NAVEX GLOBAL®

GRC BUYER'S GUIDE

5 Steps to Success

Identify, Assess & Mitigate Risk With an Integrated Governance, Risk and Compliance (GRC) Platform

Effective risk management requires comprehensive solutions. The current business landscape is increasingly defined by complex operations that include integrated technologies, processes and sociocultural trends resulting in progressively global markets, supply chains and vendors. This has contributed to a rapid expansion in the number and types of risks that organizations routinely face, as well as a complex regulatory environment that changes almost daily.

To meet these challenges, organizations require a Governance, Risk and Compliance (GRC) platform to help them manage business risk and to meet compliance obligations, as well as integrate risk management processes within their existing operations. The following guide provides businesses of all sizes with a base of knowledge about GRC platforms, as well as the information necessary to identify their needs, dispel common myths and misconceptions, and ask the right questions when choosing a solution.

Selecting and implementing a GRC platform requires investment and commitment. Organizations adopting an integrated approach to risk management must adapt their internal processes, provide support and training, and embrace changes to their status quo. However, if properly attuned and implemented, an integrated GRC platform will help businesses accurately assess and centrally manage multiple risk disciplines – resulting in streamlined processes, improved decision making and a stronger, more resilient business.

Contents

1 Understanding GRC

Understanding GRC

Simply defined, GRC is a coordinated and integrated strategy for corporate governance, enterprise-wide risk management, and compliance with regulatory and industry requirements. Organizations have been implementing GRC strategies for years. They do this to improve quality processes, assess and manage risk and control activities, as well as comply with environmental, safety and other industry-specific regulations. However, efforts have often suffered from organizational silos, a focus on proximal needs, and reliance on point solutions. Utilizing GRC as a strategy can enable a business to make informed decisions that fundamentally change the way it manages risk and compliance.

Manual vs. integrated approach

Most companies are structured as departments or silos. While this approach may be effective for some business practices such as production, risk management activities require collaboration across departments or working with vendors that are oceans apart. Businesses that are not leveraging a GRC platform are often unable to effectively automate their processes, relying on manual tools and conventions like spreadsheets, word processing documents and emails, or by adapting shared networks like SharePoint. With a proper GRC platform, however, organizations can integrate risk management activities to better manage risk and support cross-departmental collaboration.

Industries ideal for GRC

Any industry facing a mountain of regulations would find value in using a GRC platform. Three industries that are heavily regulated have spearheaded GRC platform adoption to date -- healthcare, finance and energy. All three have regulations that are challenging to comply with, such as HIPAA, FINRA and NERC. That said, every industry has regulations to comply with and risks to manage that would benefit from using a GRC platform.

Conduct a Preliminary Analysis

Implementing a GRC platform within your organization is not easy, but it is worthwhile with significant long-term benefits. The more you learn how to operationalize a GRC platform, the more you'll be equipped to lead your organization in procuring a GRC solution. Begin by conducting the following initial tasks:

Time a compliance or risk management activity

Time and record how long it takes to complete an activity like investigating a vulnerability or assessing risk to a third party. From one activity, you can extrapolate to gain an understanding of work hours spent or resources needed. This data will be indispensable when proving the case for GRC to management.

Benchmark your organization

Conduct an informal study of comparable organizations' best practices to use as a measure against your own processes and procedures. Survey your peers and search for information on social networks, podcasts, webinars, e-newsletters, and more.

Research GRC

In addition to materials available on the **Lockpath** website, an excellent additional resource is Richard M. Steinberg's **Governance, Risk Management and Compliance.** The book is written for senior executives and board members and describes how to ensure companies incorporate the necessary risk management processes, organization, and technology to accomplish strategic goals.

2 Assessing Your GRC Maturity

Assessing Your GRC Maturity

Knowing where you are is essential to embracing risk. Most companies have some risk management processes in place. But as business needs change, current processes may impede progress. Conducting a comprehensive review of your organization's current policies and procedures is a critical first step in replacing assumption with assessment.

The assessment process typically begins with an articulation and understanding of the motivations driving change. Most organizations that look to change do so for one of three reasons:

1. Current processes cannot scale to meet future needs.
2. Someone more senior – typically an executive or board member – has requested the organization consider a GRC platform.
3. A compliance failure of some type has occurred. The proper course of action is to consider all possibilities in terms of risk and opportunity while keeping your goal in mind.

Point solution vs. GRC platform

A comprehensive assessment takes into account needs across the organization. Often, departments managing a single program like policy management or SOX compliance can gravitate toward point solutions. However, your assessment should consider how your risk management policies and procedures impact others throughout the company. A GRC platform connects distributed data sources and keeps everyone involved informed.

Highly integrated

Companies with mature GRC programs are highly integrated. They see risk for what it is – impacting the entire enterprise, not just one department. They view compliance as a business function that impacts customers, vendors, suppliers and auditors, among others. A GRC platform provides businesses structured as silos visibility across the organization.

Discover Your GRC Maturity

Need help determining which type of solution fits your GRC maturity? **Request a meeting** with one of our GRC experts.

What proficiency level best describes your GRC maturity?

