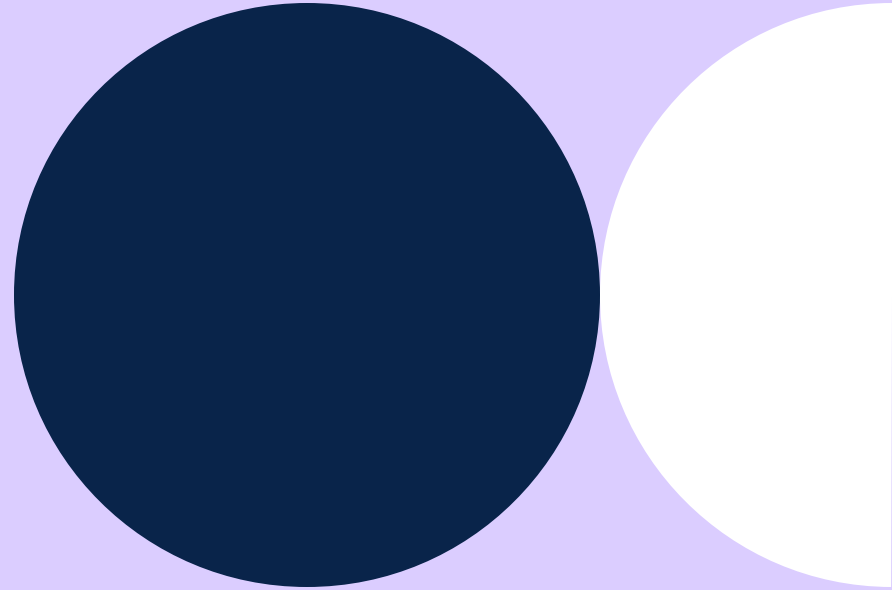


---

# GRC Buying Guide



# Contents

---

01. Knowing When to Employ a GRC

---

02. Baseline Expectations of a Quality GRC

---

03. What should I ask of GRC Vendors

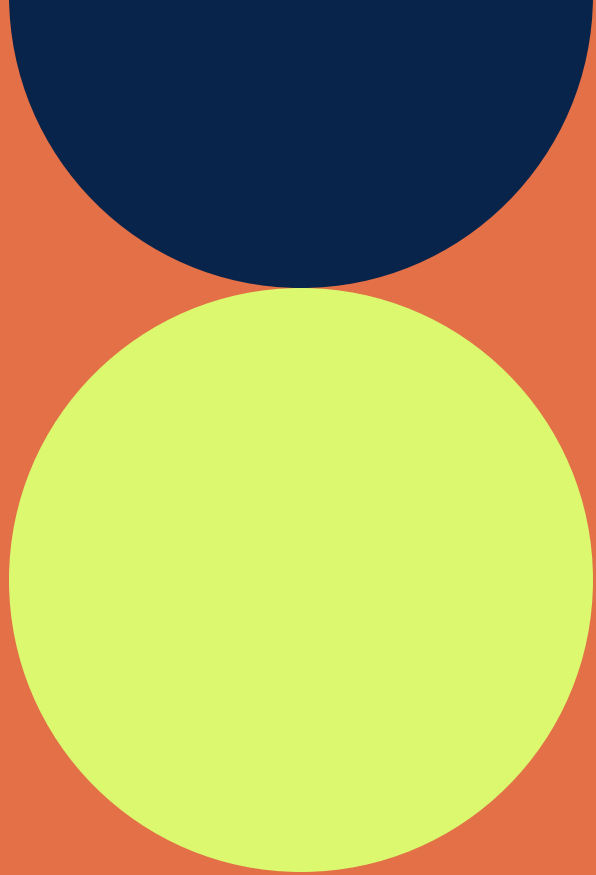
---

04. Calculations ROI and building your Business Justification

## Introduction

In today's challenging times, every organization is faced with what may seem like insurmountable difficulties; there are social and geopolitical considerations, supply chain insecurity, a high velocity of regulatory changes, economic volatility, and threats of all kinds. Even the strongest organizations find it challenging to stay competitive and accelerate growth.

If not governed effectively, these organizations' risk exposure grows, and business agility declines. Meeting the challenge requires a robust GRC solution that can keep pace with the growing external risks and the organization's needs while enabling it to meet the overarching business objectives.



01

---

## Knowing When to Employ a GRC

# Discern When to Employ a GRC

GRC adoption is not for the faint of heart and why it's easy to fall back on the 'ole spreadsheet. Timing it accurately should be the result of proper planning and a thorough assessment of your organization's maturity.



Determine the  
business objectives



Know your regulatory  
obligations



Define and document  
your current processes



Understand your  
reporting requirements

# Determine the business objectives



Understanding the business objectives – knowing your company's short- and long-term goals will help you define the scope of your requirements and build the business justification for bringing in a new technology.

