delivering new levels of insight for data-driven decisions.

The influence of social media, constant threats of cyberattacks, and demands for greater transparency also are amping up the pressure on executives and boards to make wise decisions about risk at an accelerated pace with little room for error. Senior leaders, in turn, are relying on an increasing number of stakeholders from all corners of the organization to identify, manage, and reduce risk.

To steer the organization toward success, leaders need to access facts quickly – and use those facts to inform their response. A comprehensive GRC strategy can pave the way by removing silos and building collaboration for faster, more accurate, and more coordinated action.

GRC DEFINED

The acronym GRC was coined some two decades ago by OCEG as a shorthand reference to critical capabilities that integrate the governance, management, and assurance of performance, risk, and compliance activities.

GOVERNANCE

Aligning processes and actions with the organization's business goals

RISK

Identifying and addressing all of the organization's risks

COMPLIANCE

Ensuring all activities meet legal and regulatory requirements

In the past, organizations often approached governance, risk, and compliance as separate activities. Processes or systems frequently were created in response to a specific event – e.g., new regulations, litigation, a data breach, or audit finding – with little thought as to how that worked within the whole. The result was a maze of inefficiencies, redundancies, and inaccuracies, including:

- Lack of visibility into the complete risk landscape
- Conflicting actions
- Unnecessary complexity
- Inability to assess the cascading effects of risk

The reality is that there is plenty of overlap between governance, risk, and compliance. Each of the three disciplines creates information of value to the other two – and all three impact the same technologies, people, processes, and information. An organization, for instance, might be subject to a new data-privacy regulation (a compliance activity), while also holding itself to certain internal data-protection controls (a governance activity), both of which help mitigate cyber risk (a risk management activity).

When the three disciplines of GRC are managed separately, there is substantial duplication of tasks. Multiple teams end up spending hours collecting the same data – and hours more untangling email threads and spreadsheets just to begin analysis.

More damaging, disconnected processes and lack of transparency leave the organization blind to insights and interrelationships between risks, undermining the whole system by allowing gaps and redundancies of controls to go unnoticed. Siloed teams also have no understanding of how their particular domain influences the company's risk position as a whole or its overall success.

In short, managing GRC in separate silos is a lot of extra effort – and that effort produces very little reward. Without an integrated view of all GRC-related activities, it's nearly impossible to identify issues and inconsistencies. A damaging risk can easily slip by undetected and unaddressed because you couldn't gauge the full impact until it was too late.

