Putting the 'G' into GRC

Camms.

Software to Change Tomorrow.

Is Governance Important to Organisations? You Bet It Is!

Governance influences how an organisation’s objectives are set and achieved, how risk is monitored and addressed, and how performance is optimised. Surely then, no executive leader in their right mind could overlook this cornerstone of structure and processes for decision making, accountability, control, and behaviour? You’d be surprised: rather than underpinning integrated governance, risk, and compliance (GRC), it is often side-lined by impatient executives who want to skip straight to managing risk and complying with regulations without laying the foundations for success.

What Is GRC And Why Does It Matter?

Every organisation strives to meet its business objectives. To achieve this, it must contend with a myriad of challenges that arise in the ever-changing business environment – from regulations and technology to people and processes – by addressing uncertainty and acting with integrity. For this reason, organisations have been governed and risk and compliance managed for as long as we can remember. However, many failed to approach these requirements in a mature joined-up manner, erroneously viewing them as separate entities that don't overlap.

In today's crowded, uncertain, and interconnected business landscape, GRC has evolved into an integrated set of processes and procedures that form the bedrock of an organisation's strategy for managing overall governance, enterprise risk management and compliance with regulations. The Open Compliance and Ethics Group defines GRC as: "the integrated collection of capabilities that enable an organisation to reliably achieve objectives, address uncertainty and act with integrity."

While not an entirely new concept, GRC has become integrated – and subsequently grown in stature – in response to escalating risks that have become more widespread, complex, and detrimental. If left unaccounted for, even just one risk can send shockwaves through an organisation with devastating effect – from damaging supply chains and disrupting business continuity to compromising IT security and reducing workforce productivity.

The evolution of GRC from a disparate set of requirements into an integrated set of processes and procedures has also been driven by several forces that have reshaped the risk terrain:

Increasing pace and scope of regulatory requirements: almost every organisation across all industries must comply with a growing number of dynamic regulations – a trend that has been accelerated by the proliferation of all things digital in the business environment.

Accelerating digitisation of risk management: the digitalisation of business practices has exposed organisations to new threats – most noticeably cyber-attacks – which in turn has precipitated the deployment of digital innovation to combat these threats.

Growing importance of risk management in business strategy: the increasingly perilous and costly risk environment has brought risk management into sharp focus for boards, who must steer their companies toward resilience and value by embedding strategic risk capabilities throughout their organisation.

Evolving sophistication of analytics: innovative analytical tools are delivering improved insights around risk, which is facilitating informed data-driven decisions.

A well planned and executed GRC strategy will deliver the collective approach that's required to manage the dynamic risk and regulatory landscapes – and it is something from which the whole organisation will benefit. The right people will be able to make informed decisions by gaining access to the right information at the right time; the correct objectives and controls will be established, prompting a reduction in costs, duplication, and impacted operations; and sustained, reliable performance and subsequent delivery of value will be achieved.

The Three Elements of GRC

When broken down, the constituent elements of GRC can be defined as follows:

Governance:
the ability to align processes and actions with the organisation's business objectives. In GRC terms, this will allow the organisation to set direction through strategy and policy, monitor performance and controls, and evaluate outcomes.

Risk:
a possible event that has the potential to cause harm or loss to an organisation or prevent it from achieving its objectives. Risk management is the process of identifying, analysing, and controlling risk.

Compliance:
ensuring a set of guidelines, established and regulated by a relevant industry body, are adhered to. By complying with these regulatory requirements, the organisation demonstrates that it takes the necessary measures and implements robust controls to operate in line with industry standards.

Viewing governance, risk, and compliance as separate activities typically results in inefficiencies, redundancies, and inaccuracies, including: lack of oversight of the complete risk landscape, conflicting actions, unnecessary complexity, and an inability to manage the escalating impacts of risk. This fragmented approach leads to the creation of narrow processes or systems on an ad hoc basis in response to a specific event – such as new regulations or a data breach – with little or no consideration of their holistic impact.

Forward-thinking organisations recognise that there is overlap between the three elements of GRC, which impact the same technologies, people, processes, and information. This allows them to harness the power of each discipline to add value to one another by implementing GRC in an integrated manner that encompasses the entire organisation – and ultimately build a stronger more resilient organisation in the process. According to an OCEG GRC maturity survey, 93% of organisations report that GRC integration provided benefits that met or exceeded expectations.