Here it's important that you don't speculate or make assumptions. Rather, ask to meet with your CEO and explain the importance of a full understanding where the business is going and conversely what that means for risk exposure or regulatory obligations. In fact, don't be afraid to ask to participate in a board meeting and then use the opportunity to convey that you are working in the interest of the organization.

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.

You should also use this as an opportunity to build a business rapport with the extended management team and start preparing them for the inevitable process changes that will come with the implementation of your selected GRC platform.

# Know your regulatory obligations



Know your regulatory obligations – whether resulting from your time spent with your board executives or otherwise, you should have a strong grasp of what regulations your business is subject to. Granularity matters here, if you aren't assessing with precision, it's easy to wade into a sea of unnecessary requirements. Your specific requirements will vary, depending largely on your industry and type of business.

Also, consider adopting a Risk Management Framework (RMF) and self-regulating to that framework. An RMF is a specialized structure used to manage an organization's level of risk. A sound RMF should include five main components: risk identification, risk measurement & assessment, risk mitigation, risk reporting & monitoring, and risk governance. There are many RMF's available, and ultimately, your choice should align with your business model. As it is unlikely there'll be a "perfect fit" framework, look for alignment, not a direct match. And don't be afraid to adopt a derivative of a framework.

# Define and document your current processes



Define and document your current processes – good documentation is a prerequisite in the successful implementation of risk management as it acts both as a delivery and message mechanism.

Your documentation should reflect a comprehensive inventory of the risk management processes you know to be in place currently. Once you've inventoried and documented your processes, your next step should be to rate what you perceive the maturity level of each process to be: initial, repeatable, defined, capable or efficient.

This is a critical prerequisite for a GRC implementation as it will provide the roadmap for how your platform of choice will be configured.



# Understand your reporting requirements



Understand your reporting requirements – effective risk reporting is fundamental to a strong compliance program and, frankly, crucial to a risk practitioners' job security.

A risk report should convey information about the organization's current risk. It should include critical risks as well as emerging risks. Critical risks are ones that, if realized, could cause dire consequences to the organization. While emerging risks are ones that could be problematic in the future, if not monitored closely.

A lack of quality risk reporting in the organization, leaves the board ill-equipped in determining the efficacy of the risk management systems in place. Risk reporting also enables the board to offer strategic guidance to the organization. Further, a management team that has valuable risk information is better able to drive operational improvements, to better support the business's objectives.

A risk report should include the following information:

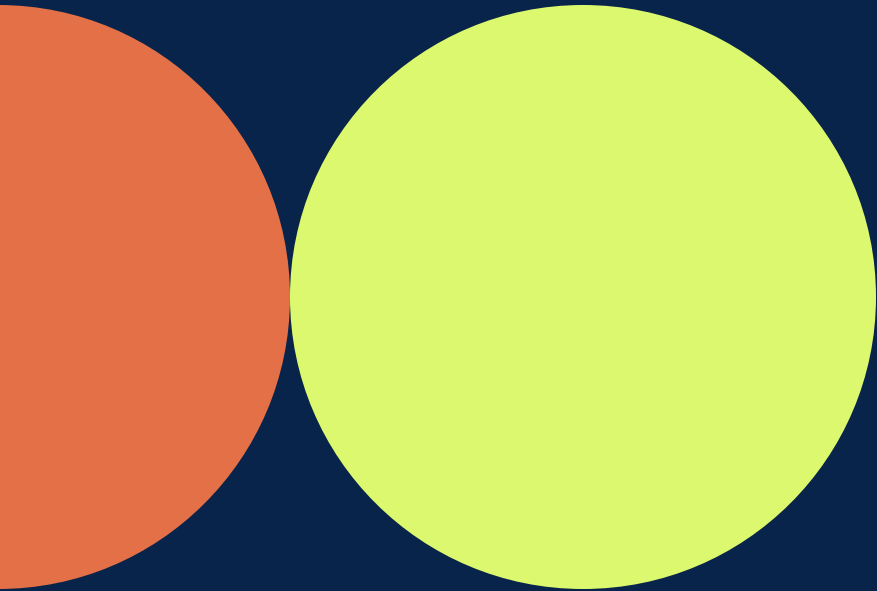
As previously mentioned, a risk report should include critical and emerging risks as a baseline. However, you may also consider including data privacy rules for markets where your company has expansion plans or government contracting rules if you're starting to bid on government contracts. Think expansively here and ensure that the report considers both short- and long-term growth objectives.

Ultimately, the broader you define possible emerging or critical risks, the better you'll be able to identify the ones that should go into your report.

Finally, an effective report maps out a plan of action or poses questions that the reader needs to answer. It involves the reader, by reassuring them that a plan exists to bring risk under control.

