CoreStream®

In the Press

How the right culture is key to successful governance, risk management and compliance

As featured in newbusiness.co.uk; growthbusiness.co.uk; real business & fresh business thinking.

Richard Eddolls, Head of Platforms, CoreStream, discusses how fostering the right culture is critical in establishing effective governance, risk and compliance within an organisation.

What exactly is governance, risk and compliance? So many definitions exist, some of them so vague, some of them convoluted and in truth not many textbook definitions will be entirely applicable to your circumstances. It's easy to become confused and even add to the complexity. Strip out the excess verbiage and the principles are straightforward:

- Governance relates to how you manage your business
- Risk management is how you deal with uncertainty
- Compliance is how you adhere to certain requirements (both established internally or mandated by externals)

Put simply, effective GRC produces objectives that are compatible with an organisation's values; and, in turn, enables these objectives to be met according to an acceptable risk profile, within both legal and ethical boundaries. Business performance is recorded, measured and reported in a consistent manner to inform future decisions. Ideally, better business decisions.

All companies need to understand and manage all three elements of the compliance challenge if they are to succeed – no matter their size or maturity. A particular risk to growing businesses, or those operating in a rapidly changing environment, is to lose control over one or more aspect, with potentially serious consequences. Such firms ought to be developing their GRC frameworks as early as possible in their formation, and in doing so should focus on some simple, yet practical considerations:

In the Press

Lead and reward

Leaders of organisations should contribute to the GRC culture by setting the example – lead from the front. Dictating policies and rigorously policing them is seldom the best way to develop the desired results. Creating incentives within performance objectives, remuneration packages or similar will also promote the adoption of new practices more easily. GRC practices should not be seen as something that gets in the way of doing a job but rather something that is a valuable part of the job..

Engage

Avoid creating a 'them and us' relationship between the business and the audit/compliance team by involving the business teams at the control design stage. Encouraging staff or teams to take ownership of the policies going forward will prove far more effective. You wouldn't make other types of change effectively without strong stakeholder management so why should GRC change be any different?

Help, don't hinder

Controls must accord with the organisation's objectives and its approach to risk management. Once significant risks have been identified and prioritised, the procedures developed should target them specifically. Avoid attempting to create catch-all processes: these inevitably create a burden on the business which is often out of proportion to the actual risks involved, and may have a negative impact on company-wide buy-in. And most of all – keep it simple. How can staff conform with process they can seldom understand?

Keep it simple. How can staff conform with process they can seldom understand? keep it simple. How can staff conform with process they can seldom understand?

Educate

It is imperative that employees are made risk-aware as they will then appreciate and value the GRC directives in place. They need to know the benefits of an effective GRC approach and the potential consequences of an ineffective one. Make them cognisant of how they contribute to the firm's success by contributing to the desired outcomes.

In the Press

Standardise

Take note - where compliance is allowed to be reactive, processes and solutions will develop organically, often leading to duplication, inefficiency and increased risk of failure. Simply introducing controls without due consideration of the how it is implemented frequently makes compliance a burden, causing employees to subvert or simply ignore the processes..

Standardisation of common frameworks, terminology and reports may seem easy but is often where some of the greatest gains can be made. Employees are more likely to embrace the simple and familiar; and leaders are better able to review performance and make good decisions when management information follows common formats.

Use technology effectively

Technology is used to improve access to information; to detect and highlight potential issues; and to automate repetitive tasks. However, it is an enabler rather than a solution: good technology won't address poor risk management, but it will improve the efficiency of those responsible – and help highlight where things aren't so good.

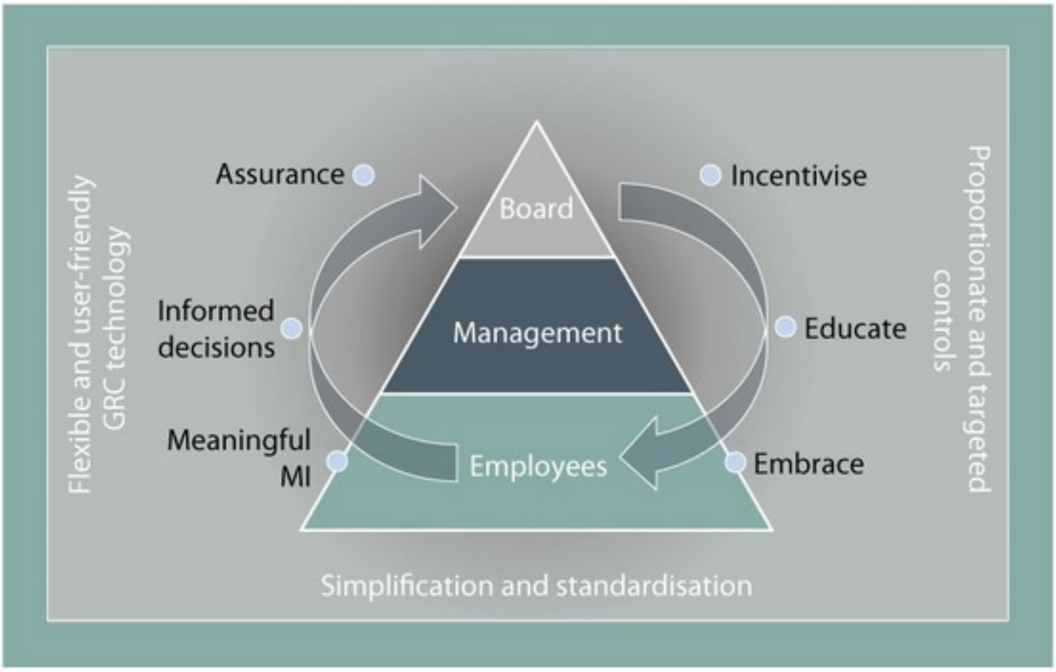
The best investments are often the simplest – a single repository and reporting tool for policies, processes and risks, for example. As complexity increases, the returns diminish. Ultimately, even the most sophisticated systems require human decision-makers, and attempts to limit human input is rarely cost-effective.

If made accessible and intuitive, technology will help to facilitate standardisation further, and encourage broader user adoption and collaboration.

Keep it simple and take small steps

All too often regulations and risks are complex. The response should be kept simple: it's impossible to foster a positive culture if only a GRC specialist can understand the processes and nomenclature. The most effective GRC practice addresses the complexity at the design stage, and simplifies the implementation.

Of course, integrated GRC is often seen as the holy grail, but problems arise when the organisation reaches for it from the start. Projects become complex, unwieldy and slow to realise, even to the extent that solutions are out of date before they're fully implemented. Change, when it occurs, is often sudden and overwhelming, leading to unnecessary disruption, resentment and more pleading for special cases. It is usually better to take smaller steps, so start by fixing the most serious problems, and proceed from there.


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

Remember, a strong GRC culture isn't about reviewing things that go wrong. It's about preventing them from going wrong in the first place. Good practice relies on common processes and knowledge sharing throughout the organisation, with the risk or compliance team on hand to facilitate, advise and review. Aside from building a reputation as an ethical, risk-conscious business, an organisation with a deep understanding of risk is better equipped to flex the risk-reward balance in negotiations, and to ultimately build a position of strength relative to its competitors.

ENDS