



WHITE PAPER

# GOVERNANCE, RISK & COMPLIANCE: FROM NAYSAYERS TO BELIEVERS



As citizens of the world, we all interact with people every day — [80,000 people in a lifetime](#), by at least one measure. Many of these interactions involve buying and selling goods, and if you think about how long humans have been interacting this way, you can easily see why selling is such an important part of daily life.

Given all the buying and selling we do every day, each of us is bound to encounter a poor sales experience sooner or later—an experience of intent without integrity, or greed without grace. And that’s perhaps why sales has come to be seen by some as a less desirable profession than, say, medicine,

The truth is we’re all salespeople—whether we’re engaging on social media, protecting clients in the courtroom, prescribing medicine to a sick patient, teaching a schoolroom of children, or presenting to a room full of shareholders. We are all sales people in the sense that we are all responsible for offering ways to help solve others’ problems and positively influence their thinking.

And that includes the people in charge of governance, risk and compliance, or GRC.

The simple realisation that we all have something of value to sell to others is missing from many GRC teams. Risk managers, for example, may believe that their role is to tick boxes and develop complex spreadsheets to manage risks. Their teams can spend weeks and months preparing reports without ever proactively engaging with the business on opportunities that drive profit. In that sense, they’re simply not selling the value that risk and compliance can provide their organisation.

One of the biggest challenges for risk and compliance teams today is a lack of engagement with their businesses—something that’s been under increasing scrutiny in light of recent events involving misconduct and unethical behaviour in the financial services industry. No organisation or country is immune to the risk of misconduct. Closing what we call the “gap of grief” between these key parts of any organisation can help reduce that risk.

Misconduct is a symptom of several deficiencies, and the lack of collaboration and cohesion between the risk and compliance team and the rest of the business is a strong indicator of this. So what can risk and compliance professionals do to help bridge the gap and inspire everyone in the business to own risk?

We’ve developed a six-step plan to help sell the value of GRC in any organisation.

## **STEP 1: START WITH WHY**

The question we must ask ourselves is this: Why is GRC important to our organisation? The answer defines the benefit you provide to the organization. It will be the start of your sales pitch and the introduction to your education and training program, and it will live on as a statement of the collective ambition and purpose of your team.

## STEP 2: UNDERSTAND YOUR INTERNAL CUSTOMER

Many risk and compliance teams miss this critical step in their GRC program, yet it is arguably one of the most important factors for success. To sell the value of risk and compliance we must first understand who our customers are.

- Where are they located geographically? Is there a cultural dimension we'll need to consider in our training approach and communication style?
- What are the informal structures within the organisation?
- Who are the most influential people among our leaders, middle managers and rank-and-file employees?
- What are the expectations we have for these groups and individuals in our business with regard to GRC?
- What role does GRC play in their daily/weekly/monthly interactions?

These questions not only help formulate a plan to close the gap of grief, but also give organisations an idea of where they currently stand. The answers should provide a clear view of where the power centres are within your organisation and your level of operational maturity.

## STEP 3: UNDERSTAND THEIR CHALLENGES

Listening is the most important skill in selling anything. When attempting to solve deeply embedded and complex problems, we need to understand the challenges and their implications before we can propose a solution.

The lack of business engagement that's such a challenge for many a risk and compliance team is the very same challenge the team's business customers face. It's two sides of the same coin. Most organisations have strong GRC frameworks that were carefully developed with buy-in from all levels within the organisation. The widening gap comes from how the business operationalises these frameworks.

A few simple questions will help you understand the hurdles from the business perspective.

- What do you find most difficult about the activities the risk and compliance team regularly expects of you?
- Which activities take the most time? Do some of these time-consuming activities seem pointless to you?
- What are the implications of these activities for you and the organisation?
- What would you change about how we currently run these processes?
- What is working well in your interactions with the risk and compliance team?

Remember that you may be talking with people who have been doing things a certain way for so long, they may not realise they even have a problem. You may have to tailor your questions to help them discover this. Without a view of how things could improve, they may have simply accepted their current situation; it may take some deeper probing to enable them to question their existing beliefs. Remember, you're not selling ice to Eskimos—you're helping them find the fish below the surface of the ice.