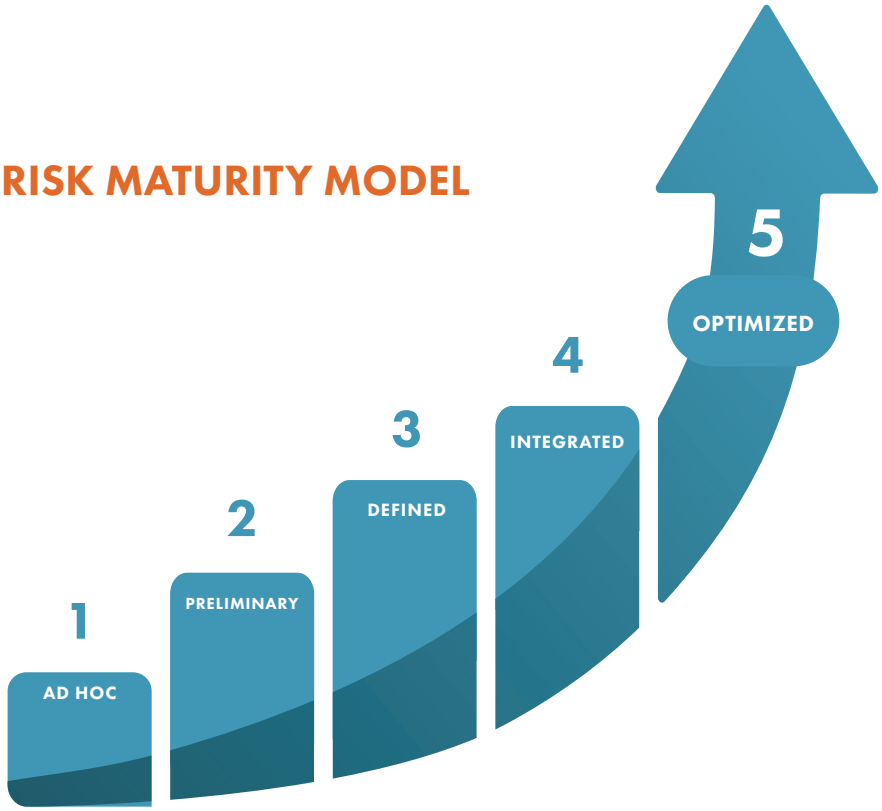
HOW TO ASSESS YOUR GRC MATURITY

Virtually every organization is engaged in risk management in some way, even if the risk management "system" is nascent. There is no single correct way to manage risk and compliance – but if your current system can't keep up with changing business needs, it might be time to reevaluate your approach. Even a world-class risk management system may have room for improvement given the ever-changing risk environment.

Using a risk maturity model that assesses your GRC position is an excellent way to identify where you are now. You then can compare your current state to where you want to be – and evaluate that against the value and cost of further investment in the management of risk. The more mature your GRC program, the more effective you will be in making decisions, taking the right risks, and achieving better outcomes for the organization.

Where does your organization fall on the continuum?

RISK MATURITY MODEL



Maturity Level	Description	Key Attributes
One	Ad hoc	The management of risk is undocumented, in flux, and depends on individual heroics.
Two	Preliminary	Risk is defined in different ways and managed in silos. Process discipline is unlikely to be rigorous.
Three	Defined	A common risk assessment/response framework is in place. An organization-wide view of risk is provided to executive leadership and the board in the form of a list of 'top' risks. Action plans are implemented in response to high-priority risks.
Four	Integrated	GRC activities are coordinated across business areas. Common risk management tools and processes are used where appropriate, with enterprise-wide risk monitoring, measurement, and reporting. Alternative responses are analyzed with scenario planning and other techniques, such as Monte Carlo simulation. Process metrics are in place. But the emphasis remains on managing a list of risks. Discussion of risk at executive committee and board levels is separate from the discussion of strategy and performance.
Five	Optimized	The focus shifts from managing a list of risks outside the context of enterprise objectives to managing for the successful achievement of objectives. The consideration of what might happen is embedded in strategic planning, capital allocation, and other processes, as well as in daily strategic and tactical decision-making. There is a reasonable level of assurance that decision-makers are taking the right level of the right risks necessary for success and not just to avoid failure. Early-warning systems exist to notify board and management both of specific risks above established risk appetite or risk-capacity thresholds – and where the likelihood of achieving enterprise objectives is less than acceptable. Reporting to management and the board integrates performance reporting (where we are now) and risk (what might happen) to project the likelihood of achieving each enterprise objective. Discussion of risk at top management and board levels (what might happen) is not separate from the discussion of strategy and performance.

HOW TO DO GRC THE RIGHT WAY

Effective GRC establishes the processes and systems that enable risk-aware decisions at every level. It's about giving all stakeholders access to the same high-quality, real-time data so they can share knowledge and collaborate on actions. A stand-out GRC approach:

- Defines a common vocabulary for all disciplines.
- Establishes one source of truth.
- Standardizes processes, practices, and policies.
- Facilitates communication and collaboration.

While heavily regulated industries like finance, energy, or healthcare are most in need of an integrated GRC solution, any organization – large or small, public or private – can benefit.

When GRC is done right, every part of the organization is aligned around the right objectives, actions, and controls to drive organizational success. Risk is no longer something to be feared, avoided, or minimized. Risk becomes a tool to create strategic value and elevate performance.

INTEGRATING AI INTO GRC

Artificial intelligence has the power to transform nearly every aspect of business – including GRC. Machine learning has long helped analyze data and predict outcomes. But the introduction of generative AI – like ChatGPT – takes that power to a new level.

For GRC, AI presents new opportunities to automate, augment, and accelerate work processes. It can expand your abilities and reach by reimagining how work gets done.

ChatGPT and other generative AI tools are built on large-language models trained on massive amounts of text scraped from the internet to learn the patterns of human language. The data supercharges its capabilities, allowing it to analyze data, find patterns, and devise solutions faster than any human could.

