A cultural guide to GRC

CoreStream offers a set of considerations when implementing or refining a practice, be it integrated governance, risk & compliance (GRC) or a single risk or compliance area, with the primary aim of fostering the right culture. There isn't a one-size-fits-all approach to effective GRC, but there are common threads that will have a significant impact on the likelihood of success

The term governance, risk and compliance (GRC) means different things to different people. To some, GRC is a vendor-driven term to categorise products and services. Others suggest the scope of GRC is flawed and should encapsulate 'performance' or that the reference to 'governance' should be removed. Is GRC a culture, a practice or a programme?

In truth, it is probably a combination of all three, depending on the level of organisational maturity. Change programmes help implement or revise GRC practice. This practice, if implemented effectively, will help the firm develop a desirable GRC culture. What matters is that the scope of a firm's GRC activity is based on what is optimal for the organisation and the environment in which it operates. Endlessly debating nomenclature will do little for you. Instead, firms would be well advised to focus on a number of practical considerations as they work towards a GRC-aware culture.

Educate

Making an organisation risk-conscious is imperative. Without this, GRC can become a mandatory bolt-on, viewed as a cumbersome burden on 'real' jobs. Employees who are risk-aware and understand the importance and value of effective GRC are more likely to embrace the content, rather than simply comply by following due process.

Education is necessary to create this awareness. Employees need to understand the importance of GRC, the benefits of an effective approach and the potentially damning consequences of an ineffective one. They also need to be aware of how they contribute to its success.

This awareness helps dispel the myth that GRC is some mythical hard-to-conceptualise theory. People make risk-based decisions several times each day, for example, when crossing the road or deciding on what time to leave for an important meeting. An effective GRC practice formalises this way of thinking and improves the availability and quality of information that informs future decisions.

Lead and reward

The desired GRC culture is frequently one that is inclusive and collaborative. Mandating policies and rigorously policing them will seldom encourage the desired culture and will likely create an 'us' (the business) and 'them' (audit or risk management teams) relationship that is actually counterproductive.

Adoption is encouraged by leadership setting the correct tone from the top and furthered by incentivising. Embedding GRC within balanced scorecard objectives, for example, helps ensure the spotlight is focused on performance. Remuneration packages directly attributable to these metrics goes a stage further towards encouraging individuals to make GRC considerations on a routine basis. To reinforce the message, senior management should consider explicitly linking company successes to GRC performance whenever appropriate (commenting on annual results, for example) so a clear benefit is demonstrated to those who operate the processes on a daily basis.

In order to be sustainable, GRC should rely on repeatable processes and knowledge sharing, not on a limited number of specialist risk or compliance professionals operating in isolation. To this end, the business should be encouraged to take ownership and be involved at the control design stage. Processes dictated by remote compliance departments will seldom be as effective as those designed collaboratively, with due consideration for business-as-usual activity. The role of an effective risk or compliance team is to facilitate, advise and review, not independently own the content or approach.

Help, don't hinder

Organisations should know what it is they are trying to guard against and prioritise controls accordingly. Unnecessary roadblocks that create a compliance burden but do not deliver on specific objectives should be avoided. Disproportionate controls can result in compliance fatigue and be detrimental to developing the desired culture.

GRC culture should encourage proactive prevention. It is less helpful to review what caused the fire once the building has burned down, and so GRC should minimise the likelihood of issues occurring and the impact of them if they do. Processes to detect, report and address issues are important – you don't want the house to burn down repeatedly– but prevention is more beneficial than simply dealing with the clean-up exercise effectively.

Beyond minimising the likelihood or impact of negative events, GRC objectives should comprise positive benefits. Consider the negotiation of a complex contract; an organisation with a deep understanding of risk is able to flex the risk-reward balance more proactively, building a position of strength relative to competitors. More simply, building a reputation as an ethical, compliant, risk-conscious organisation can in itself provide competitive advantage. Communicating these benefits internally helps employees recognise that GRC is not simply a line of defence – it can potentially improve an organisation's performance. GRC is not just about staying out of the headlines.

Standardise

In organisations where compliance has typically been a reactive undertaking, it is common for a series of silos to have formed. Something goes wrong, regulators or shareholders insist on action and a process change, technology or a particular department is put in place to address the problem. Aside from not benefiting fully from economies of scope, there are other issues attributable to this reactive behaviour. Multiple review functions digging up the same stretch of road repeatedly, but for different reasons, is not only inefficient but can also cause audit fatigue within an organisation. The more burdensome GRC becomes, the more difficult it is to develop the desired culture.

