ROUNDTABLE

Innovation and technology for GRC

REPRINTED FROM
DECEMBER 2017 ISSUE

FINANCIER WORLDWIDE corporatefinanceintelligence

ROUNDTABLE: INNOVATION AND TECHNOLOGY FOR GRC

A comprehensive governance, risk management & compliance (GRC) programme is a fundamental component of any company's business armoury. This suite of functions and values enable executives and risk leaders to mitigate risks, reduce compliance breaches and improve business performance. Additionally, recourse to innovation and technology is assisting companies in the implementation of their GRC strategies. At its most effective, GRC accommodates interconnected oversight of business segments, which, in turn, helps companies to deal with the numerous regulatory, reputational and operational risks that are part and parcel of today's corporate landscape. ■

THE PANELLISTS

Shaun Brady
Executive Director, Center for Model Based Regulation
T: +1 (410) 798 0485
E: sbrady@cmbreg.org
www.cmbreg.org

Over the last 35 years, Dr Shaun Brady has held leadership and advisory roles at some of the world's largest financial institutions and government agencies, improving their risk visualisation capabilities, managing evolving regulatory and cyber security requirements, mining and monetising data, developing new products and services and implementing a variety of technology enabled solutions to reduce operating risk, optimise capital and deliver mission critical capabilities.

Randy Stephens
Vice President, Advisory Services, NAVEX Global
T: +1 (404) 600 3242
E: rstephens@navexglobal.com
www.navexglobal.com

Randy Stephens is vice president at NAVEX Global, which he joined in 2012. A lawyer and compliance specialist, Mr Stephens has worked in roles with legal and compliance responsibility for over 30 years, including operations in Mexico, China and Canada. He has trained employees on conduct risk and programme assessments in Japan, China, Australia, UAE, KSA, Kuwait, Jordan, Qatar, Romania, Serbia, the UK and Canada, while also working with clients with offices and operations around the world.

Patrick Henz
Head of Governance US & Compliance Americas, Primetals Technologies
T: +1 (770) 740 3752
E: patrick.henz@primetals.com
www.primetals.com

Patrick Henz is the regional compliance officer for the Americas at Primetals Technologies. He began his career in compliance at the end of 2007, when he was responsible for the implementation of the Siemens anti-corruption programme in Mexico and several Central American and Caribbean countries. This gave him valuable insights into global compliance programmes, with a focus on Latin America. Since 2009, in his role as compliance officer at Primetals, he has been responsible for implementing an effective compliance programme based on identification, protection, detection, response and recovery.

Don Andrews
Partner, Reed Smith
T: +1 (212) 549 0318
E: dandrews@reedsmith.com
www.reedsmith.com

Don Andrews is a partner in Reed Smith's New York Office. He is the global practice leader of the firm's risk and compliance group (RCOM). He has the rare combination of experience and understanding of all manner of financial institutions and operational companies, small and large, combined with over 27 years of federal and private sector experience in litigation, compliance and risk management. Mr Andrews' experience in enterprise risk management includes developing ERM programmes for both operating companies and financial institutions.

Thomas Kimner
Head of Global Marketing and Operations, Risk Management, SAS
T: +1 (240) 618 1017
E: tom.kimner@sas.com
www.sas.com

Thomas Kimner leads the risk marketing and operations area within the risk research and quantitative solutions division at SAS. He is currently responsible for executing the overall marketing plan for risk management solutions and products, as well as coordinating risk priorities on a global basis. In addition, Mr Kimner has responsibility for leading the division's sales enablement, marketing and operations functions including customer messaging, budgeting, financial analysis and programme management activities.

Luis Kolster
Vice President, Chief Ethics & Compliance Officer – Latin America and Africa
Walmart International
T: +1 (479) 268 8634
E: luis.kolster@walmart.com
www.walmart.com

Luis Kolster is the chief ethics & compliance officer for Latin America and Africa for Walmart International. In his role, he leads the implementation and execution of Walmart's ethics & compliance programme, including anti-corruption, ethics and other compliance subject matter areas, in 22 countries outside the US. Prior to Walmart, Mr Kolster spent over 12 years with Schlumberger, a leading supplier of technology and services for customers in the oil and gas industry.

Could you provide an insight into the growing importance of governance, risk & compliance (GRC) for companies today? What are some of the common GRC issues that companies face?

Brady: One of the misconceptions is that GRC – or as I prefer to refer to it, risk management – is a new requirement. It has been and always will be important. The problem is that organisations, for the most part, do it very poorly because they view it as, in this case, three silos of activities, and not as an integrated business requirement, a part of the organisation's DNA. Just like the core issues with cyber security are not related to technology but rather people, the same holds for risk management. And people need to be governed by principles, generated and lived from the top down, informing everyone as to what is expected when the processes, controls and rules do not seem to apply.

Henz: The three areas of GRC create a triangle, which includes strategy, processes and people and technology. The last two are particularly important in the process of disruption. For example, the values and attitudes of millennials have become a big part of today's workforce. On the technology side, Industry 4.0 and artificial intelligence (AI) offer fascinating opportunities, but also present new risks. Machines may work more effectively than humans, but they also suffer from biases and data protection risks. Today, people and technologies change processes and strategies. The model does not mean that GRC is responsible for these four areas, but GRC has to interact with their respective owners.

Kimner: The rise in regulatory compliance requirements, coupled with more proactive oversight by organisation boards and executive management teams, has increased the need for a strong governance and controls framework. Firms face risks from several areas – not only financial and regulatory, but also cyber security, operational, organisational, geopolitical and environmental, to name a few. An important aspect of a sound GRC framework is to spend time identifying these risks, qualifying and quantifying them, and developing risk mitigation strategies. The downside of having a less than adequate programme is potentially severe reputational and financial harm.

