RENAIX

Renaix guide to governance, risk, compliance and internal controls

Contents

Introduction

Each passing year creates a new record in terms of corporate costs associated with government and industry regulation compliance. Some of these costs are unavoidable – they are just the cost of doing business. However, a good chunk of the costs is the result of sub optimal handling of certain aspects and this is directly caused by improper training and a lack of understanding about risks, regulations and compliance.

It is very likely that the regulations and costs associated with compliance will only increase in the future. It is not possible anymore to have a single department dealing with risk and compliance while the rest of the organisation operates in an independent environment. The risks and their associated costs are too great.

Here at Renaix, our team is built around specialisation and market awareness, with 20 years working in the international finance and accounting industry. Our consultants are experts in their field and are at the forefront of innovation in recruitment processes and the latest industry trends. We are therefore well positioned to assist you with any skills or qualifications-related questions or concerns you may have.

Feel free to send us your CV and a member of our team will be in contact to offer their consultancy and advice on your options and how to successfully secure your next role. As part of our service, we are also happy to review your CV and provide comments and advice on how this may be improved to increase your chances of landing your next role.

Get in touch now at info@renaix.com, give us a call on +44 (0)20 7553 6320 and follow our LinkedIn company page for the latest news, trends and open recruitment positions.

If you enjoy this guide, please look out for the next one!

Governance, risk and compliance – still going strong

Some industry observers felt that the rise in the demand for risk and compliance officers in 2008 and 2009 was temporary and a knee-jerk reaction to the financial crises. The truth is that since then, risk and compliance costs have skyrocketed as regulators, shareholders and the public have become less tolerant of compliance failures. Furthermore, the damage associated with certain risks like environmental or reputational is now much greater thanks to the ease and speed of information dissipation.

Therefore, some companies are focusing aggressively on governance, risk and compliance training across the board.

The new regime

How risk and compliance training used to work (or still does in some cases), is that the employee is provided with a lengthy document which covers all aspects related to risk and compliance for their job function and they just have to sign at the very end. This read and agree format, however, is not enough anymore. It does not prevent any compliance failures and certainly does not absolve the company of any wrongdoing. The right way to deliver risk and compliance training is through a customised, iterative and interactive approach.

Thus, training programmes are specifically created for a particular job profile and delivered through classroom or web sessions. For example, training in environmental risks might be more important for a manufacturing company rather than a trading one likewise business continuity training for senior and middle management rather than the workforce on the ground and so on.

Customised and personalised GRC (Governance, Risk and Compliance) training is certainly not cheap. However, it is essential because it actually imparts the right knowledge to the right employee. It might be compared in a way to purchasing an insurance policy – you pay a large sum in premiums but when and if something happens, the policy more than pays for itself!

GRC training – Ideal for Professional Development

Employees can greatly enhance their worth to their respective organisations by staying on top of all the developments which affect governance and compliance. The truth is that regulations are becoming more complicated and reputational risks are greater than they have ever been before. In such an environment, the manager who succeeds will be the one who understands the criticality of good governance, has a sound understanding of the regulations which affects their industry and can effectively mitigate business risks.

4 steps to better risk identification and mitigation

As a direct result of the rigged emissions scandal, Volkswagen incurred over Euro 25 billion of costs, in addition to the loss of brand value and reputational damage. Banks have had to pay billions in fines for what was essentially a failure in operational risk management – in the same way as for inadvertent sanction breaches. Samsung took a USD 10 billion loss due to a failure in vendor risk management.

Although risk management has always been in force, it was the 2008 financial crisis and subsequent events which really spurred a rethink of how risks are managed. This crisis was the result of a rare "black swan" event and it called into question the practice of using historical data to predict the probability of future events. Corporate risk management has since undergone considerable change and here we take a very brief look into the resulting best practices to improve the process and structure.

