FORRESTER®

For: Security & Risk Professionals

Build A Governance, Risk, And Compliance Strategy Worthy Of Business Consideration

by Renee Murphy, January 9, 2015

KEY TAKEAWAYS

GRC Programs Without A Clear Strategy Deserve To Be Kept In Isolation

If your GRC program responds frantically to incidents, audit findings, regulatory changes, and partner demands, then most likely you're simply transmitting that same chaos to the business, and they should ignore you. What's more, even if your team is effective, without a strategy in place, it's nearly impossible to show that your efforts have value.

You GRC Strategy Is Primarily About Keeping The Organization On Track

You will have specific goals for your GRC function, which may include elements such as the development of your team, relationships with other functions, and the breadth of impact your efforts have. However, the primary reason for your function's existence is to help your organization avoid being derailed as it strives to achieve its objectives.

You Need To Be Patient With The Maturity Of Your Program

Risk and compliance professionals have been asked to take on much more responsibility over the past 10 years. You and your peers have responded impressively; however, don't create undue pressure by taking on too much. Set practical goals for the next 12 months and show ongoing progress as you go. Momentum is essential if you want widespread support.

Build A Governance, Risk, And Compliance Strategy Worthy Of Business Consideration

Strategic Plan: The Governance, Risk, And Compliance Playbook

by Renee Murphy
with Christopher McClean and Claire O'Malley

WHY READ THIS REPORT

Governance, risk management, and compliance (GRC) are far too often positions of emergency response. What's worse, as you constantly rush to respond to new mandates, enforce policies, or pull together yet one more report, it's often impossible to track or demonstrate your positive effect on the business over time. To get your team and key stakeholders on board, and to show that all your efforts are helping your business perform better, you need a well-defined, documented, and widely visible GRC strategy. This document outlines the challenges you face without a strategy, best practice examples of companies that have successfully built one, and a checklist of elements necessary for your strategy to stand up to scrutiny at all levels of the business. This is an update of a previously published report; Forrester reviews and updates it periodically for continued relevance and accuracy.

Table Of Contents

Notes & Resources

In developing this report, Forrester drew from a wealth of analyst experience, insight, and research through advisory and inquiry discussions with end users, vendors, and regulators across industry sectors.

Related Research Documents

Maximize Business Performance With A World-Class GRC Program
May 16, 2014

Choose The Right Technologies To Support Your GRC Program
April 28, 2014

Benchmark The Performance Of Your GRC Program
February 20, 2014

FORRESTER®

GOVERNANCE, RISK, AND COMPLIANCE ARE NUISANCES WITHOUT A STRATEGY

Have you ever been through customs at JFK airport with a 2-hour layover? You have to claim your luggage, which takes about 1 hour, wait in the customs line for 30 minutes, and then recheck your luggage for your connecting flight, which takes another 20 minutes. After all that, you only have 10 minutes to get through security and to the gate, so if you want to make the last flight to Los Angeles that night, you have to run, hoping that you get there before they close the jetway door. The entire process is needlessly complicated and very time-consuming, and the value of all these steps is not apparent to you or the other airline customers. If your governance, risk, and compliance program doesn't have a well-defined strategy, this is likely how the majority of your business counterparts view your role in the work they do.

Reactive Programs Earn Their Stigma Of Business Inhibitor

Audit findings, incidents, regulatory rule changes, and evolving business demands all seem to require immediate attention, pulling your risk and compliance resources in many different directions at once. In this environment, if your team isn't operating from a shared set of principles and guidelines, it's impossible to coordinate efforts. Instead, you find yourself in a situation where:

- **External requests drive GRC decisions rather than business goals and needs.** It's now common for third parties to ask for your continuity plans, policy documents, control frameworks, and audit results. The instinct is to drop everything and bring all relevant resources together in response. For individual requests, this approach may be appropriate, but when you consider the sheer number of requests coming in from oversight bodies and business partners, it means you're routinely stopping productivity among IT, finance, legal, HR, and other core functions that otherwise would be keeping the business running smoothly.