The potential impacts on GRC are wide. Already, AI is assisting with testing controls, reviewing evidence, and documenting findings. Companies are asking how AI can make board reporting faster, easier, and better.

AI can extend the reach of GRC by making associated tasks easier and faster. AI can even reduce the steps needed in a workflow. With more automation, you have fewer manual interactions, and those actions combine into a stronger workflow.

Generative AI is best at generating content. With just a few prompts, ChatGPT can spit out a draft in a matter of seconds. That initial draft may not be flawless, but it can probably bring you about 50% - 70% of the way there. Then you can refine it with substance, tone, and voice to fit your organization.

Think of AI as an accelerator. It can simplify complex data, translate lengthy and technical information (like regulations) into plain English, and eliminate tedious manual work. However, you still must review the response, adjust it, and take it forward.

Clear GRC use cases for ChatGPT include:

- **Risk statements and ratings**
- **IT product demand**
- **Policy drafts**
- **Control content**
- **Laws and regulations interpretation**
- **Potential controls**
- **Language translations**

This list is just a start. AI could easily be used to draft business continuity plans or get started with third-party risk. The potential is almost endless. It's all about understanding what you are trying to accomplish and where AI can provide a boost.

To be sure, generative AI is not without concerns. Everyone – from regulators to the inventors themselves – is trying to figure out the proper safeguards. Meantime, here are a few risks to watch out for:

Hallucinations – ChatGPT is programmed to provide a response, specifically the best next word in a sentence. In that process, it could make up the answer with no basis in fact. Always review and validate the response before you pass along information.

Bias – ChatGPT uses historical information to build new content. The problem is that what was acceptable in, for example, 1970, may not match today's standards. And vice versa. Ensure the content generated by ChatGPT is relevant and appropriate for your question and for your organization's policies and culture.

Data privacy and security – ChatGPT captures everything you type into the prompt and incorporates it into the model. Be cognizant of what information you are sharing outside of your organization. Protect yourself by defining proper use cases and your parameters for using them safely. ChatGPT also does not cite sources, making it difficult to verify the accuracy and reliability of the information provided.

THE VALUE OF GRC SOFTWARE

Integrated GRC technology unites processes and roles across the organization for seamless collaboration and intelligent insights that support data-driven decisions. It breaks down walls and provides transparency among stakeholders so you can understand the connections between individual risks, as well as how everything comes together as a whole. And you get huge gains in efficiency and accuracy, while simultaneously reducing costs.

With GRC software, you can:

- **Get more done.** Integrated GRC technology automates routine tasks, workflows, and follow-up, drastically reducing the number of human hours needed. And because all data is housed in one place for all to use, it eliminates double work, so you can double down on analysis.

- **Deal with endless change.** At last count, more than 61,000 regulatory alerts from 1,374 regulatory bodies worldwide were sent out in a single year – which is the equivalent of an average of 234 daily alerts. Integrated GRC software is designed not only to efficiently keep up with new regulations and laws but stay a step ahead of your compliance risk and the impact on the organization.

- **See who did what when.** Having all risk and compliance data in a single repository with robust tracking capabilities provides you with a clear audit trail documenting every modification.

- **Collaborate seamlessly.** Integrated GRC software brings all corporate and legal policies, procedures, and enterprise risks into one place that's easily accessible to all stakeholders. It breaks down silos by establishing consistent processes and controls across the organization. It also fosters a risk-aware culture and creates a sense of ownership where everyone plays a role in minimizing surprises.

- **See the big picture.** Integrated GRC software allows you to connect initiatives and data to uncover real insights about how one part of the program affects another and understand the full impact on the organization. With better insight into your program as a whole, you can better identify, prioritize, and address issues before they escalate into full-fledged problems.

- **Answer tough questions.** With streamlined processes, real-time data, and built-in analytics, integrated GRC software makes it fast and easy to create meaningful reports that inspire data-driven decisions. Dashboards give you continuous insight into the effectiveness of your programs. And advanced analytics augment human intelligence by pulling out new and more detailed information from the data. Having this level of insight also allows risk and compliance teams to offer strategic counsel and predictive insights to leadership.

