THOMSON REUTERS

Best practices in GRC convergence: building a blueprint for GRC convergence

The success of GRC convergence is dependent on a well-executed, comprehensive risk identification and assessment process, and Paisley, a Thomson Reuters company, has established itself as a world leader in this area by putting in place a clear-cut series of best practices and establishing a blueprint to define the scope, taxonomy, methodology and outcome of any GRC project

GRC convergence occurs when GRC groups reach consensus on the combination of tools and practices, the framework(s) and common languages they will adopt, and the common software platform they will use to support assessment and reporting across the organisation. Companies who are most successful at deriving the tangible benefits of GRC convergence start with a blueprint of the project.

As with all complex building projects, the building of a GRC convergence initiative requires a detailed blueprint to define the scope, taxonomy, methodology and outcome of the GRC convergence project. In analysing the benefits of GRC convergence, the project should focus on five major points:

- Defining the organisation and process context
- Establishing a common language for risks and controls
- Implementing a consistent, reliable methodology
- Developing transparency, reporting and monitoring
- Leveraging technology.

Defining the organisation and process context

GRC convergence requires a single definition of the topics or subjects designed to meet the needs of all GRC groups and their stakeholders. Generally, the essential assurance contexts consist of a shared organisation hierarchy and essential business processes. Other contextual elements such as account structure, policy and procedure frameworks and the external regulatory frameworks governing the organisation's conduct are all important. But only the organisation and process structure requires consensus upfront from all groups.

Today, individual GRC groups acting independently to create the contexts they require. Each GRC group defines the organisation structure differently, for example, legal entity versus business unit, and may require different levels of organisation structure on which to assess and report. This leads to inconsistent definitions of core data, inconsistent ratings, inconsistent scoping, and hides systemic problems, duplication and gaps in coverage.

To derive the benefits of GRC convergence, all GRC groups must use the same organisation and process structures for planning their work, allocating resources and reporting.

For most organisations, inefficiencies from assurance fragmentation are so great that huge savings are possible from taking the simple step of eliminating silos and operating on a common context of a shared GRC organisational and process structure. The outcome of these efforts will enable an organisation to:

- Co-ordinate planning across all GRC profiles
- Eliminate gaps and duplication in coverage
- Decrease time spent by business managers
- Increase ability to spot trends as they develop
- Utilise a single system of record for assurance information.

Establishing a common language for risk and control

A comprehensive assessment of risks and controls requires the use of standard risk and control taxonomy. Effective GRC convergence requires that risks and controls be classified and reported against standard models on which GRC groups agree. For example, if malicious code is considered a type of risk important to the organisation, then all instances of malicious code risks should be categorised accordingly and reported as such wherever they occur. Organisations could decide which risks, defined by risk type, are critical to identify and manage across all contexts and by all GRC groups.

Without a standard naming convention or common methodology for determining or classifying risks and controls, assurance professionals from different disciplines are unable to share information. The cost of this siloed state, for many organisations, is a driving factor for GRC convergence initiatives. Risk assessments are performed multiple times by multiple assurance groups on the same risks, and corporate boards are communicated a complex set of redundant, overlapping information.

On the contrary, the benefits of utilising a common language for risks and controls are far-reaching and include:

- Improved reporting throughout the organisation
- Consistent coverage – all risks are considered
- Improved business performance – risks explain performance gaps
- Better decision-making – decisions are risk-based
- Less external oversight and audits – controls are standardised.

Implementing consistent, reliable methodology

GRC convergence requires a set of decision rules that guide what GRC information must be gathered and how it will be gathered. The decision rules include defining risk types to assess and the risk thresholds to drive the depth and quality of the review. Successful GRC convergence projects define: thresholds beyond which risks would require mitigation or additional management; definitions of what controls require testing; and rules governing the creation of issues for reporting and resolution. The intent of the GRC methodology is to ensure all GRC groups address risks, controls and issues in the same way.

Examples of where agreement needs to happen between assurance groups include:

- What top-down risk criteria should be used
- What top-down scores require assurance
- What processes require risk identification
- What risks must be assessed (type or level)
- What risks require response (type or level)
- What risk responses require remediation
- What control groups/types are mandatory
- What controls are most cost-effective.

By adopting a common and consistent methodology towards risk and controls, organisations can benefit from:

- Aligned management and GRC assurance groups
- Improved external risk ratings – lower cost of capital
- Efficient resource allocation
- Increased management ownership
- Reduced conflict between assurance groups
- Increased management self-assessment
- Reduced reliance on audits and inspections
- Earnings stability – no shock events.

Developing transparency, reporting and monitoring

Effective GRC convergence dictates that management and staff have primary responsibility for assessing and reporting significant information on GRC objectives. More importantly, to assess the continued effectiveness of GRC convergence efforts, all information on the status of risks and controls should be available for continuous reporting. If implemented effectively, GRC convergence projects provide a common scoring and rating communication between management and the board of directors so that both have relevant information to fulfil their roles with respect to the GRC objectives. Also, matters affecting the achievement of GRC objectives are communicated with internal and external parties who need the information, including boards and their committee members, shareholders, creditors, suppliers, customers, communities, governments and regulators.

The benefits of a consistent and disciplined reporting structure include:

- Availability of accurate and consistent reports
- Positive knowledge and reporting of risks and controls for all participants
- Integration of assurance functions through information
- Positive knowledge of the reliability of all risk and control information
- Higher share multiple – rewards for better governance.

Leveraging technology

Technology is the cornerstone of GRC convergence. The development and maturation of GRC technology, largely driven by the *Sarbanes-Oxley Act*, has enabled GRC convergence.

For effective GRC convergence, all GRC information should be available on a single platform, appropriately accessible to all parties to GRC convergence, including management. Collaboration is critical to GRC convergence. GRC assurance experts, business managers and even some stakeholders will require access to regularly read, update and report on status.

By eliminating information silos and redundant data entry, and taking a unique holistic approach to regulatory challenges, GRC technology provides greater efficiency, improves collaboration and reduces the time and resource costs associated with GRC processes. GRC technology enables organisations to break down the walls between audit, risk and compliance groups and provides expanded value as organisations deploy the software across the enterprise.

Additional benefits that can be gained by utilising a single technology solution for GRC convergence include:

- Single universe of all convergence data
- Elimination of duplicate documentation
- Elimination of white space
- More processes, risks and controls assessed
- Increase in management accountability/certification
- Consolidated, reliable reporting
- Improved business performance through key performance indicators/key risk indicators.

About the Author

Bruce McCuaig, vice president risk & compliance at Paisley, a Thomson Reuters company, has more than 20 years of experience in the field of risk and control management. Mr McCuaig has been instrumental in positioning the company as a knowledge leader in governance, risk and compliance solutions.