Step 1: Risk identification

The process of risk identification varies significantly across sectors, the type of organisation and even for each project. In a mature industry, potential risks are generally well known, and failure is usually not the result of an unexpected risk but rather that of not managing the risk properly. For a company at the growth stage however, there can be numerous unforeseen dangers, and this is where management experience is essential to prior identification.

Step 2: Screening and impact analysis

Prioritising risks in order of severity and impact is undoubtedly the most important step as it determines the level of resources dedicated to mitigating specific risks. This is usually done in the order of their probability-weighted impact.

There are certain risks which are numerically quantifiable – in terms of probabilities and expected losses. However, certain types of risks like reputational or political require a more subjective analysis. Some organisations rely on weighted factors to calculate these risks, while others use historical data. None of these models are perfect however, and this itself needs to be accounted for as model risk.

Step 3: Risk mitigation planning and strategies

The risk mitigation process aims to minimise the impact of an adverse event. The exact process varies depending on the type of industry and type of risk, but the broader strategy falls into one of these areas:

Avoidance – changing business strategy to avoid a high-risk event. For example, delaying the launch in a new country until local elections are over.

Controlling – putting thresholds or other controls in place and then monitoring them for any breaches. Risks are not avoided here but rather kept at an acceptable level.

Hedging – a simple example would be an airline buying future oil contracts to hedge against the risk of a future increase in oil prices.

Transfer – transferring risk to a third party such as for example buying insurance protection.

Maintaining flexibility – the ability to quickly change direction in the case of an adverse event.

Step 4: Monitoring and feedback

This is essentially the feedback loop. Whatever strategies have been put in place, these are monitored to assess their effectiveness. Internal or external risk management professionals may be tasked with stress testing and providing feedback. The result of this analysis is then fed back into the existing risk management structure.

In summary, the basic structure of risk management has not changed a great deal. What has changed however is how risks are weighted and prioritised.

Third-party risk management – the new elephant in the room

The era of globalisation has added a new complexity to supply chains. Already intricate vendor and distributor networks have become even more labyrinthine. The drive to increase efficiency has also necessitated a move towards a greater concentration on core competencies – with many ancillary business activities assigned to third party vendors and solution providers.

All this has undoubtedly led to improved profitability, in addition to increased valuations. It has also, however, exposed businesses to an ever-increasing third party risk. Consider for example, a global electronics corporation which outsources manufacturing to a vendor in Asia. It is obvious that the company would have strict guidelines in place to ensure that the vendor follows not only regulatory but ethical best-practices as well. However, this gets more complex as more and more vendors or distributors are included. With hundreds or perhaps even thousands of vendors, it becomes increasingly difficult to effectively monitor all of them. Moreover, in the digital age, the reputational damage which may result from the actions of an errant vendor can be extremely high (as one would expect).

With these challenges in mind, third-party risk management, or TPRM, is gaining increasing importance. The risk management process involves identification, assessment, mitigation of third party risks, as well as responses to adverse situations.

The third-party risk management process

A good TPRM plan requires the creation of a framework that assesses the current situation and then puts robust policies and procedures in place. This is followed by the actual implementation with the relevant IT infrastructure and resource training and most importantly – continuous monitoring and assessment.

The basic framework requires comprehensively capturing all relevant public and verifiable information about a potential vendor. While on boarding a third party vendor, checks relating to past legal actions, regulatory violations, adverse media reports etc. are performed, along with a thorough vetting of the main stakeholders. For larger vendors, it might even be optimal to hire a professional auditor in order to gather all relevant information. This information is not only related to the company's past history, as stated above, but it also assesses the strength of their governance standards as well environmental and social policies which are good predictors of any possible future trouble.

Some companies use databases that are specifically maintained by professional auditing firms which can help them identify any red flags. There are also computer programmes or bots that scan the internet in real time for adverse news related to certain companies or groups of people and can throw up an alert when something specific occurs.