WHAT TO CONSIDER WITH NEW GRC SOFTWARE

Strong, technology-enabled GRC programs can be a real competitive differentiator for organizations, and making the right choice is essential. With multiple technology options and no common definitions, knowing when you need a GRC solution – or which one you need – isn't easy.

Here are four questions to help define your focus when beginning the GRC software purchase process:

1. **What problems are you trying to solve?**
   What are your greatest concerns? Cyber risk? Trade compliance? Reputational impacts? Emerging risks?

   The first step in your GRC software purchasing journey is to understand your distinctive needs. It's easy to get hung up on finding and buying the "best" and most feature-rich product on the market. But if these solutions don't deliver the actionable intelligence you need to accomplish your goals, then they won't bring the value you need.

2. **Which features and functionalities are most important today?**
   Do you need an ERM solution, plus an audit tool? Or ERM software with added compliance capabilities? What about analytics and reporting capabilities? Should you go the with a single platform with multiple tools for better collaboration – or look for separate point solutions for each function?

   With so many solutions on the market, questions inevitably arise around the right combination of tools, features, and functions. The best plan of attack is to separate the must-haves from the nice-to-haves. Look at what you need today and what you'll likely need in the future. Buy the combination of tools that will deliver both the functionality you need right now and the scalability to carry you forward – within a reasonable budget.

3. **Who should be directly involved in the purchasing process?**
   Assemble a buying team based on three factors:
   - Who needs the software?
   - Who maintains the software?
   - Who controls the funds?

   Involving too many stakeholders can lead to buying tools you don't need or wasting money on multiple point solutions with overlapping features. You can't please everyone, so focus on addressing the practicalities of those who have skin in the game.

   It usually makes sense for risk management to lead the charge. The risk management team typically has the most visibility into what features and functions will accomplish the organization's priorities. This team also has the best view of how risk affects the entire organization and has the power to help everyone see and think about risk more uniformly.

4. **Who should advise?**
   Other departments and stakeholders get a voice, but not equal say. Internal audit, for instance, is a valuable advisor in the GRC software buying process. This department can verify that the solution under consideration has good controls, so the right people assess the right risks, and the information is reliable. Similarly, IT can offer important expertise around deployment, training, and integrations.

The best GRC solution enables organizations to understand what could happen and what can be done about it, so leadership can make fast and smart decisions to protect the organization.

READY TO DRAFT A GRC REQUEST FOR PROPOSAL? START HERE.

Selecting a GRC software solution can be overwhelming. Do you look at a raft of point solutions? Or do you look for a comprehensive solution with broad functionality to make it easy to share data and collaborate across the organization? Either way, an RFP is critical to finding the right partner.

Download the RFP template for a list of the most critical GRC-related questions to help guide your purchase process. The questions are presented in a downloadable spreadsheet, which can be easily modified to suit your own needs.

DOWNLOAD THE RFP TEMPLATE →

HOW TO EVALUATE GRC SOFTWARE

Keeping up with constantly changing risks, regulations, and policies takes a GRC technology solution that's flexible, scalable, and integrated. The right GRC software will add efficiency, prove effectiveness, and elevate the value of the risk management function to the organization. As you evaluate possible solutions, ask:

- **How easy is the technology to use?** Even the best GRC software is virtually useless if it's too difficult to use. And the easier it is to use, the more people will engage – and the higher the level of engagement.

- **How accessible is technology?** No one wants to be chained to a desk anymore. The software should be accessible anytime, from anywhere, from any device – laptop, desktop, tablet, or phone.

- **How secure is the system?** Make sure your data is protected with the highest end-to-end security that has been independently certified.

- **Where is risk and compliance information stored?** Cloud-based solutions are widely considered more secure than locally hosted systems. They also offer the advantage of automatic upgrades with minimal disruption.

- **How reliable is the system?** To keep users happy, you want a consistently reliable system that will give you the answers you need with virtually no wait time for queries, searches, or analytics.

- **How easy is it to make changes and updates?** You should be able to easily add fields, customize page layouts, and otherwise modify the configuration to accommodate changing regulations, new requirements, or evolving priorities – without the help of IT or your software vendor.