Kolster: Every successful organisation must be able to show that it has a clear set of rules to guide the conduct of employees and efficient internal controls to identify and correct deviations. It is also expected that companies conduct risk assessments periodically and allocate resources to address the highest risks. In today's world, wrongdoing by senior managers in an organisation may bring not only fines and penalties in multiple jurisdictions, but also a loss of trust and a reputational damage that may take years to overcome. Companies today have a duty to be responsible members of the communities where they operate, and GRC plays a key role in this area.

Andrews: Regulators have raised the standards considerably for GRC, especially for financial institutions. There is an expectation not just of board-level involvement, but also of advanced technological competence in connection with GRC. Particularly with large banks, robust and sweeping enterprise risk management programmes that are driven by the board are an expectation, not an exception. But even given the differing requirements for smaller institutions, regulators expect the board to be instrumentally involved in directing the implementation of comprehensive and effective risk management and compliance management systems. In addition, digitisation is a key GRC challenge. As the data footprint for companies continues to grow and new technologies transform industry, a company's ability to govern, evaluate, understand and report on its operations is necessarily impacted.

Stephens: GRC has taken on added importance because of globalisation. Few organisations are governed purely by limited, domestic concerns anymore. They must comply with a confusing web of international and local laws, regulations, customs and culture. Also, there is increasingly more cooperation by governments and investigators. Information and data sharing make cross-border investigations easier to conduct and substantiate. Additionally, more laws are holding individuals, in addition to organisations, responsible for misconduct. The risk is amplified due to the proliferation of third parties engaged at multiple levels throughout organisations. These third parties can be a source of misconduct or illegal activity, which may result in regulatory investigations, fines and penalties and may ultimately harm an organisation's brand and reputation. The risks that many organisations face still revolve around bribery, corruption, conflicts of interest and, of course, cyber security. Overlay GRC risks with a greater availability and awareness of whistleblower protections and financial bounties, and the likelihood of detection rises.

FW: Do you believe it is becoming increasingly difficult for companies to keep abreast of regulatory developments, compliance demands and government enforcement initiatives, without the help of technology-based solutions?

Henz: As Leonardo da Vinci once said, "Simplicity is the ultimate sophistication". GRC includes legal, formal, technical and psychological elements. The legal- and rules-based part is an ideal field for automation and AI. Machines can connect to different global databases, take over GRC tasks like contract reviews or vendor due diligence. Considering the value that such technology offers, it is possible that governments could require this in the future to ensure an effective compliance system. On the other hand, AI can further support other functions like human resources. This is more challenging, as potential biases and questionable predictions may lead to legal and ethical pitfalls.

Kimner: It has certainly been a challenge for many firms to stay current on regulatory demands and requirements over the last decade. Not only have regulators increased their focus on capital management – including more rigorous analysis, additional reporting requirements and transparency related to stress testing – there are new requirements for consumer protection, fraud, privacy and other operational areas. And now, national and international financial standards boards are requiring companies to meet increasingly complex accounting standards with new requirements for loss provisioning, as seen in new rules related to expected credit loss: IFRS 9/CECL. As compliance requirements become more pervasive, organisations are finding it more challenging to have a holistic view of risk without adopting technology. Traditional governance and oversight methods, where individual teams work with spreadsheets and other documents to capture controls, is not adequate in today's regulatory environment.

Kolster: It is absolutely impossible for companies operating in multiple jurisdictions to be aware of all legal and regulatory requirements and to keep track of all government enforcement initiatives without the help of technology. Insights into local enforcement are also important. Technology can help you identify, for example, the environmental requirements that are in force in one specific city for building and operating a factory. Local knowledge will help you understand how those requirements apply to the factory you need to build and operate in your line of business. It is not enough to have access to data through technology; it is important to use that data in a way that will benefit the company.

Andrews: It is becoming increasingly difficult for companies to keep up with regulatory developments and compliance demands without the assistance of technology-based solutions. But it is important to remember that technology is not a panacea; it is only as good as the people who use it. It is more important for institutions to attract and retain talented and experienced compliance professionals who have the institutional knowledge and regulatory background to effectively employ any technology, and to evaluate the suitability of existing technology to meet GRC objectives. For example, the EU's Markets in Financial Instruments Directive (MiFID II) imposes new business communications – including telephone – retention requirements. This requires effective technology implementation to achieve compliance.

Stephens: Increased global regulations and enforcement have heightened legal, regulatory, financial and reputational risks worldwide. Tracking and ensuring compliance with GRC, as well as an organisation's own policies and procedures, is even more difficult in the global economy. Technology makes it easier to conduct and document necessary training, due diligence, risk mitigation and investigations. When confronted with misconduct or an allegation of wrongdoing, organisations which can demonstrate and document reasonable, risk-based automated processes are far more likely to successfully defend the allegations or demonstrate that a rogue employee was the culprit, rather than a cultural predilection for misconduct. This evidence goes to the heart of what constitutes an effective compliance programme, as recognised by international guidelines and regulators.

Brady: Complexity begets complexity, and the value of tools to help manage it has always been the source of most of the related innovations – but also, unfortunately, the drive to build solutions in search of problems. Consequently, it starts with understanding what the goals are you are trying to achieve, the outcomes that are important to the business' success, and then strive to build in the processes that generate the measures necessary to inform whether you are achieving them or not. Only then should you look to technology to see if it can more effectively or efficiently enable and control those processes, as well as support the timely visualisations of the related risks to your success.

FW: In your opinion, have companies yet to fully harness innovation and technology in their everyday GRC decision making? In what areas are they missing out?