- **Responses to events or issues are managed in a vacuum.** If a perceived threat or weakness arises, there may be a number of stakeholders with risk and compliance responsibilities who will step in with remediation action plans. Without guidelines for how such efforts are selected and carried out, the business may suffer. For example, after the loss of a device storing customer card data, you might see security require more training, audit conduct a surprise data and device inventory, compliance demand a lengthy report, and regulators ask for more transparency. If there is no coordination, productivity in this part of the business may suffer for months.

- **Your efforts end up providing little, if any, real value.** Companies are in business to win, serve, and retain customers. If your risk and compliance efforts are driven by fleeting affairs, you're missing opportunities to help your organization become more well-governed, risk-intelligent, and principled in its pursuit of these goals. Parts of your organization that are driven by successful customer interactions will see your requests as roadblocks.

Even Proficient Programs Appear Ineffective Out Of Context

Even if your team is talented enough to overcome such tangible shortcomings, your stakeholders will more likely perceive a GRC program without a plan as a failure, because there are no means to measure the results. Hours and resources spent will amount to nothing in their eyes if you can't articulate how the organization is better off than it was before your efforts began.

YOUR GRC STRATEGY KEEPS THE ORGANIZATION ON THE RIGHT COURSE

Building a strategy is, of course, more than a way to improve your governance, risk, and compliance functions — it's a way to help ensure that the entire organization meets its goals and objectives. This is true whether the scope of your GRC program is to support your IT organization, a specific business unit, or the enterprise as a whole.

Unexpected events can be distracting, disruptive, or disastrous to an organization as it strives to meet customer demands.[1] Risk and compliance professionals exist to make sure the right stakeholders can anticipate how such events may affect performance and allocate resources appropriately to stay on target. Critically, your top-level GRC objectives should rarely, if ever, differ from your organizational objectives.

Demonstrate Alignment To Gain Support And Participation

As manager of a GRC program or function, you have your own goals for how your group operates. Common GRC functional goals include extending program coverage (number of systems, locations, business units, etc.), improving documentation (of controls, risks, incidents, etc.), or expanding team capabilities (risk quantification, control automation, etc.).[2] However, your top-level objectives should focus on how you support the company.

For example, the head of vendor risk and compliance for a national retail company said her team's strategic plan ties all efforts back to the company's culture, which means their GRC program has to provide capabilities that fit their corporate goals of serving customers in a fast, friendly, and fun environment. If their GRC program is going to be successful, it can't have a reputation for being slow, demanding, and stodgy. Every GRC program should heed this advice and mesh with their culture, not buck against it.

Maintain Focus, But Allow Flexibility In The Midst Of Change

Without a doubt, your risk profile and your compliance obligations will change before you execute all elements of your strategy. Despite the data, insight, and analysis you pull together while planning, a single industry event or even a discussion might be all it takes for you to reconsider your initial assumptions.

Your strategic plan should have regular reviews and adjustment mechanisms built in to accommodate such changes. The goal is to find a balance that allows flexibility without losing your focus. One of the top oil and gas companies in the world accomplishes this with different levels of tracking for its risk strategies: Executives review progress reports monthly or bimonthly, and the audit committee reviews them annually to determine whether changes or adjustments are necessary. At one of the top global financial services firms, functional leaders individually define their own risk and compliance success metrics, capability assessments, and key risk indicators; the overall strategy is used to guide discussions and decisions about risk during monthly executive committee meetings.

A COMPLETE STRATEGY CONSIDERS MANY FACTORS, COVERS MANY FACETS

Because governance, risk, and compliance touch all aspects of your organization, building your GRC strategy will be understandably complicated.[3] Be wary of oversimplifying the process; one Forrester client whose organization has been investing heavily in creating a risk-aware culture and rolling out assessment tools confessed that his risk strategy was really just a set of the most critical risk categories that the company hoped to address over the next year. They could not describe what their end goals were, let alone how their efforts would help the business. Avoid this situation with a comprehensive plan.

A Complete Strategy Considers Many Factors

Your risk and compliance efforts need widespread support and participation, so show that you've taken input from a wide range of sources.[4] As you develop your plan, make sure you:

- **Map out your function's role in organizational performance.** Are you expected to help maintain a robust corporate brand, improve customer loyalty, strengthen corporate culture, or be a spokesperson in front of shareholders? Most likely, your highest-level stakeholders haven't described your role to that detail yet, so it's up to you. Before putting pen to paper, consider what value you could provide.