While this holistic approach has become the foundation of successful GRC strategies, some organisations struggle to marry governance with risk and compliance, resulting in an imbalance. If governance involves an overall management approach used to direct, monitor and manage GRC effectively for the achievement of an organisation's objectives, the culture of governance must start from the top down. Unfortunately, organisations often fail to initiate the necessary transformation within their corporate culture to take risk and compliance management seriously. Deprived of the holistic view that's required to educate, embrace change, and obtain buy-in from all stakeholders involved, their GRC strategy is doomed to fail.

The process of achieving a top-down governance culture is often tripped up by a major hurdle: communication. GRC policies and processes that are developed within the confines of the boardroom, without consulting the wider business, are left rudderless. Consequently, the people that are impacted by them on the coal face subsequently feel disenfranchised and unwilling to embrace them.

The challenge does not end there: even perfectly crafted policies resulting from effective collaboration can be hamstrung by communication bottlenecks that prevent vital information from being disseminated across the organisation – stunting adoption by stakeholders at all levels of the business who remain disengaged.

Risk and compliance without effective governance causes organisations to remain stuck in the past, when the confluence of the three disciplines was a mere pipe dream – and when a siloed approach to GRC created as many problems as it solved.

Why Is Governance Important and Why Should It Integrate with Risk and Compliance?

Good governance has four key components:

Transparency:
clearly defining the organisation's structure, operations and performance – internally and externally – and opening a robust dialogue with relevant stakeholders.

Accountability:
ensuring informed decision-making within the organisation, by implementing processes that provide the right people with the right authority to make effective and efficient decisions.

Stewardship:
establishing an enterprise-wide view that the organisation is managed for the benefit of its shareholders/members, while taking account of the interests of other relevant stakeholders.

Integrity:
fostering a culture committed to ethical behaviour and regulatory compliance.

They subsequently drop the ball when it comes to establishing robust governance processes and procedures using innovative software solutions, focusing instead on native integration between risk and compliance at its expense.

Consequently, only risk and compliance apps are integrated with one another via application programming interfaces (APIs). Yes, valuable data can flow between the apps and become more readily available to employees; but they are missing the vital element that allows them to set direction through strategy – and without this strategy, they will struggle to align processes and actions with the organisation's business goals.

The benefits of delivering these four pillars of governance success are compelling: preserve and strengthen stakeholder confidence; provide the foundation for the organisation's output to accelerate; and ensure the organisation is agile enough to respond to a changing external environment.

Poor communication from the top down is not the only thing that leaves governance licking its wounds. Commonly, this vital process of creating the right environment to mitigate risk, optimise performance and protect the organisation is overlooked in favour of risk and compliance management, because they pose an immediate threat: whether it's the risk of a data breach resulting in reputational damage or failure to comply with the latest piece of industry regulation resulting in a hefty fine.

This failure to see the bigger picture and recognise how governance underpins effective risk and compliance management renders organisations short-sighted.

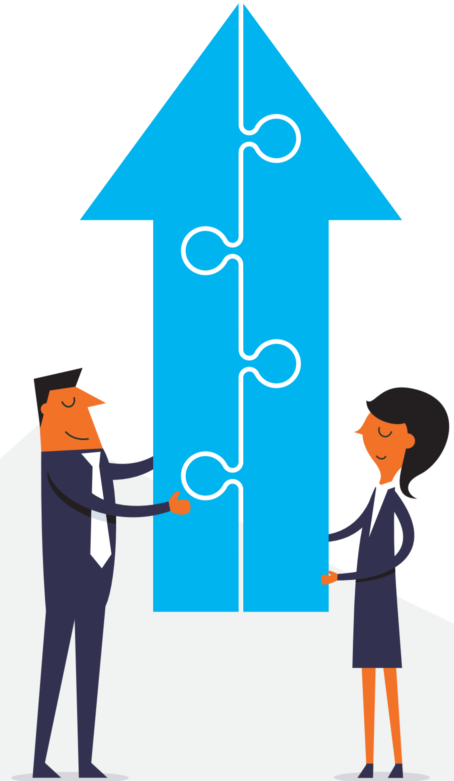
Benefits of Integrated GRC

The process of implementing GRC in an integrated manner, aligned with business processes and strategic objectives, demands the collaboration and synchronisation of information and activities. To achieve this, several roles – including audit, risk management, and compliance – must work in unison to share information, data, assessments, metrics, risks, and losses.