The future

It is clear to any observer that corporate inter-dependability will only increase in the coming years. As companies take on more and more third party risk by continuously increasing the number of direct relationships, the need for better tools to effectively scrutinise them will likewise increase. Greater regulation and increased active public participation additionally will mean that companies have far less leeway in dealing with potential risks. Given all of this, it is very likely that artificial intelligence tools will play a major role in effective TPRM frameworks. These tools can be deployed both to preemptively assess potential risks as well as to reactively raise the alarm in light of a developing situation. Having delivered sufficient functionality in deployment, it is likely the development of such tools will be well worth the costs.

6 key compliance trends for 2018 and how they can optimise effectiveness in the sector

The Compliance function has come a long way over the last decade. It has evolved rapidly to keep pace with the digital transformation of business and has become more agile to better respond to emerging situations. Rather than being a static annual risk assessment, compliance is now an ongoing and dynamic process that is sensitive to evolving risks and stress points.

Here are six of the key compliance trends for 2018:

- Effectiveness in the compliance sector is being driven by technology. The last decade saw a rapid increase in the number of compliance professionals to tackle newer threats, although that growth seems to have stabilised to an extent. The focus is now on creating better tools for these compliance professionals and establishing more effective procedures, communication channels, monitoring techniques and so on.

- The greatest focus in compliance is on training, the emphasis shifting from quantity to quality. Organisations are seeking experienced compliance professionals and are more than willing to bear the additional cost of providing the best compliance training opportunities to their existing staff.

- There is an increasing focus on data quality and assessment capability. Moving to digital processes means that organisations generate a tremendous amount of additional data. This data can be indispensable not only from a business standpoint but for compliance and risk management as well. However, the challenge here is to ensure that the data is of high quality and usable. This requires expertise and investments into data analysis.

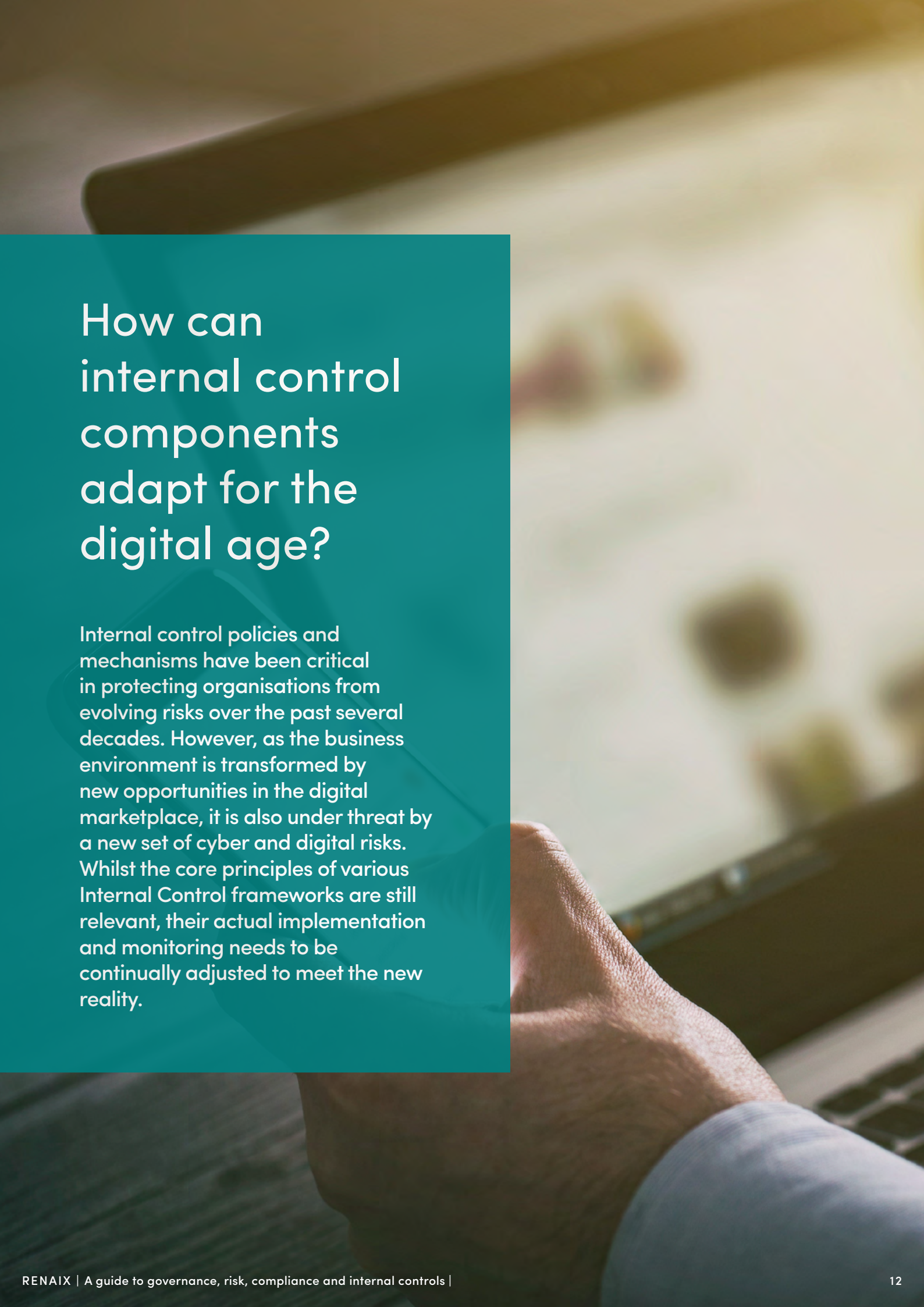
- Many organisations are increasingly focused on new emerging risks such as cyber crime, fraud, financial crime and so on. However, there are newer risks on the horizon as well – such as those emerging from the use of virtual currencies or artificial intelligence.