Expert

Experienced, plus leverages a GRC platform to continually integrate risk management processes enterprise-wide

Experienced

Rely on a GRC platform to integrate compliance and risk management functions

Intermediate

Use a GRC platform to perform one or two compliance activities

Beginner

Use manual processes like Excel, Word, email and SharePoint

By 2021, more than 50% of large enterprises will use an integrated risk management solution set to provide better decision-making capabilities.[(2)]

[2] Gartner.com

Putting Guidance Into Action

With your assessment complete and your GRC maturity determined, you will now need to prepare your organization for change. Take the following steps to help secure support for GRC platform adoption:

Construct and present a comprehensive risk profile

A GRC platform can give you a holistic view of company risk, as well as a focus on specific compliance and risk management activities. Identify and work with key individuals within your organization to develop a vision for your program as well as strategically think around major steps.

Secure leadership buy-in

Maturing your GRC program is a major initiative that benefits from leadership involvement. Having a senior level executive supporting your efforts can help promote GRC adoption and ease disruption.

Turn risk into a competitive advantage

A GRC platform manages risk enterprise-wide and brings clarity to the complexity of compliance, freeing the business to focus on value creating activities. With risks managed, your business can take on appropriate risks as you grow.

3 Asking the Right GRC Questions

Asking the Right GRC Questions

Asking the right questions is key to selecting a GRC platform. Understanding how software will adapt to your internal processes, as well as the level of vendor support you can expect, are critical when evaluating the purchase of any solution. When selecting a GRC platform, asking the right question lowers your risk and increases the favorability of the desired outcome. Important questions include:

What or who is driving the need for a GRC platform?

Determining what or who prompted the search for GRC platforms is revealing for fit and other factors like time to implementation. Typically, there are three forces at work:

1. The current solution can no longer meet the demand.
2. An executive or board member requested the search.
3. A compliance failure has occurred.

How are you going to support your GRC platform?

A GRC platform should integrate with your organization's processes. As such, you'll need to consider how you will support the platform: Will you need an infrastructure team comprised of compliance and risk management staff, IT and GRC champions? How will you train staff on using the platform? Knowing what is necessary to support each potential GRC platform is critical to success.

Where are you now?

Knowing where you are helps you strategize where you need to be. Have you purchased a GRC platform before? Are you moving away from a point solution like policy management software? Answers to questions like these will help determine the priorities, features, and requirements most important to you.

How responsive is the customer support?

As a business, you know the lengths your company will go to keep a key customer happy. What happens when you are the customer? Do you receive exceptional service? Do they go above and beyond? With any GRC platform, ask about their approach to customer support and request their methodologies.

GRC Question Checklist

Internal Questions

- □ What is driving the need (for a GRC platform/solution)?
- □ Who at your organization is driving the call to consider GRC?
- □ Where are you now (GRC maturity)?
- □ How are you going to support your GRC platform - initially and ongoing?
- □ Do you have a specific use case or regulation you are trying to solve?

Implementation Questions

- □ How many users will use the GRC platform?
- □ How long will it take to implement the solution and have it functional?
- □ Does the GRC platform have unwanted features that require additional consulting hours to remove?
- □ Have you budgeted for internal training on how to use the GRC platform?
- □ Do you see this as a one and done project or part of a larger initiative?

Platform Questions

- □ How do I get information/data into the GRC platform?
- □ What can I do with the data once it is in the GRC platform?
- □ Does the GRC platform require programming knowledge to fully utilize its functionality?
- □ What reporting options does the GRC platform have?
- □ What type of support, if any, comes with the platform?

Developing Your Questioning Mind

Asking is knowing. And what you know is critical when selecting a GRC platform. To help you, here are three resources:

Knowledge is Power

Download the Sample RFP for a GRC Platform. This Excel document will equip you with the standard and some specific questions. Use it when requesting proposals from GRC vendors.

Consult with GRC experts

The GRC industry has several credible sources for guidance on GRC platforms and integrated risk management processes, including Crowe, Deloitte, EY, and PwC. Before you procure a platform, it is a good idea to research and speak with consultants who have the requisite expertise.

Create a GRC Bookmark Toolbar

Many excellent GRC resources are currently available online. Add these sites to your daily browsing. Here is a partial listing of websites covering compliance, information security, and privacy: complianceweek.com, cio.com, darkreading.com, isaca.org, ponemon.org.

4 Dispelling GRC Platform Myths

Dispelling Common GRC Myths & Misconceptions

Solutions that are as complex and transformative as a GRC platform are easily misunderstood. Incomplete facts and limited exposure to these technologies can too often result in misconceptions. Sometimes these assume a life of their own, transforming simple misunderstandings into myths. Here are three of the biggest myths you'll encounter when procuring a GRC platform.

Myth 1: There is no risk in using a free GRC solution

Truth: Beware of vendors who offer compliance and risk management capabilities or add-ons for free. You are likely to spend more on additional tools, professional services engagements and staff to support the resulting piecemeal system than you would on a GRC platform that has long-term value.