Kimner: Many companies are still approaching governance in a piecemeal fashion. They use various siloed technologies and processes with no centralised technology, programme or oversight. This makes it difficult to fully capitalise on their GRC activities. Divisions run various governance programmes independent of one another, which makes it difficult for the corporation to assess overall programme effectiveness and difficult for the divisions to have a strong understanding of any cross-cutting risks or deficiencies in governance that may impact them. Leveraging technology to consolidate information and review key dependencies and risks across the enterprise can help shed light on governance weaknesses and potential issues.

Kolster: Monitoring compliance and responding to issues identified through such monitoring processes are key elements of an effective compliance programme, and this is an area where the use of technology may provide amazing benefits. GRC decision making must be informed by data. This is where there is still a lot of room for development. We see self-driving cars, voice recognition devices that control all connected electronics in your house, and apps for everything, but we are only starting to see analytics that combine data with insights in order to help us predict compliance risks. Technology also allows the relevant compliance messages to be delivered faster and more efficiently than ever before. This works for top-down compliance communications from company leaders, as well as training that is delivered timely and efficiently to teach employees what they need to know, when they need it.

Andrews: There are a number of reasons why companies have yet to fully harness innovation and new technology for GRC. First and foremost, technology must be employed by people who truly understand the regulatory regime, the institution and the technology in order to make effective use of it. Given how rapidly technology is changing, it can be difficult to find the individuals who are prepared to effectively leverage new technology for

GRC purposes. Furthermore, technology is not a replacement for a full-blown enterprise risk management programme; it is an enhancement. There are burgeoning developments with technologies such as AI, blockchain and contract analytics that have the potential to enhance GRC programmes in meaningful ways, including vendor management, cyber security, surveillance, monitoring and data protection.

> AN EFFECTIVE GRC PROGRAMME SHOULD BE DESIGNED AROUND FIVE KEY COMPONENTS – LEADERSHIP, RISK ASSESSMENT, STANDARDS AND CONTROLS, MONITORING AND RESPONSE, AND TRAINING AND AWARENESS.
>
> LUIS KOLSTER
> Walmart International

Brady: Automation is too much of a crutch – an excuse for not tackling the hard problems first, and instead relying on a sales pitch that 'if only you buy X, all your problems will be solved'. Very few organisations use technology effectively and those that do will tell you their success is based on putting the necessary requirements gathering and assessment processes in place first. One of the key gaps and challenges is defining and getting the data organisations need to make the right decisions. And instead of searching for the data throughout the silos and spreadsheets that are created in most businesses, and trying to determine what is important, until you know what is important to support your decisions and it is a by-product of your processes, no amount of technology investment will make a meaningful impact.

Stephens: Many companies do not harness the power of technology effectively. Yet, innovation and automation are both making inroads into GRC and automation is proving to be invaluable. In surveys we have conducted, compliance professionals who responded about the 'effectiveness' of their programmes against 12 elements resoundingly replied that advanced programmes, which usually included automation, were more effective. Nevertheless, many programmes remain reactive or are still maturing and lack automation and data for predictive analysis and measurement.

Henz: Depending on the industry, innovative technology is more or less integrated into GRC decision-making processes. Traditional companies are still sceptical about implementing such tools, based on the costs, but also due to a mistrust of the underlying technology. Although the machine decision-making process is more transparent than the human one, the AI 'black box' is perceived as being more menacing than known human biases. By contrast, modern start-up companies tend to underestimate classic business and compliance risks. Trusting their technology, they often push it out without implementing adequate human governance. In so doing, they ignore the fact that humans are ethically and legally responsible for their technology, even if it acts autonomously.

FW: What, in your opinion, is essential to an effective GRC programme? What factors should companies consider when developing a GRC programme that allows them to think about, respond to and manage risk?

Kolster: An effective GRC programme should be designed around five key components – leadership, risk assessment, standards and controls, monitoring and response, and training and awareness. Leadership includes an independent team with the right size, appropriate resources, and full support from the leaders of the organisation. The risk assessment must be a documented process involving key stakeholders with a clear result that generates mitigating action items. Standards and controls are all policies and procedures on the relevant areas of compliance, including the process to investigate any potential wrongdoing and apply disciplinary actions when appropriate. Monitoring includes the regular tracking of key elements of compliance, and the implementation of controls where the level of compliance is below the acceptable thresholds. Through training and awareness the organisation ensures that the employees are aware of the procedures that are applicable to their activities, and that the culture of compliance is properly communicated at all levels.

Andrews: A successful GRC programme is built on five essential elements. First, a robust, honest and politically neutral process to identify and assess risks within the institution by skilled professionals. Second, working with internal and external professionals to understand the full implication of the regulatory and operational risks unique to the institution. Third, a well-devised and executed plan to rate risks in order of their importance and mitigate those risks. Fourth, a governance programme that includes effective reporting and auditing to elevate all such risks to the board and senior management to make it part of their daily decision making. Finally, ensuring that the appropriate technology and operational systems are employed by knowledgeable professionals to address ongoing risks. Without effective training, reporting and escalation of issues once reported, the quality of the solution will not matter.

Stephens: Organisationally, the most essential elements of a GRC programme are a willingness and ability to identify risks and address them proactively. This cannot be done if silos exist and risk responsibility is not ultimately integrated into the business, measured and controlled. Automation can help identify and track risks, as well as address many forms of mitigation, including policies, training, incident management and due diligence. Trying to manage this process using spreadsheets, email or internally built databases lacks the coordination, integration and ability to provide real time predictive analysis. All business units must participate and share information. GRC and compliance cannot function with maximum organisational efficiency in silos. Also, culture must be addressed. The best GRC programmes in the world are still only 'tick box' exercises if the organisation's culture is at odds with its values and objectives. A strong values-based code of conduct, supported by training, awareness and monitoring, is essential.