  For example, the head of information risk strategy for a global life sciences company views his team as a solutions provider that, among many other things, delivers industry loss data, risk trends, and proposed mitigation strategies proactively to management and project planning meetings. These stakeholders now see his team as a vital resource for the success of their initiatives.

- **Assess the gap between your current state and an achievable desired state.** You may not be able to position your role as an essential aspect of performance right away; be realistic about what you can achieve in the next year given existing skills and resources. For example, compliance professionals at a large US healthcare company used the Forrester GRC maturity model to determine their current state, and then focused their efforts to raise scores in the areas that align most closely with the team's strategic priorities, such as a risk-based approach to security initiatives and technology, to help them transition from a compliance- to a risk-based view of their technology strategies and projects.[5]

- **Anticipate changes in the external and internal environments.** Although incidents and audit findings may be impossible to predict, you should be able to look at trends or upcoming events that will require consideration. An aggressive acquisition strategy may require more frequent review of the strategic plan, and growing overseas competition might require greater involvement from your colleagues in business development (for partnership strategies) or government affairs (for lobbying strategies).

  The risk manager at a large insurer noted that there was a great amount of inherent risk in the firm's public relations and advertising strategies, and the firm was looking to its GRC program to assess and mitigate the risk of the extra exposure. Worrying that the extra press would make it a target for security-related incidents, the firm leveraged the risk program to find solutions to work more closely with PR and marketing to help anticipate those events and prepare for them before they became incidents.[6]

- **Envision the end results for your function and the organization as a whole.** Consider how much more impressive a home run is when the batter calls his shot first. Make sure your team and your key stakeholders know what you're aiming for, so when you achieve success your efforts get the recognition they deserve. Many risk managers are being creative in how they talk about risk to their stakeholders. Talking about risk management in terms of improving product and service quality or working with marketing professionals to effectively communicate the GRC strategy to the rest of the organization has proven successful for many clients.

A Complete Strategy Covers Many Facets

Now that you've considered the key elements that will guide development of your strategy, make sure your document encompasses sufficient information to hold up to broad scrutiny. A complete strategic plan will include:

- **Executive summary.** Briefly describe the purpose of the plan, key priorities, expected results, and benefits to the organization — in 2 minutes or less.

- **Mission and vision.** Explain why your team or function exists and the impact that it will have on the broader organization. The mission statement must be consistent with the vision and values of the enterprise as a whole and support the mission statement of the business.

- **Current state.** Using maturity scores, independent assessments, or simply descriptive context, describe the current state of governance, risk, and compliance in the organization. Provide a straightforward view of any perceived gaps or weaknesses.[7]

- **Goals and priorities.** Based on the current state and organizational goals, explain the specific things your team will accomplish in support of the mission and vision. You must prioritize and logically sequence each goal based on importance to the mission statement and feasibility with current and future capabilities, resources, and budgets.

- **Alignment.** Link your goals and priorities to those of the broader organization. If applicable, this may require multiple levels of alignment; for example, IT risk management priorities support IT service delivery objectives that in turn support business goals.

- **Roles and responsibilities.** Document the key stakeholders involved in carrying out the strategy, including those that may need to be involved in reviews and approvals of any changes. For especially complex and critical aspects of the strategy, consider a "RASCI" chart to document who is *responsible, accountable, supportive, consulted, and informed*.[8]

- **Success factors.** Make clear what is required for your strategy to be successful, such as board-level support, budget approval before a certain date, or the availability of resources from other relevant business functions.

- **Metrics and milestones.** Explain how the business should judge the success of your plan. Include metrics based on milestones when possible to give your initiatives the opportunity to build momentum and encourage more widespread support.[9] Also include review points or triggers to decide whether the strategy needs adjustment.

- **Expected results.** Describe the specific conditions that will result based on the successful execution of your strategy. Will you have higher customer satisfaction scores, fewer quality issues, or a more productive employee base? Once again, be sure these results demonstrate support for the organization as a whole.