Myth 2: This GRC platform can automate all your processes

Truth: While GRC platforms can automate processes, much has to happen first, including documenting your processes and configuring the platform. Even then, not everything is automated. Best practice is to start small with automating processes and add on later.

Myth 3: GRC platforms are ready to go once the software installs

Truth: A lot must also occur after you buy a GRC platform for it to perform as advertised. Configuring it to your business processes, importing data, building out reports, and offering training and support are essential for a GRC platform to be a catalyst for your company. When these aspects are factored in, the platform should provide visibility across the company, effectively integrate risk management practices, and empower compliance activities.

Why Excel doesn't excel with GRC

Microsoft Excel is a veritable workhorse inside organizations. Because of that, Excel spreadsheets are often relied on for compliance and risk management. While your workforce may know how to use Excel, it is manually intensive, and ill-suited to the GRC requirements of collaboration across departments and locations, archiving, automation, version tracking, history reporting and more.

600,000
500,000
400,000
300,000
200,000
100,000
PROFIT
1
6

Myths Impeding Progress

Here are a few tips to help dispel the GRC myths that can prevent your company from buying a GRC platform or maturing your program:

Calculate ROI of using a GRC platform

It is one thing to tout the benefits of GRC over the status quo. It is quite another to show a return on investment. Access this **data sheet** for computing ROI with a GRC platform.

Survey stakeholders about GRC

You know who you will need on your side to make a GRC goal or program a reality. A survey directed at stakeholders (executives, the board) can be revealing in awareness of GRC and potential hurdles you'll need to overcome. Knowing is essential to solving.

Compel with a GRC use case study

A case study is compelling because the company profiled has a similar challenge to your own. Executives and the board can relate to the case study format of: problem, solution, and result.

5 Justifying a GRC Platform

Justifying a GRC Platform

As a GRC champion, you will need to justify your request for a GRC platform to decision makers in order to secure funding and the necessary support. Compelling reasons for a GRC platform include:

A GRC platform will help our company better manage risk

GRC platforms come in many shapes and sizes. If your compliance staff is small, be aware of what the platform requires and what your department can take on. Look for a GRC platform that fits your processes, scales, and does not require coding or excessive customization.

A GRC platform will enable us to do more with less

Businesses of all sizes and budgets face resource constraints. Fortunately, once a GRC platform is up and running, it saves time and increases efficiency. With the productivity gains from a GRC platform, businesses can do more with less.

A GRC platform equips the company to reach new heights

The right GRC platform sets your company up for success. It gives you visibility across the organization, which can be invaluable when the company grows, adds vendors, enters a joint venture, or expands internationally. Visibility is critical to risk management.

Turn Risk Management into a Competitive Advantage

Risk management is a multifaceted and complex discipline. Advance your learning in this recorded webinar on turning risk into a competitive advantage. Three success stories are profiled. Watch now or at your leisure.

Making the right decision takes teamwork and commitment

Whether moving from spreadsheets to a GRC platform or maturing GRC processes, risk and compliance professionals need to generate support, set expectations, and advocate consistently. When implementing an integrated risk management solution, remember the following:

Form a GRC team

Implementing an effective GRC platform requires support across departments as well as from senior management. Seek advocates among executives, department heads, and coworkers committed to doing governance, risk management, and compliance the right way.

Research your GRC options & set expectations

Always be sure to verify vendor claims. Find a GRC platform that fits your company, vetting it through sources that are independent, unbiased, and reputable. Understand and communicate that results won't be immediate. Invest not just in the platform but also in education and training that will help ensure success.

Make a bottom-line case

Making a case for a GRC platform is key. Company executives want to know the bottom-line impact before making the investment. To learn more, download the data sheet, Estimating ROI from a GRC platform.

Profiles of GRC Success

Learn how leading companies are using GRC platforms for integrated risk management.

● IT RISK MANAGEMENT

A hugely successful mobile game developer manages its IT risks with a GRC platform, everything from correlating scan data to reporting on vulnerabilities and policy adherence.

● VENDOR RISK MANAGEMENT

A multi-billion-dollar retailer uses a GRC platform to manage its vendor risk program - from performing risk assessments on hundreds of vendors to auto-scoring of risk profiles.

● AUDIT MANAGEMENT

A major health insurer relies on a GRC platform to be audit ready. The internal audit team uses the platform to document and track all phases of the audit cycle as well as avoid HIPAA fines.

● **BUSINESS CONTINUITY MANAGEMENT & PLANNING**

A Fortune 1000 payment processor configured a GRC platform to create and test its continuity plans, from business impact analysis and workflows to collaboration between stakeholders.

● **OPERATIONAL RISK MANAGEMENT**

A Fortune 1000 public utility uses a GRC platform to manage operational risk, including policy management, incident resolution, KRI monitoring, and reporting.

● **POLICY & COMPLIANCE MANAGEMENT**

A global industrial manufacturer encountered regulatory headwinds in China. A GRC platform helps the company comply with new and existing regulations and manage all the details.

NAVEX GLOBAL®

Learn more about the Lockpath GRC Platform from NAVEX Global.

Info@lockpath.com | 913.601.4800 | lockpath.com