Get this right and organisations can reap the rewards:

- ✓ Accuracy of risk and control information facilitates quick and informed decision-making, preventing financial and reputational loss, data breaches, and compliance violations.
- ✓ A centralised view of risk is provided to executive leadership teams to help them understand enterprise-wide risks more clearly, while also providing process owners at the business unit level with the autonomy to independently assess and manage their own risks.
- ✓ Provides a transparent 'single version of the truth' to employees, management, auditors, and regulatory bodies. Effective compliance horizon scanning allows organisations to address constant changes in regulations, technology, and the business.
- ✓ Provides the ability to respond proactively to risks by breaking down restrictive functional, business, and organisational silos and reducing fragmentation among departments.
- ✓ Provides the agility needed to manage emerging risks.
- ✓ Facilitates worthwhile IT investments that mitigate risk proactively.

Transforming GRC from fractured independent processes into an integrated discipline offers strategic advantage by helping risk and compliance professionals to analyse and share data for a 360-degree view of the organisation's risk posture. This holistic perspective enables boards and executives to make decisions that align management activities with business strategy and performance.



5 Steps to Successful GRC Integration

Achieving integrated GRC is not an overnight process, nor is it prescriptive. After all, no two organisations are the same: they have different objectives, challenges, resources, and requirements. To pave the way to successful GRC integration there are five steps to follow on this journey to your desired destination, where governance, risk and compliance become one discipline that enables you to reliably achieve your objectives, address uncertainty and act with integrity:

1 Identify operational gaps to prioritise areas to improve

Having collected pertinent data and information relating to existing fragmented GRC processes, you can assess the maturity of each process, evaluate the quality of the data, and identify operational gaps – from duplicate processes to manual processes that can be scrapped or automated.

2 Plan a robust GRC strategy

Having reviewed your current internal approach to GRC and assessed the external landscape – both its strengths and challenges – identify the gap between your current and desired state and develop a GRC roadmap that considers key GRC aspects. This will enable you to begin planning a comprehensive GRC strategy that achieves several vital goals: ensures systems and processes are integrated across all business units, allows you to better manage risk, and keeps the organisation compliant with relevant regulations and requirements.

3 Engage your team with an effectively communicated strategy

You must bridge the gap between your strategy remaining a set of well-meaning ideas and it becoming an established force for positive change by achieving user acceptance. This requires you to break down the barriers between the boardroom and the business by effectively communicating your strategy from the top down, so it's implemented from the bottom up.

4 Lay a solid foundation to support your GRC strategy in the long-term

A solid foundation will ensure your GRC strategy can withstand the test of time. Failure to establish foundational components can cause challenges and turmoil further down the line. From a GRC perspective, this includes a policy inventory, regulations, risk framework, controls framework, and vendor and engagement inventory. If the key foundational components are established effectively, future workflows will align succinctly with the business, ensuring the right decision-makers are informed and involved.

5 Deploy an integrated risk management system

The use of disparate GRC tools in silos, none of which integrate, is a common roadblock for organisations. Yes, each department has a tool in place, but the data they produce is not connected because the applications do not communicate. This lack of connectivity prevents them from establishing an integrated approach to GRC.

Therefore, the most effective platforms are those that seamlessly connect to and co-exist with other IT applications that provide data to facilitate risk, compliance, and audit exercises. This delivers the power to leverage existing risk solutions that are fit-for-purpose for a truly integrated GRC approach – and the benefits are compelling:

Consistency and standardisation of data:
requires less oversight and supports fast, risk-informed business decisions by optimising the downstream flow of data.

Transparency and oversight:
allows stakeholders to review and predict risks with greater accuracy and take advantage of worthwhile opportunities when they arise.

Operational resilience:
provides the ability to respond proactively to risks by breaking down restrictive functional, business, and organisational silos – preventing financial and reputational damage caused by potential risks, such as data breaches and compliance violations.