RECOMMENDATIONS

EXPECT MATURITY TO TAKE TIME

Risk and compliance functions are currently asked to perform very complex and difficult tasks that were not part of the business five or 10 years ago. Professionals in the industry have done a remarkable job trying to keep up with expectations, but be careful not to add undue pressure by trying to climb the maturity ladder too quickly. Forrester recommends that you:

- **Balance practical and aspirational goals.** If your function is currently operating in isolation, it's unlikely you will gain widespread visibility and support within the year. Make a goal to become a service-oriented team first, or position yourself as a respected advisor for a single business unit. Demonstrating success in that model will convince others that your approach may be worthwhile to them.

- **Plan to show progress over time.** There will be a lot of skeptical eyes watching as you execute your strategy, and if it takes a full year before any tangible results, you will likely see detractors jumping ship before you reach the half-way mark. Set your milestones and metrics so that there's visible progress and value along the way.

- **Make it about the business, or expect a cold response.** You will ask business counterparts to participate in risk assessments, controls assessments, awareness surveys, training, and other key risk and compliance functions. If they get nothing from the engagement, they will need convincing every time; but if they get value from the process, they will be the ones inviting you to the table. For example, show how peer organizations successfully managed (or failed to manage) risks that they might face, or provide benchmarking data to show the level of control and oversight normally needed for initiatives like the one they are planning.

ENDNOTES

[1] Risk professionals cannot help businesses succeed without a clear strategy to win, serve, and retain customers. With countless delivery channels and untapped target customers, companies find themselves looking for competitive advantage with strategies to develop market-leading customer experiences. But if you want your company to truly become "customer-obsessed," it's not all about strategy — it's also about risk. Considering the amount of visibility and investment in customer-focused strategies and the amount of risk to the organization if they don't work, there is alarmingly little customer-related risk management going on. Without a better understanding of the risks that could impede successful customer engagement, far too many projects, and even many businesses, will fail. For more information, see the November 24, 2014, "Mitigate Risks In The Customer's Journey" report.

[2] Building the business case for GRC ideally starts at the highest levels of the organization, where objectives like improved oversight, greater control, and long-term value protection are critical. However, many of you will have to start with more basic ROI arguments upfront and demonstrate higher-level value over time. In these cases, Forrester recommends presenting the benefits of GRC value in the following three categories: efficiency, risk reduction, and strategic performance. For more information, see the December 10, 2014, "Build The Business Case For GRC" report.

[3] Your governance, risk, and compliance (GRC) efforts set the parameters by which your organization achieves performance and meets objectives, so it's no surprise that putting together your GRC plan for the next 12 months can be as difficult as strategic planning for the organization. This process should include careful consideration not just of internal drivers but also the key trends affecting other businesses or agencies in your industry. As you put your plans together, expect the biggest trends in 2015 to include more of a platform approach to GRC product implementations, emphasis on programs for content aggregation and process standardization, continued struggles to include risk earlier in decision cycles, a slow but steady evolution of controls automation, and increasing scrutiny on programs rather than results. For more information, see the January 6, 2015, "Measure GRC Performance To Show Processes And Data Reliability" report.

[4] Risk professionals often disregard organizational culture in the design, implementation, and communication of risk and compliance initiatives. While it's common to talk about issues like executive buy-in and training programs, risk professionals usually view these aspects of culture as either existing

or not; they don't fully evaluate them to understand how their existence (or lack thereof) impacts risk management and compliance. Without a well-tuned culture, where employees understand what's expected of them and act accordingly, policies and controls are easily thwarted. Employees will find loopholes and control gaps — sometimes with the best intentions, sometimes with the worst — that may expose you to substantial risks. For more information, see the December 9, 2014, "Cultivate Culture For Sustained GRC Performance" report.

[5] With risk and compliance issues now at the forefront of organizations today, the need to evaluate and strengthen governance, risk, and compliance (GRC) programs has never been greater. Whether your organization uses the term GRC or not, The Forrester GRC maturity model helps you establish all of the functions and components that comprise optimized, fully functional governance, risk management, and compliance efforts. For more information, see the December 12, 2014, "Assess Your GRC Program With Forrester's GRC Maturity Model" report.