- One of the most obvious trends in compliance has been the rise of RegTech. The use of RegTech platforms cannot only help reduce compliance costs, but also assist in finding threats that otherwise would have remained unseen. For transaction-heavy business, RegTech tools can provide near instantaneous fraud detection and help companies reduce losses from fraud and unauthorised access. RegTech remains a top area of focus for companies, developers and regulators alike.

- Another popular trend in the compliance function has been that of continuous compliance. Rather than monitoring thresholds at set intervals, compliance tools can act as surveillance systems that continuously monitor the environment and raise an alarm when anything seems out of place. This is especially useful in today's fast paced business environment where a breach or error can cripple a business in a matter of hours.

Conclusion

The compliance function has not only evolved with technology, but it has also grown in its role. Rather than being just an advisory function, it is now right at the vanguard – protecting businesses from all sorts of risks. With the digital transformation of business, compliance departments have had to become more agile and responsive, in addition to being thorough and meticulous. The focus now is on meeting new challenges in a cost-effective manner and using technological tools, bespoke employee training and RegTech innovations to optimise the compliance function.



How can internal control components adapt for the digital age?

Internal control policies and mechanisms have been critical in protecting organisations from evolving risks over the past several decades. However, as the business environment is transformed by new opportunities in the digital marketplace, it is also under threat by a new set of cyber and digital risks. Whilst the core principles of various Internal Control frameworks are still relevant, their actual implementation and monitoring needs to be continually adjusted to meet the new reality.

Here are how some of the core internal control components need to adapt to the digital age:

Control Environment

The digital environment is a whole different beast compared to what organisations have been used to previously. Many companies might be content with just hiring a few experts who understand this new environment, but clearly this is not enough. The senior management team has to dive in and understand the organisation's new cyber profile.

Risk Assessment

The risk profile of the organisation can change every year. As the tools with which we do business and communicate change, so does the makeup of the risks that we face. Organisations have to be fully aware of how their operations, reporting mechanisms and compliance objectives are changing. New cyber and digital risks will most certainly have an impact on the existing mechanisms and objectives needing to be addressed.