## STEP 4: COMMUNICATE YOUR PURPOSE

Every pitch should start with why you do what you do. You want to win hearts before you win minds. Present your pitch with conviction and share your beliefs about what problems you intend to solve. Once people understand why you want to do something, you can start talking about what you'll do to achieve the outcome. Keep it simple to help them understand your pitch and how the changes you're proposing will benefit them.

Make sure your purpose and pitch align to the information you've already gathered about their challenges. Summarising your understanding of their needs shows that you listen and you understand. Remember to tailor your pitch based on the individual or group you're presenting to. You will be delegated to the person you sound like. GRC has many dimensions, and different levels within the organisation interact with these processes differently.

## STEP 5: PRESENT THE PLAN

This phase gives you an opportunity to be creative. Will you come up with an eight-step plan to close the GRC gap of grief? Will you develop a three-step plan for improving business engagement? Whatever your approach, this phase is important for moving from abstract idea to concrete plan.

How will you present the plan? Consider meeting with key executives individually to be sure you're answering their questions and meeting their concerns. Then target key groups within the organisation to present your plan, address the high level objectives of the solution and describe the benefits it will provide to each group.

## STEP 6: EXECUTE AND MEASURE

You've made your case. Now it's time to walk the walk. Let these questions guide you as you execute your plan.

- Who do you need to make the plan successful?
- How much time will you spend outside of "business as usual" activities?
- How will you measure success?
- What metric best represents improved engagement with the business?
- How often will you measure against these metrics, and who will receive the outputs?

An initiative in the GRC framework doesn't have an end date. You increase the organisation's profitability and drive operational excellence by solving problems on an ongoing basis. Measuring progress along the maturity scale is a great indicator to the business of the success of your initiative and the value that the risk and compliance team is providing to the organisation.

## GET STARTED NOW

Wondering what activities you can execute today that will sell the value of risk and compliance? Here are a few ideas to get you started.

- **Risk scorecards:** Scorecards demonstrate the power of simplicity in managing risk. They break down risk into a manageable and digestible format for executives and business units, delivering the information to help them make decisions about their appetite for risk.
- **Tone from the top:** Organisations with a positive risk culture have a strong, consistent tone from the top about the role of risk. When the head of the business accepts that risk management is key to profitability and sustainability, the impact goes far beyond what risk management teams can do on their own. Just like corporate social responsibility, risk needs airtime from the top.
- **Job descriptions:** Set the expectation early. In *Good to Great*, Jim Collins tells us that successful companies have “the right people on the bus.” In this case, the right people are those who understand that risk management is an important part of their role. (There’s also no better place to discuss this expectation than during the hiring process.)
- **Success stories:** Internal marketing of examples of good risk management in action is a good way to highlight and reward good behaviour, and provide an example to others. Highlighting success stories also sells the value of the risk management team in helping the organisation avoid all types of risks.
- **Regular training:** Employees are already expected to complete regular training for ethics, compliance and security. Risk management training should be another module of regular training and awareness.
- **Linking directly to remuneration:** Directly linking risk management to bonus payments is arguably the most effective way to integrate risk management into the corporate culture. If someone’s tempted to flout company ethics in pursuit of revenue and profitability, the fact that there’ll be no financial reward may be enough to prevent misconduct.

Risk management, like a map or compass, exists to help organisations steer the right course. It’s about striking the balance between profitability and doing right by customers, shareholders, partners and employees.

For more information on how RSA can help you sell your organisation on the business value of governance, risk and compliance, please reach out to your local representative.

## ABOUT RSA

RSA® Business-Driven Security™ solutions provide organizations with a unified approach to managing digital risk that hinges on integrated visibility, automated insights and coordinated actions. With solutions for rapid detection and response, user access control, consumer fraud protection and integrated risk management, RSA customers can thrive and continuously adapt to transformational change. For more information, visit [rsa.com](https://rsa.com).