THE Network
Integrated GRC Solutions

Battling Your GRC Demons

Solving The Top 5 Concerns of Compliance Professionals

A GRC WHITEPAPER
FROM THE NETWORK

Solving The Top 5 Concerns of Compliance Professionals

A WHITEPAPER
BY THE NETWORK

Organizations face mounting pressure to deal with their ethics and compliance infrastructures. Increased scrutiny, global regulations, enforcement actions, and the reputational need to be viewed as a company driven by ethical culture have led compliance leaders to seek out new ways to meet their objectives.

There are inherent risks for companies operating in today's complex business world, which can be largely impacted by the actions of their employees, customers and business partners. Regulators are cracking down on violating companies. Demands for information – demands that are higher than ever and that will only continue to build – are coming from regulators, executive management and the audit committee. Executive leaders need to be able to make strategic decisions with an informed, risk-based approach.

There are many GRC movements underway, including endeavors to operationalize GRC as an integral part of doing business on a day-to-day basis. Engaging the employee base and empowering them to be part of the compliance initiative, instead of just being subject to it, has also become a driving factor in how more innovative leaders are finding success. This collaborative risk strategy is what GRC pundit Michael Rasmussen calls engaging the "coal face" of the business – the front lines of the enterprise where policy must become de facto operating procedure if compliance is to actually make a bottom-line difference to the organization.

Instead of the old school ad hoc approach, where high-risk areas garner the majority of compliance resources, organizations are looking to an integrated process where they can manage cross-enterprise issues (large and small) in a more centralized fashion. This has required a value-centric view of the ROI of ethics and compliance, bolstered with better metrics and risk analysis capabilities so these organizations can see risk three-dimensionally. This, in turn, allows organizations to deal more effectively with misconduct and illicit behavior when it

Five Areas of Compliance Concern

While the compliance function and responsibility varies according to industry and company size, the primary focus of the compliance practitioner is to establish standards for ethical business conduct.

The Network has identified the five areas that address the "bigger picture" for ethics and compliance – areas where compliance teams must excel in 2014 if compliance is to make a positive difference within the organization.

- **Making Compliance a Concern for Leadership**
- **Employee Engagement**
- **Driving a "Speak-up" Culture**
- **Managing Potential Risk of Doing Business with Your Partners and Vendors**
- **Globalizing and Socializing Compliance**

occurs, and allows them to keep an eye toward how issues can be prevented in the future.

How are successful organizations accomplishing this? What can enterprises that are truly vested in using better compliance to drive performance do to raise the bar? What trends are happening now in the GRC space that will add to an organization's level of protection and defensibility?

In working with a multitude of diverse companies and institutions, we have identified five initiatives that are and will continue to be critical for compliance success well into 2015 and beyond. While specific issues remain high priorities – such as the mobile enterprise, social media risks, globalization, bribery and corruption, workplace and employment law, regulatory change management, to name only a few – the five areas discussed here are intended to address the "bigger picture;" a maturation of ethics and compliance as essential drivers required for organizations to remain viable and thriving.

> "That fact of life for compliance executives means that for them to succeed, they should master the art of working with and leveraging resources in other functions (legal, IT, HR, and internal audit) to achieve compliance goals, and they should continuously communicate to management and the board that a strong compliance function is a valuable strategic asset that not only focuses on risk avoidance, but also looks to find ways to gain strategic advantage from intelligently managing risk. "
>
> *Compliance Trends 2013, Deloitte and Compliance Week*

1. Securing a Seat at the Table

But first, compliance leaders must work to get a "seat at the table," to demonstrate the ROI of great compliance to senior executives and the board of directors. It's all about accentuating the positive – positive visibility of the benefits of good compliance and an ethical culture, as well as the positive recognition of a well-run program.

But first, compliance leaders must work to get a "seat at the table," to demonstrate the ROI of great compliance to senior executives and the board of directors. It's all about accentuating the positive – positive visibility of the benefits of good compliance and a ethical culture and the positive recognition of a well-run program.