[6] Governance, risk management, and compliance (GRC) programs have matured well over time. Unfortunately, this maturity has come mostly in response to new and changing regulations, which has resulted in programs that are narrowly focused on protecting employees, investors, consumers, and other stakeholders — not on protecting the business itself. Companies rarely fail because of poor financial controls, but they fail frequently due to their inability to understand and address disruptive technologies, market fluctuations, changing customer expectations, and competitive pressures. To really have a positive impact on business performance, expand the fundamentals of GRC to the aspects of your company that drive success with customer interactions, which will in turn drive growth and revenue for your company and better participation in GRC. For more information, see the June 11, 2014, "Extend Compliance And Risk Management To What Really Matters For Your Business" report.

[7] Whether your organization uses the term GRC or not, the Forrester GRC maturity model helps you establish all of the functions and components that comprise optimized, fully functional governance, risk management, and compliance efforts. At their most fundamental, these functions and components are everything required to help your organization maximize performance within acceptable levels of risk and within acceptable boundaries of internal and external compliance requirements. Leveraging this model, you can objectively assess your GRC efforts to identify areas of weakness as well as centers of excellence, and then outline a strategy to make appropriate improvements. The model consists of 14 functions and 59 components within the domains of oversight, technology, process, and people, each with detailed assessment criteria to provide a consistent and objective method of assessment. For more information, see the October 2, 2013, "The Forrester GRC Maturity Model" report.

[8] To build and maintain an effective GRC organization, outline the major tasks of your program and designate key stakeholders across the enterprise whom you will hold accountable when they don't meet expectations. Coupling the structure of Forrester's GRC Maturity Model and a detailed "responsible, accountable, supportive, consulted, informed" (RASCI) task assignment format, Forrester provides the requisite materials necessary to define your GRC program, designate roles, and set expectations for GRC participation across your organization. For more information, see the September 23, 2014, "Designate Clear Lines Of Risk And Compliance Accountability" report.

[9] Your business executives are focused on increasing revenue, streamlining operations, and delivering top-notch customer service. To do this, they're developing new products and services, expanding their geographic presence, identifying acquisition targets, and forming new partnerships. You must support these goals and communicate how effectively you do it. To that end, Forrester adapted seven metrics categories. For more information, see the July 18, 2011, "Don't Bore Your Executives — Speak To Them In A Language That They Understand" report.

About Forrester

A global research and advisory firm, Forrester inspires leaders, informs better decisions, and helps the world's top companies turn the complexity of change into business advantage. Our research-based insight and objective advice enable IT professionals to lead more successfully within IT and extend their impact beyond the traditional IT organization. Tailored to your individual role, our resources allow you to focus on important business issues — margin, speed, growth — first, technology second.

FOR MORE INFORMATION

To find out how Forrester Research can help you be successful every day, please contact the office nearest you, or visit us at www.forrester.com. For a complete list of worldwide locations, visit www.forrester.com/about.

CLIENT SUPPORT

For information on hard-copy or electronic reprints, please contact Client Support at +1 866.367.7378, +1 617.613.5730, or clientsupport@forrester.com. We offer quantity discounts and special pricing for academic and nonprofit institutions.

Forrester Focuses On Security & Risk Professionals

To help your firm capitalize on new business opportunities safely, you must ensure proper governance oversight to manage risk while optimizing security processes and technologies for future flexibility. Forrester's subject-matter expertise and deep understanding of your role will help you create forward-thinking strategies; weigh opportunity against risk; justify decisions; and optimize your individual, team, and corporate performance.

« **SEAN RHODES,** client persona representing Security & Risk Professionals

Forrester Research (Nasdaq: FORR) is a global research and advisory firm serving professionals in 13 key roles across three distinct client segments. Our clients face progressively complex business and technology decisions every day. To help them understand, strategize, and act upon opportunities brought by change, Forrester provides proprietary research, consumer and business data, custom consulting, events and online communities, and peer-to-peer executive programs. We guide leaders in business technology, marketing and strategy, and the technology industry through independent fact-based insight, ensuring their business success today and tomorrow.