Interested in learning more  
about effective risk reporting?

Check out our blog [here](#).



02

---

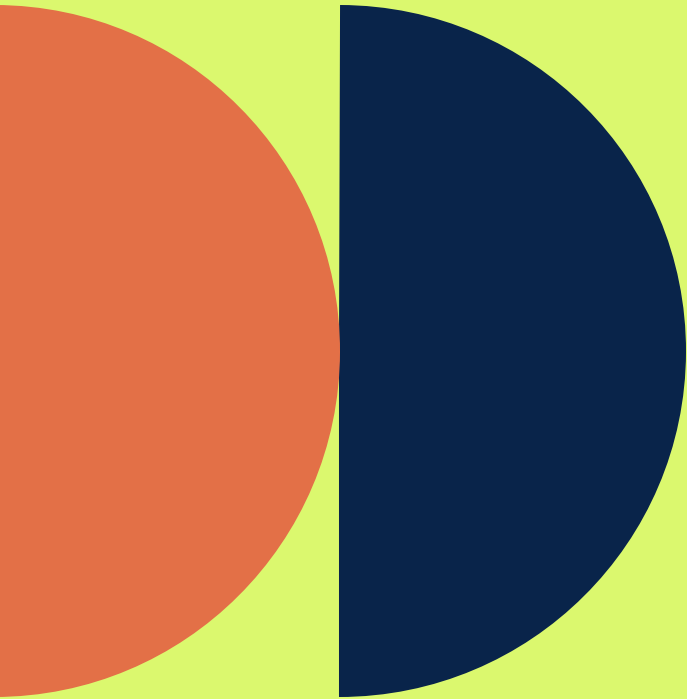
## Baseline Expectations of a Quality GRC

# Baseline Expectations of a Quality GRC

Enterprise GRC Platforms deliver a range of cross-department functionality across functional areas into an integrated technology ecosystem. For some, this is a single GRC platform for the entire organization. For others, it is a GRC platform with integration capabilities in which there can be a core platform, which leverages existing technology investments to help extend functionality and data sources.

At a minimum, an Enterprise-class GRC platform should be a single platform architecture that has multi-department, multi-entity use across the following areas

- Operational Risk Management
- Compliance Management
- Internal Control Management
- Issue Management (i.e. incidents, issues, investigations)
- Note: an Enterprise GRC should also supply a content library, workflow, and tasking capability, exception management, cycle repeatability, audit trail, version control, enforcement, RBAC, asset tracking, and robust reporting.



03

---

What Should I Ask  
of GRC Vendors?

# What Should I Ask of GRC Vendors?

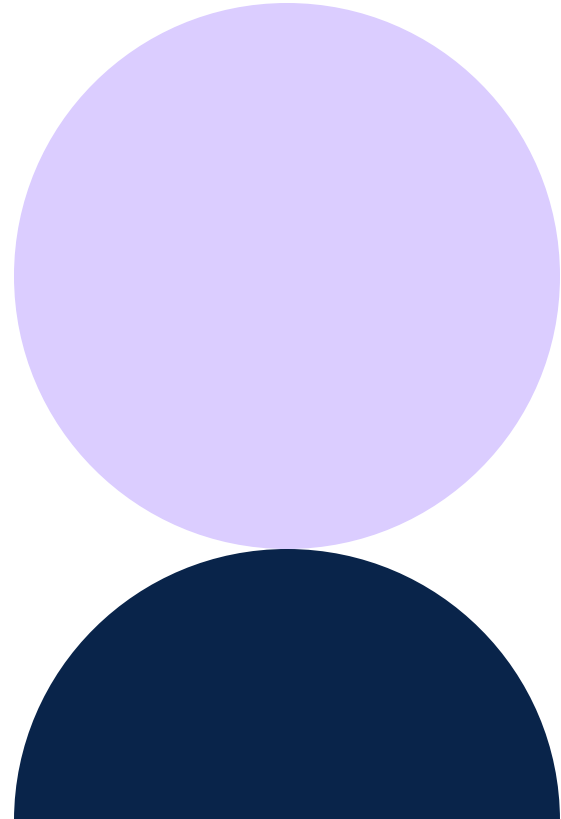
While your considerations should mirror the needs of your specific organization, there are several over-arching considerations in evaluating a GRC provider:

- Cost
- Ease of Use
- Security
- System Architecture/Data Sovereignty
- Agility/Scalability
- Content
- Technology Debt
- Client References
- Configurability
- Implementation Team
- User Experience

Asking the most relevant questions to your requirements is key to selecting a GRC platform. Knowing how the software will adapt to your internal processes as well as the level of vendor support you can expect are both critical data points when evaluating the options.