Control Activities

As the risks evolve, new procedures are developed to manage them. These procedures must then translate into control activities. The control activities to manage cyber risks must take into account the unique aspects of each technology and its limitations.

Information and Communication

As more cyber risks are monitored, the amount of information that needs to be generated and reported also increases. It is important to identify that the information is critical to the internal control function and ensure that the said information remains of the highest quality. Information itself is useless unless it can be communicated effectively and to the right stakeholders, internally as well as externally, using the appropriate channels.

Monitoring Activities

Monitoring is what determines the effectiveness of the control policies, procedures, activities and communication channels in place. The process of selecting a suitable evaluation methodology must be formalised to ensure that the control mechanism is working as intended. Deficiencies need to be identified and communicated to the relevant stakeholders. Finally, corrective action must be taken and improvements made to the process in a timely manner.

Conclusion

The digital revolution provides ample opportunities for companies to optimise their internal processes and even expand their business footprint. However, with these opportunities come a unique set of cyber risks and threats. Too often companies don't take these risks seriously and it can lead to losses, legal exposure or even regulatory penalties. Companies must therefore make a sincere effort to update their internal control policies, procedures and activities for the digital age. This will not be a one-off exercise either. The rapid pace of technological advancement means that the risks evolve continuously and so therefore must the mitigants.

How is corporate governance preparing for the future?

2018 has been a rather hectic year for Corporate Governance professionals. Issues ranging from board diversification to executive pay as well as increasing stakeholder interest in social and environmental issues etc. has kept everyone on their toes. Whilst it is indeed a good sign that stakeholders are demanding companies to be more socially responsible, there are some serious emerging risks as well. These range from ever-evolving cyber threats to regulatory and environmental concerns. How can you therefore prepare your organisation for the future?

- The first step towards good governance is selecting the right board. Investors and other stakeholders are increasingly looking for more experience, diversity, initiative and commitment from board members. The focus is shifting more towards stewardship and accountability.
- Compensation is another hot topic with executive pay under the spotlight across the world. Stakeholders are ever more conscious of how incentive schemes are structured and performance rewarded. Pursuing fair remuneration should not stop just at the executive level either. Ensuring that staff members at all levels are fairly compensated is key to minimising the risk of internal fraud or breaches.
- The employee feedback loop continues to be the most fundamental way for management to take the pulse of the organisation. It is important to encourage employees to speak up when they see something that is off and report it to the right authorities without fear of retaliation. In addition to encouraging whistle blowing, periodic surveys to assess the mood of the organisation might also help. It can be enormously beneficial if employees are aligned with the vision and goals of the organisation .
- It is the responsibility of management to ensure Diversity and Inclusion (D&I) at all levels of the hierarchy. Surveys have shown that D&I can increase productivity as well as employee morale. Additionally, a more diversified workforce is generally more creative and likely to spot hidden trends.
- Although good governance means managing all risks, special emphasis must now be placed on cyber risks. Rather than treating it as the responsibility of the IT department, each individual should be made aware of the potential risks and know how to mitigate them. This is not only a technical subject, but also requires redefining roles and responsibilities, authority levels and backup plans.
- With an increasing consciousness around environmental and social issues, the focus is steadily shifting from shareholder management to stakeholder management. Businesses are corporate citizens and as such they must ensure they are having a net positive impact on everyone around them. It is not only about managing reputational risks, but moreover ensuring business is conducted responsibly for the sake of our planet.

Conclusion

The era of only looking at the numbers is long over. Consumers are becoming ever more conscious about how much they consume and their own carbon footprint, as well as the social impact. This translates to greater corporate scrutiny and the new Corporate Governance paradigm must take all of this into consideration. The companies that are likely to be customer favourites in the coming years will likely be the ones which lead in terms of ethics, governance and responsibility, in addition to delivering the numbers.

Thank you

if you enjoyed this guide, then look out for the next one...

RENAIX Ltd.
5A Underwood Street London N1 7LY
United Kingdom
+44 (0)20 7553 6320
info@renaix.com
www.renaix.com