- **Is everything needed in one place?** You want to be able to access all relevant documentation, see the current status, and communicate across departments, functional areas, and locations without ever leaving the platform. And every activity needs to be automatically logged for a clear audit trail.

- **What can be automated?** An efficient solution automates workflows, assessments, attestations, alerts, and action plans so the risk and compliance team can focus on tasks that require human intelligence.

- **Does the technology integrate with other functions?** The value of GRC software skyrockets when it seamlessly integrates enterprise risk, compliance, third-party risk management, internal audit, and other risk management functions to give you an accurate picture of your total risk. With technology that's truly integrated, you can see how one risk event flows through the entire organization – and gauge the cumulative impact from compliance all the way to enterprise risk and beyond.

- **Can you extract the full story from your data?** Look for a GRC solution that provides data analytics, visualization, and insight into your risks and trends – and that shows you how those impact other risks and the organization overall.
- **Are dashboards available – and are they customizable?** Dashboards that can be customized allow everyone – from risk and compliance team members to the C-suite – to keep their fingers on the pulse of the metrics they care most about.
- **How easily can reports be created?** Nothing is more frustrating than having great data and no easy way to make sense of it. The most useful solutions offer point-and-click reporting for required regulatory submissions, a comprehensive overview for executives, and drill-down capabilities for tacticians.

Imagine the Power of Integration

Breaking down silos between enterprise risk, compliance, third-party risk management, and internal audit makes for more agile and coordinated response to risks that often overlap. And that's powerful.

Now imagine if you could follow that through to the insured side of the house. Technology that's truly integrated not only shows you the impact of your enterprise risk, compliance, third-party risk management, and internal audit risks – it shows you if those risks could lead to any claims, for instance, and the expected cost to resolve those claims. You'll finally be able to understand the full impact of any risk on the organization.

Imagine what you could do with that kind of power.

HOW TO SUCCESSFULLY IMPLEMENT GRC SOFTWARE

The success or failure of implementing GRC software rests largely on the strength of your partnership with your chosen vendor and how prepared you are in advance of the implementation. With that in mind, here are eight tips to put you on the path toward a successful software implementation:

1. **Define the finish line before you start.** Would you start a race without knowing where the finish line is? Of course not, since you might waste precious time and energy going in the wrong direction. Likewise, beginning a GRC software implementation project without clearly defining a finish line – that is, success criteria – can lead to delays, confusion, and scope creep. Start with well-defined business requirements that are fully aligned with your organization. Those requirements will drive the functional/technical specifications and user-acceptance testing criteria – and ultimately, will measure the success of your project.

2. **Don't automate a broken process.** Comfortable as you may be with your current workflows, designing the new GRC system around the old ways is a costly – yet common – mistake. Heavily customizing new GRC workflows to mimic your old ones can have grave implications, including extended implementation timelines, increased scope, future supportability issues, and inability to use other core (or future) standard functionality. Vendors invest countless hours and dollars to develop configurable standards based on best practices, so be open to learning how these standards can meet your business requirements.

3. **Communicate, communicate, communicate.** Don't assume the vendor will automatically know what you mean without you spelling it out. When it comes to a successful implementation, there is no such thing as too much communication. Discuss every possible issue in the early stages of an implementation – and don't be shy about asking questions or voicing concerns. Even seemingly small issues can have a big impact on the success of the implementation if they aren't addressed until the later stages, or worse, not addressed at all.

4. **Successful implementations are like a marriage.** Just like a marriage, your company and the vendor both need to contribute for the union to be successful. Communication and trust are essential, both parties need to be held accountable, and it's going to take hard work for the relationship to thrive. If one side hangs back on the sidelines, their needs may not get addressed properly, which can jeopardize implementation. And if the relationship gets too far out of balance, you could end up with a nasty divorce.

5. **Yes, you do need a designated project manager.** While an implementation can be successful without the PM role, your odds of success increase exponentially when a project manager is involved. Coordinating all resources and tasks during a large implementation can be an arduous task. Something as simple as scheduling a meeting for multiple people in separate organizations can prove difficult if the PM role is split between several implementation team members. Having a single point of contact centralizes communications, streamlines all implementation activities, and keeps everyone on track.