One option is to centralise. A compelling business case can be put forward as technology and resource cost savings are measurable, as are the efficiency gains through reducing duplication. However, the significant cultural, political and operational challenges in centralising disparate units may outweigh the benefits. Whether an organisation chooses to centralise or not, standardisation will almost always drive significant benefits.

The majority of GRC efficiencies are actually gained from having a common framework, common terminology and common reporting. A standardised approach breeds familiarity from shop floor to board level. The former are more likely to embrace something that is less convoluted and the latter can more easily review performance and make decisions using management information (MI) with common categorisation, structure and format.

Get the best from technology

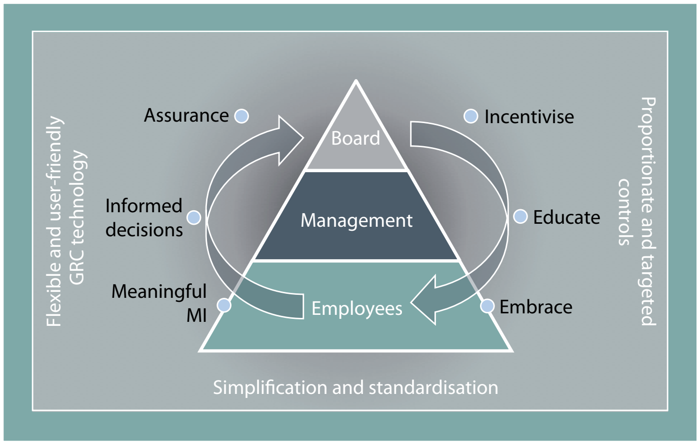
Irrespective of the level of investment or sophistication, technology is not a self-contained GRC solution. It should be regarded as an enabler that improves the efficiency of people and processes; not as a substitute for them.

Technology improves the management of information, highlights potential issues and automates what is repetitive and inefficient. A previously cumbersome process for reporting enterprise-wide operational risk, for example, is far more efficient when data is input to a single register and MI is produced automatically and in a consistent format.

The automation of decision-making should be handled with care. Decisions that lend themselves to automation will typically have few variables and are generally based on a static response to a threshold; when *x* happens, the consistent response is *y*. Even when this is the case, the automation is usually only the short-term reaction, and the longer-term response will still need to be determined by management. Absolving people from the responsibility of making decisions is not only impractical, it also serves to distance them from GRC if they believe 'the technology takes care of that'.

The use of GRC technology is also susceptible to the law of diminishing returns. At a basic level, it is notable how many organisations would benefit from simply providing access to central repository for policies, processes and risks. The next step might be to use technology for assigning ownership of controls, or raising and tracking audit issues and associated remedial actions. As the use of technology begins to address more sophisticated areas, management should consider the net benefit of implementing and maintaining a technology-based solution. If 80% of the benefits can be realised with 20% of the effort, it might be wise to stop there. If the technology itself is becoming a burden, then the GRC culture will suffer.

1. GRC –The virtuous circle


Board
Management
Employees
Assurance
Informed decisions
Meaningful MI
Incentivise
Educate
Embrace
Flexible and user-friendly GRC technology
Proportionate and targeted controls
Simplification and standardisation

Deployed effectively, technology can contribute towards establishing a GRC culture. Technology encourages user adoption and collaboration through being accessible, intuitive and uncomplicated. Experience tells us that the more pleasurable something is to use, the more likely we are to use it. Implemented properly, technology can contribute towards making GRC a habit.

> "Our life is frittered away by detail. Simplify, simplify"
>
> Henry David Thoreau

Keep it simple

Keeping things simple is overarching and something to be conscious of at all times. Education can only be effective, collaboration only encouraged and technology only successfully adopted if the content, approach and associated benefits are understandable. You can't expect to foster a culture outside of GRC professionals if the practice is too complicated to be understood by a wider audience.

While regulation and risks can be inherently complicated, there is no need to add to this complexity by adopting a convoluted response. The most complicated regulation can still often be boiled down to a set of logical controls that are embedded in well-thought-out processes. The most effective GRC practices will address the complexity at the design stage and avoid reflecting it in the controls themselves. Keep the implementation simple and it unlocks the potential to foster the desired culture.