Henz: Simplicity is the priority. Processes have to be as robust as required, and as simple as possible. Information is the company's most important resource and GRC has to ensure that the cost of gaining information is as low as possible. If not, the organisation loses its people, as bureaucratic processes lead to demotivation and temptation to violate guidelines and laws. Next, it must be clear that risk is nothing negative, but a natural part of doing business. An open working culture must allow individuals to speak up about potential risks without fear of repercussions. All risks and opportunities have to be analysed by the GRC processes, but it is up to management to decide which risk levels the company is willing to accept. GRC has to ensure that agreed-upon follow-up actions are implemented and in order to control identified risk levels, stay inside agreed-upon parameters.

Brady: Buying a tool to solve a GRC or risk management problem, is putting the cart before the horse. If you have not defined your metrics and outcomes based risk management programmes, buying a tool is not going to give it to you. It begins with everyone in the organisation knowing what the business or mission requires them to do and to achieve in order to be successful, which then, in turn, defines what data you need to capture to monitor your efforts. To the extent technology can cost effectively support these requirements, apply it where it does. GRC or other tools may be good for automating existing, good processes, but that assumes you know they are good and the right ones to focus on.

Kimner: The first critical element in developing an effective programme is to adequately identify, evaluate and capture the potential risks the organisation faces. The goal here is not to try to 'predict' when these risks will occur, but to identify their likelihood and potential severity. The second key element is to develop an appropriate framework or architecture for the overall programme. This involves mapping appropriate controls and management actions, including escalation procedures and developing a clear communication strategy. The third element is to proactively develop a specific and suitable mitigation strategy, complete with clearly identified actions and accountabilities. Too often, organisations experience some type of negative event – for example, a data or privacy breach or rogue trader – that not only catches them off guard, but also exposes a lapse in mitigation planning.

FW: Once defined, what steps should companies take to roll out a comprehensive and innovative GRC programme? How important is staff training and buy-in, for example?

Andrews: Board and senior management buy-in is critical. Rolling out a comprehensive and innovative GRC programme should include sufficient C-suite level communication to ensure that the programme is received with the proper level of gravity and importance. In terms of training and buy-in, every employee must be integrated into the programme to the extent that they are a 'risk owner'. This is especially the case for operational line managers who will need to work with the risk and compliance team to report relevant risks in a timely manner, serve on the relevant committees and sub-committees and become owners of the enterprise. Buy-in can be further incentivised by implementing results-measurements or performance evaluation components

> TOO OFTEN, ORGANISATIONS EXPERIENCE SOME TYPE OF NEGATIVE EVENT – FOR EXAMPLE, A DATA OR PRIVACY BREACH OR ROGUE TRADER – THAT NOT ONLY CATCHES THEM OFF GUARD, BUT ALSO EXPOSES A LAPSE IN MITIGATION PLANNING.
>
> THOMAS KIMNER
> SAS

that reward active participation in GRC programmes.

Henz: In a complex and changing environment, it is impossible to define all potential scenarios. It is imperative that rules must leave enough space for the heart. This is no contradiction, as effective guidelines can be designed to include this freedom. Furthermore, clear rules protect employees as they can act based on their values inside a defined space. Parallel to this, employees not only have to know 'what' they have to comply with, but also 'why'. If individuals understand the cost of corruption, failing strategy, risks of new technology and so on, they will not comply because they have to, but because they believe in the cause, or they have empathy for the potential victims. Training serves not only to communicate information, but to motivate employees. In addition, management and GRC must 'walk-the-talk'.

Brady: I would start by asking how involved business owners are in the company's requirements and implementation processes. There are a few old adages I have found to be true – 'until the pain of the status quo exceeds the pain of change, nothing will happen', 'it is not your words but your budget that really defines your strategy' and 'culture eats strategy for breakfast, lunch and dinner'. Understand these in the context of your organisation and you will know what needs to be done.

Kimner: Before examining some programme best practices, it is worth looking at how companies have approached the notion of a comprehensive GRC programme over the last 15 to 20 years. For a period in the early 2000s, many consultants, analysts and some companies jumped on the enterprise-wide GRC bandwagon to get a better handle on how to identify and mitigate internal and external risks. Attempts were made to create centralised divisions and deploy common technology packages. Over this period, however, many companies abandoned their efforts to create truly

> ROLLING OUT A COMPREHENSIVE AND INNOVATIVE GRC PROGRAMME SHOULD INCLUDE SUFFICIENT C-SUITE LEVEL COMMUNICATION TO ENSURE THAT THE PROGRAMME IS RECEIVED WITH THE PROPER LEVEL OF GRAVITY AND IMPORTANCE.
>
> DON ANDREWS
> Reed Smith

comprehensive, consolidated programmes as complexities grew and various risks – requiring more specialised knowledge and skills – were increasingly managed by different divisions. What has emerged in many cases is a less centralised corporate programme with consolidation and evaluation focused only at the reporting level.

Stephens: A comprehensive GRC programme starts with an assessment of the highest risks and a multi-year plan of awareness and communication. Next, organisations must identify and address any gaps in programme effectiveness, such as policy creation and management, third-party due diligence or other risks. Finally, assign responsibility, timelines and KPIs to measure effectiveness. Mix in cultural awareness and communication and you have covered all your bases. Communication must come from all levels and should be coordinated and relatable. Translate communications where necessary. Make sure these processes are regularly repeated and revised as necessary.

Kolster: When it comes to technology, an innovative GRC programme is not built based on the technology that is available to support it. On the contrary, the programme should set up all key requirements and processes that have to be implemented to add value to the business, and find the right technology that will support them. This is also a key test of how committed the company is to building the right GRC programme. If Excel and email are your best examples of technology, you are not going to go far in terms of innovation. Additionally, technology is only useful as long as it is adopted by the users, and a high adoption rate is driven by how easy and user-friendly technology is, and how users are encouraged to adapt to changes.