6. **Be realistic with your other time commitments.** Being part of an implementation team may be just one of many tasks on your plate. Be realistic about the time you have available to devote to the implementation process, and let the vendor – and team members – know about other commitments or conflicts you have as soon as the project schedule baseline is produced.

7. **Don't short-change the testing process.** As tempting as it may be to speed up testing to meet your deadline, this is not the place to cut corners. Bypassing or condensing integral user acceptance testing can set you up for mountains of post go-live issues, extra work, and delays to your business processes. Proper UAT takes time to do correctly – but the extra effort will save you from plenty of headaches down the road.

8. **Prepare for the unexpected**. No matter how diligent you are, it's virtually impossible to identify and prepare for every possible issue. Something unexpected is bound to happen, but the impact often depends more on how you react than on the issue itself. When an unexpected issue threatens to derail the implementation, work constructively with your team to tackle it head on and move forward. And if you chose the right vendor, together you can expertly manage whatever surprises come your way.

HOW TO BUILD A BUSINESS CASE FOR GRC SOFTWARE

Boards and the C-suite may recognize that GRC technology will provide better oversight and enhance risk and compliance overall – but still be reluctant to allocate budget. The challenge is defining and measuring value – cost, flexibility, efficiency, effectiveness – in a way that's meaningful enough to sway those holding the purse strings.

Integrated GRC software standardizes processes, streamlines data collection, and enforces security. Automating routine tasks allows the risk and compliance team to shift from collecting data to higher-value work like investigating and remediating issues. Built-in analytics and centralized data provide fresh, data-driven insights, identify interdependencies that otherwise would have gone unnoticed, and give you an early look at risk indicators that can be used to drive strategic vision.

Add to that real-time reporting that extracts the story from your data for better, faster decisions. Dashboards also allow continuous monitoring of key indicators and metrics. In short, integrated GRC software gives you hard data on the current status of your risk and compliance program, where your weaknesses are, and what needs to be done. Right at your fingertips.

Dollars – and Sense

While it's difficult to put an exact dollar figure on the ROI of integrated GRC software, there are ways to quantify the value.

For starters, evaluate staff resources that would be saved with greater efficiencies and tie that to a dollar value. For example, if automation saves you 20 hours per week for a salary that breaks down to, say, $50 per hour, then that's a savings of $1,000 per week for the business. Multiply that by the number of people and hours saved, and the impact of automation alone could be significant. Those extra hours can then be redirected to tasks that provide more strategic value to the organization.

As significant as that amount may be, the real value of GRC software lies in its ability to improve decision-making. You have a clear picture of what's happening, so you can confidently decide what risks are worth taking – and which are not.

But what will speak loudest to leadership? No surprises, for one. There is nothing the board and C-suite loathe more than being blindsided by something they should have – could have – known about.

An integrated GRC platform puts all risks on your radar, which minimizes surprises. And then there's visibility. With integrated GRC software, every risk is documented and presented within the context of other risks – as well as the organization's goals.

Top leaders are well aware that the organization's very survival may depend on their ability to get instant access to real-time risk data to inform hard strategic choices that will drive organizational success. And with a well-planned GRC strategy – supported by integrated GRC technology – you finally have both the visibility to see your risks and and the agility to dodge roadblocks to keep your destination routed straight to success.

ABOUT RISKONNECT

Riskonnect is the leading integrated risk management software solution provider. Our technology empowers organizations with the ability to anticipate, manage, and respond in real-time to strategic and operational risks across the extended enterprise.

More than 2,000 customers across six continents use our unique risk-correlation technology to gain previously unattainable insights that deliver better business outcomes. Riskonnect has more than 800 risk management experts in the Americas, Europe, and Asia.

Visit riskonnect.com to learn more – or schedule a meeting with our experts here.

CONNECT NOW →

RISKONNECT'S INTEGRATED RISK MANAGEMENT SOLUTIONS

- **Risk Management Information System**
- **Claims Administration**
- **Third-Party Risk Management**
- **Enterprise Risk Management**
- **Environmental, Social, Governance**
- **Business Continuity & Resilience**
- **Internal Audit**
- **Compliance**
- **Policy Management**
- **Project Risk**
- **Health & Safety**
- **Healthcare**

riskonnect.