In most companies, leaders set priorities for employees, and the organizational structure can send a message to employees as to what these priorities are. Employees need to know that ethics and compliance are not to be taken lightly. All too often, compliance draws executive (and public) attention only when things go wrong. Accountability aside, leaders look for holes in the dam where the process broke down. Blame is almost always reactionary. A proactive approach, on the other hand, calls for compliance leaders to show value in initiatives that work to strengthen policies and procedures so that those bad actors never get on the stage.

Compliance professionals need to align compliance with strategic goals, presenting key risk issues and trends when pursuing certain opportunities and assessing the state of compliance with regulations, in order to proactively mitigate risks. One key way to do this is using continuous monitoring tools and integrated reporting systems that work to proactively detect risk and deliver strategic value to the company.

Compliance leaders should leverage two types of metrics to drive this proactive, strategic vision: first, implement systems to measure the effectiveness of the program (such as training certification, hotline benchmarking and employee surveys); and second, address specific high-risk areas (those indentified through audits and monitoring).

Continuous incident monitoring systems and integrated GRC systems allow organizations to merge monitoring results into their ethics and compliance strategies and provide greater insight into the effectiveness of a corporate compliance program.

Aside from quantitative ways to prove value, an independent compliance function that reports directly to executive management or the board of directors is able to command respect within the company.

Survey results show that 27% of chief compliance officers report formally to the CEO, a statistic that is on the increase, while about the same percentage reports to the legal function within the organization. Less than a quarter reports to the board of directors. The remainder report to the chief financial or risk officer, to the audit committee, or to another functional area.[2]

By communicating risks to senior management and garnering respect, the compliance function stands to gain more resources, as well as the ability to use current resources more effectively to mitigate risks. In addition, compliance professionals need to position potential violations as opportunities to improve programs and increase their resources. By doing so, they grow the credibility for their compliance function as an essential element of the business.

To complete the cycle, the added credibility and resources convey to employees that ethics and compliance is viewed as a “serious undertaking” by the organization.

2. Keeping Ethics Top of Mind Amongst Employees

An uneducated employee is a company’s greatest risk to upholding its reputation and competitive edge. An individual who is not aware or does not understand company values or guidelines may behave in an unethical manner and cause disruption internally or externally. Companies spend lots of money trying to address this issue but are jaded from wasting their resources on ineffective training. Moreover, companies often have trouble maintaining the same awareness level regarding compliance topics throughout the year. The number of reported incidents often increases immediately after training, then decreases again over time

The DOJ and SEC look at “whether a company has taken steps to ensure that relevant policies and procedures have been communicated throughout

the organization, including through periodic training and certification for all directors, officers, relevant employees, and, where appropriate, agents and business partners." In addition, the information must be presented in a manner appropriate for the targeted audience.

Training not only needs to be memorable, but it also needs to be culturally and professionally relevant. Ethics and compliance issues can have serious implications for companies, and employees need to be made aware of company policies in a manner that does not trivialize the respective issues (e.g., by over-using humor, sarcasm or parodies in training).

"Typical" ethics and compliance cycle...

Companies should provide their workforce a memorable experience when communicating with them and educating them. This can be done by providing employees a centralized portal in which they can consume interactive policies and training, which will encourage employees to take part in nurturing an ethical culture as active participants rather than passive listeners. Companies need to deliver policies and training that are memorable, relevant and informative. Companies can also deploy refresher communications to maintain the same level of awareness throughout the year.

...compared to an integrated system, where risk identification and communication are constant parts of the workflow.

In today's global workforce, many workers are constant travelers and are provided mobile devices by their companies. Companies need to address the compliance needs of these workers as well and keep ethics top of mind when those employees are outside the office, and possibly traveling to risky environments or participating in business engagements that involve risk. Companies can extend the reach of their compliance programs by providing their employees the ability to report issues, read and attest to policies, and receive training and other communications – all on their mobile devices.

3. Overcoming a "Speak-Not" Culture

Fewer reported incidents do not mean that risks are low, or that there are fewer problems. It may just mean that people don't trust the system, either because they are afraid of retaliation, or because they do not believe their reports will make a difference. And there is always the possibility of hidden risks, issues that lurk just outside of accepted company policy, business processes and activity that could lead to unethical practices.