FW: How can technology and innovation help to streamline GRC processes so that decision making is enhanced, and processes are effectively and efficiently executed?

Stephens: Data is important but can often be overwhelming, particularly when it is communicated without context. Automation can make it possible, especially for larger organisations, to collect and use data in ways that make predictive analysis possible. Home-grown systems may help collect and store data, but they are rarely as helpful as purpose-built, third-party systems when it comes to analysis and real-time dashboards. These analytics are a driver of innovation, compared to data reporting alone.

Kimner: Because many banks today manage GRC processes within separate lines of business and geographies, management is somewhat limited in gaining a clear understanding of the multitude of processes in play and their criticality, owners and status. Technology can aid in consolidating and analysing information related to governance and control procedures, as well as risks. And, technology that embraces innovation – including open source code, cloud-based solutions and the integration of streamlined workflow – has been shown to add transparency and enhanced control to a comprehensive GRC programme. Additionally, through the efficient adoption of technology, management can more readily identify where resources should be focused, both in terms of the criticality and status of processes.

Brady: Automation initiatives can help, but it is important to know which problems, workflows and processes are important before starting a tool acquisition. It is equally important for companies to have or to generate the data they need to actually accomplish something measurable. Make sure the right data gets to the right people in the right format and at the right time. Once again, understand these requirements in the context of your organisation and you will know what needs to be done.

Kolster: The best decisions are the ones that are taken with all available information. Today, when we face a problem, we may have just too much information to process effectively. Technology may help us organise the information we need to make more informed decisions. But this will not come from technology alone. We need to be able to design the technology that will help us filter and organise information, and adapt it to our company's characteristics and realities. Technology may play multiple roles, from basic record keeping to really enhancing the way decisions are made through information analysis and identification of relevant trends that impact the business.

Henz: Technology can and must support a philosophy of simplicity. AI uses Big Data from its connection to global databases and from the real-time information that it receives from cloud connected equipment. With local assumption and statistical methods, Big Data becomes Smart Data. Based on this, today's information overload gets reduced to a size that makes it possible for human employees to process it. GRC allows a better understanding of a corporation's processes and risks. Transparency enables the employees to analyse the actual business and to envision long-term goals including a realistic strategy to reach them.

Andrews: In the hands of capable, experienced and knowledgeable team members, technology can be utilised as a tool to identify and mitigate potential risks. Technology and innovation can streamline GRC processes by more efficiently collecting, analysing, reporting and presenting information for assessment. Rather than overwhelm a decision maker with the breadth of data that may be available and introduce the possibility of analysis paralysis, technology can produce visualisations of actionable data and metrics to centralise the data in a way to facilitate a GRC evaluation. Technology can also streamline the identification and tracking of sources and levels of risk through mapping, which can be beneficial to a holistic GRC process and can facilitate the appropriate deployment of resources across the organisation.

FW: Could you outline the potential cost savings involved when innovation and technology is deployed as part of a GRC strategy? Should companies reasonably expect to reduce costs in essential areas while eliminating unnecessary expenses elsewhere?

Kimner: An efficient, cost savings strategy for GRC requires adopting innovative solutions that embed project experience and subject matter expertise within the technology. Automating and linking disparate workflows and systems with this approach is key to improving the effectiveness of an enterprise. Deploying technology, and especially appropriate levels of automation, can provide cost savings through streamlined processes, reduced manual effort and improved reporting. Additional savings can be derived from eliminating redundant processes and improving transparency for audit purposes. Knowing which lines of business, models or products need prioritisation enables banks to more efficiently allocate resources, leading to a

> AI'S CORE STRENGTHS ARE ITS PREDICTABILITY AND HIGHLY REPEATABLE PROCESSES. EVEN IF THE FULL POSSIBILITIES OF AI ARE STILL NOT UNLEASHED, THE EARLY RESULTS ARE PROMISING.
>
> PATRICK HENZ
> Primetals Technologies

reduction in GRC costs as a percentage of operating expense.

Brady: I have never seen an enterprise-related project driven by cost savings, or for that matter, compliance or regulatory requirements, succeed. Nor were the people that championed them based on those objectives still around when they inevitably failed. These outcomes need to be by-products of making the business more successful, and thus they are ancillary metrics for evaluating and selecting the various technology or other options that are required to make the business a success.

> COMPLIANCE SURVEYS OFTEN SHOW THAT THE OVERALL EFFECTIVENESS OF COMPLIANCE FUNCTIONS INCREASES SIGNIFICANTLY WHEN PURPOSE BUILT, THIRD-PARTY AUTOMATION IS USED.
>
> RANDY STEPHENS
> NAVEX Global

Kolster: Technology is an investment. There are good investments and bad investments. When using technology as part of a GRC programme, the budget owners must consider how that technology is going to strengthen the company's processes and procedures, and how it is going to make things easier and faster for all the users. Showing this value to all stakeholders is essential for the adoption of the technology, and ultimately for its success. The most innovative GRC departments have dedicated resources to implementing new technologies that add value, not only to the department, but to the organisation. They are also in charge of quantifying that value and showing it to the key stakeholders.

Henz: AI's core strengths are its predictability and highly repeatable processes. Even if the full possibilities of AI are still not unleashed, the early results are promising. For companies to implement such tools, not only should the technical costs be considered, but also how to conduct an effective change management process. Without the second, the first will fail as unengaged employees may passively or actively sabotage this technology out of fear that their positions may be eliminated. Companies must also consider the potential benefits. AI can reduce costs and, depending on the topic, even lead to higher output. It is up to the organisation to decide if it wants to reduce costs or enhance productivity. In general, we can expect Industry 4.0 to eliminate some jobs while creating new ones. Historically, this has been true for every new wave of automation.