# Example preparation questions:

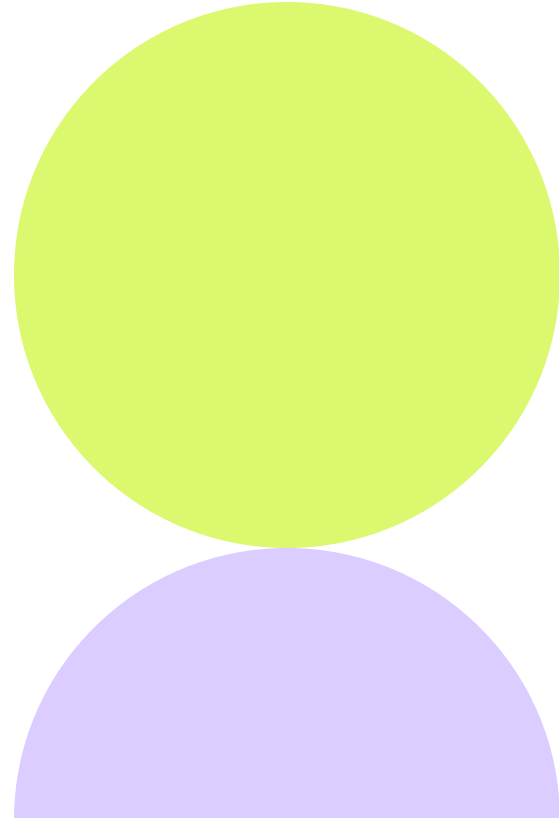
1. What is driving the need for a GRC solution?
2. Who from your organization is behind the initiative?
3. Where are you now from a maturity standpoint?
4. Do you have specific use cases you are trying to solve?
5. How will you support your chosen GRC platform (during the implementation phase as well as long term)?



# Example implementation questions:

Some of the initial questions to consider when implementing a new GRC solution include:

1. How many entities within the organization will need GRC functionality?
2. What is the average implementation time for an organization of our size and use case?
3. How easy is the software to configure and how reliant will I be on your Professional Services?
4. What level of expertise will be required to manage the system?







04

---

## Calculating ROI and Building your Business Justification

# Calculating ROI

A GRC solution can provide significant value to your company. Unfortunately, because the benefits are difficult to quantify, so is making the case to implement GRC software. Having a quantifiable Return on Investment (ROI) makes it easier to build a case for upper management, which in turn will help you garner the necessary budget and advocacy.

GRC implementations vary considerably across industries and businesses, but there are agreed commonalities in the value achieved. This ROI Calculator takes both an Implementation and Procurement Based ROI approach.

Our selected business case provides a summary of all benefits realized using a comprehensive, integrated GRC platform.

When you partner with 6clicks, you get access to a comprehensive, integrated, and scalable platform. Thus, we chose to base our analysis on the benefits of using a software like ours.

Further, we have found that a more comprehensive GRC platform provides a higher ROI. It should be noted, however, that implementing one GRC area can provide similar benefits but at a smaller scale. In fact, many of our clients begin by implementing one area of GRC, such as Internal Control, and then expand to implement other programs as they realize the value of a GRC platform and as their business needs grow.

# Business Justification

Given that not all GRC platforms are created equal, be aware of what the platform requires from a care and feeding standpoint in comparison to what your department can bear. Look for a solution that fits your processes today and can scale to meet your long-term growth objectives.

Your chosen solution should also enable you to do more, with less. Even in the face of resource constraints, an efficiency-focused GRC platform will save you time and increase your operational productivity. Those productivity gains will translate to cost savings, less human error, and greater efficiency. The result should be to bring agility to the organization and equip you to reach new heights.

The increased cross-organizational visibility the right GRC platform will bring, will set you up for success. That visibility is invaluable when the organization grows, introduces new offerings, adds vendors, enters a joint venture, or perhaps expands internationally.

# Conclusion

Deciding on a GRC solution to fit your organization's various needs can be overwhelming. There are several vendors to choose from in the GRC market – making the decision process much more difficult.

When evaluating tools, it's most important to first consider your requirements, your users, and your desired outcome of implementing the technology. Once you've landed on your organization's success criteria, the evaluation process will feel easier, more organized, and less burdensome. Beginning the GRC buying journey without clearly defined requirements or success criteria for your GRC program can prove detrimental to the process and lengthen it significantly. So, take it one step at a time and, before you know it, you'll be on your way to a successful GRC implementation.



Determine if you are ready for a GRC



Determine baseline expectations of a quality GRC



Questions to ask a GRC vendor



Calculating ROI and business justification



Our service and products allow our direct customers, consultants, lawyers, assessors, auditors and service providers in general to leverage the 6clicks Risk and Compliance Operating System easily and quickly. With offices across APAC, UK, U.S. & India - there is a 6clicks maestro near you.

Visit [6clicks.com](https://www.6clicks.com)