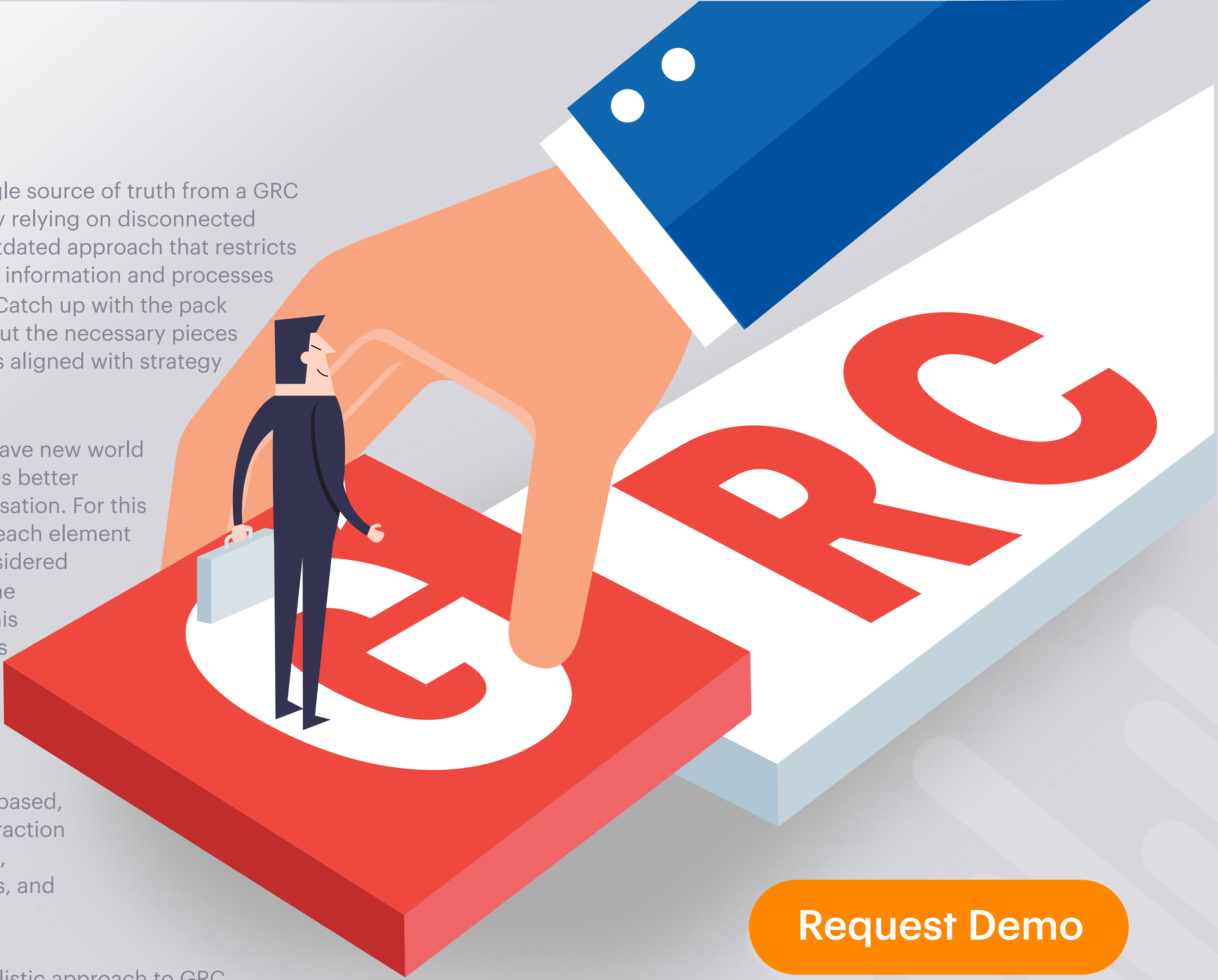
Regulatory change:
facilitates effective compliance programmes that address constant changes in regulations by linking them to risks and policies.

In true integrated GRC style, these factors combine to create an overarching benefit of adopting an enterprise-wide approach to GRC: greater efficiency – with actions performed proactively instead of reactively, holistically rather than in silos, at greater speed, and more accurately.

Conclusion

Organisations perform best when they have a single source of truth from a GRC perspective. So, don't remain behind the curve, by relying on disconnected disciplines, isolated tools, and siloed data – an outdated approach that restricts the scope of GRC management by scattering vital information and processes across multiple systems in unstructured formats. Catch up with the pack by ensuring risk managers no longer struggle to put the necessary pieces together to make risk-informed business decisions aligned with strategy and linked to performance.

To move with the times, you must embrace the brave new world of integrated GRC – a burgeoning trend that drives better results and builds a stronger more resilient organisation. For this to be a success, equality is key; by that we mean each element of GRC must be shown equal respect and be considered a vital cog in this unified discipline – because if one is neglected the whole will suffer. At the core of this is the adoption of innovative software and systems that communicate and exchange data with each other to solve business problems holistically.



Camms.Connect provides your organisation with access to robust business services via standards-based, real-time APIs. These APIs facilitate seamless interaction with many critical areas of the Camms ecosystem, including staff, financials, projects, incidents, risks, and measures.

You can use Camms.Connect APIs to provide a holistic approach to GRC management in several compelling ways: from extracting data for use in third party business intelligence solutions and extracting data for input into other systems to integrating staff, user and organisation structure details into Camms from your HR system and integrating information to automatically update actual values for KPIs.

We're here to help you change your tomorrow. To learn how Camms can support your approach to GRC, request a demo today.

Request Demo

Camms.

Software to Change Tomorrow.

cammsgroup.com