Andrews: Effective GRC strategies should focus on risk identification, mitigation and containment, not on cost reduction. It is a mistake to deploy innovation and new technologies for GRC with the expectation that the company will see immediate cost reductions. Nor should companies expect to immediately and drastically reduce their compliance and risk teams and replace them with technology alone – this presents a risk in and of itself. Instead, companies should be focusing on how to deploy innovation and technology for more effective GRC programmes and better risk management. Any potential cost savings from proper implementation of technology for GRC purposes are likely going to be felt downstream as relative, not net, costs. Over time, as technology becomes more reliable and integrated into GRC processes, we may see compliance teams gradually reform with a focus on fewer individuals who are highly-skilled at leveraging technology for risk management.

Stephens: We must be careful not to focus solely on cost, but instead address cost and the return on investment (ROI). The ROI often reduces GRC costs, but in some cases, slight increases in costs may be warranted by the value of the end product of the automation. Much of automation's value comes from the savings generated by moving from manual to automated data collection. This may reduce FTE or software costs but greater value or ROI may come from the ability to regularly analyse and report in real time. The resulting quality of information and reporting is superior to manual generation. Compliance surveys often show that the overall effectiveness of compliance functions increases significantly when purpose built, third-party automation is used.

FW: In what ways can companies use technology to collect and refine data, feed this into risk management reporting and identify any gaps in risk coverage?

Henz: Cloud connected equipment can strengthen AI's prediction capabilities. This gives manufacturers more control over production performance, including insights into failure- and risk-rates. Knowing the different parameters, AI can predict the equipment's efficiency rate, not only for similar environments, but also different setups. AI can not only analyse and predict the efficiency of technical systems, but also social organisations. Such information can be included in risk management efforts. But the behaviour of AI is just as relevant as the results it achieves. It is imperative that this technology acts according to the same values, attitudes and guidelines as human employees. Complete automation of the risk process is not the goal, as experienced individuals can add value by interviewing various key employees.

Kolster: Technology is not used only to capture and store information; it supports an efficient use of that information. Just like in many other areas, innovation in GRC is thinking about the end user – the internal or external client – and making things easier, faster and friendlier for them. For example, if a company operates in multiple countries and the compliance programme includes a number of subject-matter areas, the business executives will want to see the risks they face, both from a geographical perspective and from a subject matter perspective. They may also want to identify those risks easily, with colour codes, or through a simple risk ranking. At the end, all this may be presented in a tablet that shows access to all available information and allows the business executive to be in control of what they want to see.

Stephens: Once a risk assessment and gap analysis have been completed, technology and data can be mined and analysed for mitigation opportunities. For example, using the risk of bribery and corruption, databases can be reviewed to see what online training was provided, when it was provided, and if there was any correlation with training and a reduction in incidents. To ensure proper diligence with respect to third parties, GRC professionals can use third-party automation to confirm that appropriate due diligence was performed and documented, prior to the execution of a contract for each third-party. This step would likely support an auditable trail to demonstrate that third-party engagements were following the policies and procedures established by the organisation's GRC practices. Since many organisations engage and manage thousands or tens of thousands of third parties, doing this manually would require considerable investment in staff and resources. Automation can manage this process on a cost-effective basis. Also, often there will be client contract requirements on training, certifications and data access. Automated systems can easily confirm this information in client audits. This saves time and may ensure contract compliance, renewal and so on.

Andrews: Technology is a shortcut and an essential tool in collecting data, aggregating it from a number of sources and delivering it in a customised and efficient manner. When properly implemented by knowledgeable personnel, technology can help companies manage risks in a number of ways. However, technology alone will not be useful unless the individuals utilising the technology can identify and interpret the essential data elements. That is, technology can assist in more efficiently aggregating and condensing large volumes of data, and in reporting on potential anomalies or recognising pattern disruptions. But skilled individuals are needed to interpret the meaning of the data analytics or purported anomalies, and to institute appropriate response plans.

Brady: Companies must educate themselves on what risk management really is, find the data that helps visualise those risks, and make sure it flows as a by-product of the company's core business processes. The reality is that imposing data collection and reporting processes that add no value to a person's job, and more often than not make it harder, are doomed to fail – the same reason that cyber security requirements are so often circumvented and fail.

Kimner: Many organisations use GRC programmes simply for tracking and compliance, missing opportunities to leverage data across other GRC activities. For example, some organisations collect loss data but do not use it to inform the risk assessment process. Using a simple trend chart based on actual data can help analysts formulate much better predictions and quantify potential risks. Backtesting assessment results is another area not often fully addressed but potentially beneficial to organisations; for example, comparing projected loss data forecasts with the actual loss data collected for that time horizon. Backtesting is a standard practice for many quantitative risk areas but it has not been fully leveraged for improving assessment predictions. Using data and understanding risks through predictive analytics, for example scenario-based testing, is a powerful method for assessing risk coverage as well as mitigation strategies.

FW: To what extent can an enterprise-wide programme that delivers specific

COMPANIES MUST EDUCATE THEMSELVES ON WHAT RISK MANAGEMENT REALLY IS, FIND THE DATA THAT HELPS VISUALISE THOSE RISKS, AND MAKE SURE IT FLOWS AS A BY-PRODUCT OF THE COMPANY'S CORE BUSINESS PROCESSES.

SHAUN BRADY
Center for Model Based Regulation

GRC functions help support a company's strategic vision and objectives?