When it comes to ethics and compliance issues, millennial employees (GenY) are the most at-risk generation in today's workplace. Due to their work environment and personal characteristics, they are more likely to engage in

and observe misconduct, and also to experience retaliation for reporting it. Millennials are our future business leaders. If they do not feel confident or safe in voicing their concerns, their takeaway will be that compliance programs are a futile effort. The result could be that, over time, their commitment to their work and to doing the right thing will diminish. Even more disturbing is the thought that we are teaching our future business leaders that ethics and compliance initiatives are useless – imagine what the companies they will lead will look like? The millennial workforce, as with most employees, values organizations that are willing to do the right thing and are aligned with their own personal values and morals. They want to be able to see a dedicated effort toward ethics and integrity in action in their workplace.

Compliance needs support from both the executive level and middle management. Senior leaders need to set the tone for the entire organization by reinforcing the importance of reporting any issues so the company can act proactively address them. Employees need to be informed that their identity will be protected and they will not be subject to retaliation. They also need to be assured that their voice matters and the company will assign appropriate disciplinary actions.

Immediate supervisors of millennials need to stress ethics and compliance messages, as they are more likely to have a direct influence on them than executives. Since younger workers are relatively inexperienced and more influenced by social interaction, companies should also emphasize the resources of their ethics and compliance program as opportunities to interact with knowledgeable people who can provide guidance and support. Further, leaders need to reassure employees that reporting is safe and effective, and that they will stay informed throughout the investigative process.

4. Addressing Third-Party Risk

An organization can face reputational and economic disaster by establishing or maintaining the wrong business relationships. The negative results of bad third-party relationships – dissatisfied customers, unexpected customer financial loss, interactions not consistent with institution policies, inappropriate recommendations, security breaches resulting in the disclosure of customer information, and violations of laws and regulations – are all examples that could harm the reputation and standing of the institution. Any negative publicity involving the third party, whether or not the publicity is related to the institution's use of that third party, could result in reputation risk. FCPA and money laundering violations have received much press due to the big-name companies and enormous fines resulting from corrupt dealings with foreign third parties.

Further compounding this dilemma is the fact that regulatory bodies such as the FDIC, SEC, FFIEC, OCC, OIG and others are increasing their focus on potential third-party risks. They want to see organizations proactively identifying potential risks, verifying that business partners and their employees are compliant, monitoring for changes that might create new risks or compliance gaps, and managing the investigation and remediation of

incidents.

Many companies will drop a potential third party upon even the rumor of bribery without any hard proof. This can be a strategic risk in and of itself, as a company's business base can quickly deteriorate from this practice, and competitors not as adverse to these risks can move forward doing business with these former partners, further increasing the impact of this "drop."

Even customers can be considered a source of third-party risk. For example, financial services companies need to implement monitoring controls to mitigate money-laundering risk for customers engaged in online banking. Understanding expected customer activity, monitoring for unusual or suspicious transactions, and maintaining records of electronic funds transfers are all ways in which financial services organizations can bolster their third-party compliance programs.

Compliance officers need to ensure they are building a relationship of mutual trust with their business partners. All companies must have due diligence procedures in place to assess third parties during on-boarding and monitor the risk involved throughout the lifecycle of their relationship. Risks need to be identified as to where and how non-compliance can occur, as well as the likelihood and severity of an occurrence. It's particularly crucial that companies understand the relationships of their partners with foreign officials.

Companies should look to deploy their compliance program policies and training to their third parties with the same diligence as their internal efforts, to ensure their partners share the same expectations and commitment to ethics when conducting business. Companies can also survey their third parties to assess their understanding of the compliance program's content.

In addition to constantly and consistently monitoring third-party activities and performing risk-based assessments, companies need specialized investigative procedures to look into incidents involving third parties. Keeping an audit trail of all activities associated with third parties will assist in this endeavor. This will allow companies to vet their third parties actions and avoid unnecessarily losing business.