Kolster: The main role of the leaders in a GRC function is to identify how their programme can help support their company's strategic vision and objectives. The best strategy can fail if key risks are not identified, and if proper controls are not in place to make sure that the company's activities are in line with the applicable legal requirements. The most advanced organisations today include some element of trust, integrity, transparency and responsibility as part of their strategic vision. If this is the case, these objectives should be owned by the GRC function and the company's leadership teams. If this is not the case, the GRC function should influence to make it happen.

Brady: Back in the 1980s, when I first started working on 'enterprise-wide' initiatives in the banking system we were trying to come up with ways to identify all the relationships they had with their customers – unfortunately a problem that still exists today, and for the same reasons. The promise of enterprise resource planning (ERP) solutions, straight-through-processing, chief information officers (CIOs), and so on, have given way to GRC, cloud and AI solutions. The related visions have not changed, nor have the sales pitches to achieve them – only the buzz words have changed to cover up the failures. Once again, take the time to know what needs to be done to be successful and then look for the tools that can help achieve the related objectives.

Andrews: An enterprise risk management programme is precisely what should support a company's strategic plan. Understanding key risks and how they are being addressed is an essential step to acquiring new businesses, launching new business initiatives, rolling out new operational strategies and engaging in virtually any other business activity. Fully understanding whether the company or business has the capacity to effectively undertake these activities is critical for success. This may be viewed as a 'compliance-by-design' approach. GRC should be built-in to business initiatives and processes at the outset, instead of being grafted on after-the-fact. Put another way, GRC and business functions should support each other and their goals should be aligned, rather than compromising one for the other.

Stephens: An effective GRC programme does not just support an organisation's strategic vision and objectives – it is the foundation of GRC success. There are a number of universally recognised elements of an effective compliance programme and those are intertwined with the governance and risk elements required to create an organisation's GRC programme. Risk assessment, followed by the programme structure, integration with HR policies and practices, training and communication, policies and procedures, audit and monitoring, reporting and response mechanisms, and monitoring and auditing of the entire process, are all elements intertwined in GRC success. Nevertheless, all of this can be undone by a weak or misaligned culture. 'Compliance trumps culture' and 'compliance is what happens when no-one is looking' are truisms that GRC leadership and senior leadership ignore at their peril. When the GRC programme works effectively, it provides employees with the information they need to understand what is expected of them. By providing policies, training and communication, the organisation demonstrates that it is investing the time and effort into providing this information because it wants its employees to have the information and guidance to do, or avoid, the conduct that supports the organisation's strategic vision and objectives. Most people want to 'do the right thing' and will. By providing and advertising multiple means to report actual or perceived misconduct or actions which conflict with the organisation's strategic vision or objectives, the organisation makes it clear that it wants employees to be able to report potential misconduct so that it can be investigated and addresses promptly. When coupled with a strong non-retaliation policy and culture, employees are more comfortable reporting issues. A culture that allows or supports retaliation completely shuts this down and causes employees to stop reporting or forces them to go outside the organisation, to regulators or the news media, or in some cases to quit.

Kimner: Model governance and model risk management are good examples of how specific GRC functions can help support corporate strategies and objectives. Financial models represent the core intellectual property of most financial institutions and support a range of functions, from the introduction of new products and pricing to scenario-based risk management and regulatory compliance. Keeping track of models throughout their full lifecycles, including managing appropriate controls and the governance around them, requires an increased use of technology. Innovative technology solutions enable organisations to centrally govern the entire model lifecycle – identifying which models are critical to operations, how they are interconnected with activities across the firm and the marketplace, and whether they have been properly vetted, tested and deployed. Models that are not properly tested before being released into production have had disastrous results for some financial institutions. On the other hand, models that are well governed in concert with a company's strategic goals can help mitigate risk, efficiently allocate capital and optimise profit. Beyond these strategic incentives, there are international regulatory objectives that must be met for model governance.

Henz: Accurate predictions and forecasts are vital for developing and implementing strategies. With higher levels of certainty, a company can have a more precise strategy and be more aggressive with its operational actions, with fewer 'safety nets' required. GRC establishes indicators to understand if the company is 'on course' to reach its visions and objectives. An enterprise-wide programme offers different indicators. Similar to an aeroplane's flight-deck, this can show if the organisation is on the right path. If not, management can take the steering wheel to implement required measures and guide the organisation to its desired destination. With the infusion of real-time data, GRC's indicators get more powerful and management can act faster with fewer safety nets.

FW: Is it possible for companies to actually enhance business performance by taking a holistic approach to GRC issues? Does this allow them to respond quickly to new risk, compliance and regulatory developments – and take advantage of potential opportunities?

Stephens: A fully integrated GRC programme with a holistic approach creates both the will and the means for employees to do the right thing. An integrated GRC programme should also enable an organisation to be nimble and identify and respond to new or changing risks utilising the current GRC structure and automation.

Andrews: Companies should think of GRC less as a regulatory burden and more as a proper way of doing business, avoiding ill-advised decisions, unnecessary operational breakdowns and unforced errors. It should be a significant part of everyday decision making in terms of where to apply resources, personnel or whether to launch business initiatives. A holistic GRC function can benefit business units by fostering learnings and synergies across departments to exchange and make use of the same information for different use cases. For example, contract analytics solutions could both identify or manage risks for compliance, and inform pricing decisions for a business unit. A siloed or decentralised GRC function that only focuses on one business line or function will be less efficient and more costly in the long run, and integrating centralised, holistic GRC perspectives into business decisions upfront will benefit the entire organisation.

Kimner: Understanding the links to and between processes, both systems and manual, is key for improving the efficiency of an enterprise. If organisations do not know who is performing which process at what time, and how the processes differ across departments, then they do not fully understand the severity of any potential loss. Many companies have spent millions of dollars on external consulting projects to document their processes, but often what results is merely a set of binders with suggested policies and procedures and piecemeal documentation of processes that are not well understood or followed, internally. For many companies, simply 'auditing' all internal processes and linking data to each step would allow them to identify where processes are sound and where they have gaps. And communicating the findings of such an 'audit' would also help staff better understand what to do and how to execute processes correctly, especially when being linked to internal guidelines and manuals. One benefit of a robust technology solution is to capture these procedures and prompt appropriate actions throughout the process. This form of guidance reduces the risk of misinterpretation of procedures and ensures that the correct tasks are followed and completed.

Henz: Risk, compliance and regulatory developments span a triangle where the three edges stand in a close interaction. Simple and effective processes ensure people's behaviour based on the individual's values. Industry 4.0 ensures that technology adapts to people and not the other way around. It can simplify organisational processes for individuals. Risks have to be known and addressed, as they can cause stress for the employees, blocking their abilities for logical thinking. As a result, inadequate behaviour and ethical blindness may get triggered, similar to how biased information leads to wrong machine decisions. GRC topics are highly connected, so a holistic approach avoids frictional losses and supports a fast and adequate decision-making process.

Brady: At its core, proper risk management requires a holistic approach. That means it needs to be part of the organisation's DNA, creating an almost instinctual capability in everyone in the company to seek out and respond to the threats and opportunities facing the business. Consequently, adopting this kind of approach is really the only way to optimise your performance and chances of being successful – including surviving those black swan events that land in your path. If you cannot find the time to do it right, find those few companies that have done it right, and then make sure you are not in their crosshairs.

Kolster: There are two key requisites for a GRC function to be able to enhance business performance. First, the GRC programme has to be embedded into the business. Second, the GRC team members must have a business mindset. Both requisites are interdependent and one cannot exist without the other. For a GRC programme to be embedded into the business, it has to understand the business needs, as well as the challenges and issues, and present easy solutions. In many cases, technology may enable and facilitate those solutions. The business mindset is having the right approach to addressing the company's problems. At the end of the day, GRC is about doing the right thing, in a way that is fully aligned with the company's goals and objectives.

FW: How do you expect the GRC landscape to evolve in the months and years to come? How will technology and innovation continue to transform systems and processes?

Andrews: Inevitably, technology will fundamentally change how GRC programmes operate. The use of technology for GRC will become more prominent, especially considering that the use of technology in business operations is becoming more prominent; the majority of trading now consists of algorithmic trading and the global marketplaces are inherently complex and intertwined. There is a great deal of promise for GRC in areas like AI, machine learning, sentiment analysis, pattern matching, anomaly detection and smart contracts, and we expect to see more process automation implemented by GRC functions moving forward. The potential for cross-system analysis and interoperability between systems and across business units will allow GRC to more effectively and efficiently identify and manage risk. Yet much of the available technology has created new risks without providing a clear path on how to mitigate those risks, making the investment in retaining and engaging the GRC personnel capable of understanding, preparing for, and applying new technologies to meet regulatory requirements as they continue to evolve all the more important.

Kimner: One area ripe for development in GRC is bringing in text analytics and ultimately expanding into machine learning or artificial intelligence. This potentially allows companies to better analyse the importance of contemporary trends and regulations and uncover patterns in news and other media about events that can impact an organisation. Analytics applied to key web pages, news and other social media allow firms to identify the items frequently mentioned and discussed. Identifying and prioritising these issues programmatically at an early stage allows them to focus on what is important, and design efficient processes, thereby addressing multiple potentially conflicting requirements simultaneously. Here, GRC technology 'enriched with analytics' not only provides the means to collect data automatically, but also to discuss and establish best practices across the enterprise.

Henz: We are living in the golden age of AI. This is not only because of technological developments, but it is now up to us to find an adequate use for them. Business leaders cannot decide this in a vacuum. Rather, they should do so in close cooperation with 'Generation Y' and 'Generation Z'. These digital natives are not only used to working with technology, but actively demanding this from their employers – not in a self-serving way, but as a way to support their ability to live and act according to their ideas and values. Machine and human behaviour are fascinatingly alike, and the two productively working together in all processes is likely. But it has to be clear that Industry 4.0 is different from all earlier waves of automation and, due to this, there are no known paths so far.

Brady: Those that understand what they need to be successful will continue to cut through the noise and look for investments in technology and innovation to help enable their efforts. As such, for those that know where and how to apply technology and innovation it will continue to provide opportunities to transform their systems and processes, and for those lucky enough to be in a position to piggy back off those efforts it will help them also, at least until the market changes.

Kolster: It is now common to see companies that have innovation teams. Many people think about innovation and can only see it with technology. I think technology can definitely support innovation, but innovation is not only about technology. Many GRC professionals are not necessarily perceived as the greatest innovators. I think the GRC landscape must continue to evolve by promoting innovation as a way of thinking, and technology as an enabler. Changes take place at a much faster pace today, and when change is happening in all areas of an organisation, the GRC function must be perceived as a driver for change, and not as an obstruction. Technology will facilitate faster and more informed decisions, allow the identification of risks before they materialise, and enable communication between different groups in a company to address compliance-related issues as soon as they arise.

Stephens: I expect GRC and compliance to continue to develop and mature as a discipline, and I expect automation and technology to develop in ways more specific and responsive to GRC needs. More organisations will be able to recognise and justify automation so GRC can be become more robust and responsive. This should further reduce unintentional misconduct and help identify and remedy intentional misconduct faster. This should also minimise fraud, waste and abuse in organisations and ultimately bolster the bottom line. Additionally, organisations which are perceived as more compliant and socially responsible are more attractive to existing employees and to new talent. The most talented employees will be a prized commodity going forward as the current, aging workforce retires and replacements become scarcer. ■