5. Dealing with a Wide-Open World

We live in an ultra-connected world, and two risk areas – data privacy and social media – require constant vigilance by compliance practitioners. Many companies maintain confidential information regarding their customers, and keeping that data secure is essential to the company's business. These organizations need to act quickly in the event of a data breach or socially engineered attack that could allow unauthorized entry into the corporate network.

For the most part, these are IT security issues – not strictly the arena of compliance officers. According to Michael Rasmussen, however, "Identity and access governance is a critical enterprise GRC technology. Many risk and

compliance issues boil down to who has access to what in both the physical and logical environments and whether that access is rational and justified. This includes making sure individuals are trained and aware of policies appropriate for the level of access they are given."

Exposed confidential company information may also result in reputational risk as well as a loss of competitive edge. Activities that result in dissatisfied consumers and/or negative publicity could harm the brand and standing of an organization, even if the company has not violated any law. This could include employees posting negative comments about their company or coworkers via social media.

More than 1 out of 8 millennials find it acceptable to blog or tweet negatively about their company. In addition, fraudsters can masquerade as a company using social media as their outlet, which can also damage the company's brand. All are reasons why compliance teams need to re-focus their efforts on ways to protect company information and set strong policies concerning social media.

To maintain this level of protection, companies need to implement controls (such as policies and training) that clarify which employees have the access or authority to speak for the company and what information is not permissible to share. Companies must remind employees routinely of their social media responsibility, including their liability for comments posted on personal accounts.

In addition, companies need to implement tools that enhance situational awareness and detect and predict potential sources of fraudulent behavior, to prevent malicious attacks. Having a compliance-focused crisis management plan in place will allow organizations to mitigate the impact of attacks that have already occurred.

Summary

The role of compliance has shifted dramatically in just the last few years from one of "corporate cop" to focusing on the overall integrity of the organization and the value proposition that ethics can offer. Constant regulatory change, increasing audit demands and near-static compliance resources are obviously concerns as well for today's compliance chief – issues that are being addressed by constantly evolving technology, most especially the growth of integrated GRC systems. While the compliance function and responsibility varies according to industry and company size, the primary focus of the compliance practitioner is to establish standards for ethical business conduct. And although this role also calls upon them to be the creator and enforcer of corporate policy, with all due consideration paid to audit analysis and compliance metrics, carrying the torch of an ethical, integrity centered organization will continue to be objective number one for the successful compliance officer – today as well as tomorrow.

REFERENCES

1 *"A Record Year for Corporate Criminal Fines,"* Jeff Kaplan, Conflict of Interest Blog, January 2, 2013

2 *"State of Compliance: Deeper Insight for Greater Strategic Value,"* PricewaterhouseCoopers LLP, June 2013

3 *"Resource Guide to the U.S. Foreign Corrupt Practices Act,"* Criminal Division of the U.S. Department of Justice and the Enforcement Division of the U.S. Securities and Exchange Commission, November 2012

4 *"Generational Differences in Workplace Ethics,"* Ethics Resource Center, June 2013

ABOUT THE NETWORK

The Network is a leading provider of integrated governance, risk and compliance (GRC) solutions that allow organizations to create better workplaces and ethical cultures. The Network's Integrated GRC Suite, recognized as the "Apple of GRC" by GRC 20/20, is the first natively integrated enterprise GRC software platform in the compliance industry. The Suite was built to leverage the way employees retain and apply ethics and compliance information and helps companies prevent, detect and remediate non-compliance and unethical conduct. A SaaS-based technology solution, the Suite integrates policy management, training and communications, Code of Conduct, surveys and assessments and case management, all on a reporting and analytics platform. Originally established as the first whistleblower hotline provider in 1982, The Network serves thousands of organizations in every industry, including nearly half of the Fortune 500.

THE Network
Integrated GRC Solutions

For more information about The Network,
call 1-800-357-5137 or visit www.tnwinc.com

grc 20/20
Technology Innovator
2013
© 2013, GRC 20/20 Research, LLC