

REPRINT

R&C risk & compliance

# CULTIVATING A CULTURE OF COMPLIANCE

---

REPRINTED FROM:  
RISK & COMPLIANCE MAGAZINE  
JAN-MAR 2018 ISSUE



[www.riskandcompliancemagazine.com](http://www.riskandcompliancemagazine.com)

Visit the website to request  
a free copy of the full e-magazine

MITRATECH

Published by Financier Worldwide Ltd  
[riskandcompliance@financierworldwide.com](mailto:riskandcompliance@financierworldwide.com)  
© 2018 Financier Worldwide Ltd. All rights reserved.

MINI-ROUNDTABLE

# CULTIVATING A CULTURE OF COMPLIANCE



**PANEL EXPERTS****Jason Cropper**

Vice President, Business Development

Mitrotech

T: +1 (512) 646 8867

E: [jason.cropper@mitrotech.com](mailto:jason.cropper@mitrotech.com)

**Jason Cropper** has over 10 years of experience in the software industry and is focused on helping organisations execute best practices in the area of information governance, risk and compliance. As Mitrotech's subject matter expert, Mr Cropper promotes the concept of total risk management with the goal of helping organisations bridge typical functional silos, to promote a culture of compliance and establish effective compliance programmes.

**Mark Delgado**

General Manager, EMEA &amp; APAC

Mitrotech

T: +44 (0)1628 600 900

E: [mark.delgado@mitrotech.com](mailto:mark.delgado@mitrotech.com)

As general manager of EMEA and APAC at Mitrotech, **Mark Delgado** works with the leaders of the company's sales, services and support organisations globally to provide senior leadership for customers and prospects. He also has responsibility for the company's partnerships and strategic alliances. Mr Delgado joined Mitrotech via the acquisition of Hitec (Laboratories) Ltd where, as chief technology officer, he gained more than 22 years of experience in information management, governance, risk and compliance, policy and risk management.

**R&C: To what extent are you seeing a greater focus on compliance efforts among companies in today's business world?**

**Cropper:** There is no question that compliance has a greater focus today than it did 10 years ago. Since the Wall Street crash in 2008, daily alerts in regulatory activity are up 600 percent, globally. However, it is not just activity that is on the rise; compliance spend, compliance hiring and regulatory fines have never been higher. The need to hold organisations and individuals accountable for compliance related breaches is more visible and public in nature. There is significant pressure for organisations to demonstrate their compliance and, more importantly, to prove they are doing it effectively.

**Delgado:** It is not just the significant increase in regulation that has been at the root of the clear increase in the focus on compliance, especially in highly regulated businesses around the world, but it is also the accompanying clout that has been given to many of the regulatory authorities. Fines are now truly punitive and the shift from corporate to personal liability is a highly significant factor in driving the ever-greater importance businesses are placing on compliance.

**R&C: In your experience, do companies tend to fall short when it comes to assigning responsibilities for compliance and risk within the organisational structure? If so, how can they improve their efforts in this regard?**

**Cropper:** From my experience, it is not so much that they fall short in assigning responsibilities for risk and compliance, the issue is more that many do so purely as a tick-box exercise. There is no accountability, and this is where the rise of regulatory guidelines around what constitutes effectiveness in compliance comes in. The Department of Justice (DOJ) recently released a whitepaper on 'evaluation of corporate compliance programs', which went further than the typical guidelines by providing challenging questions that addressed the issue of whether an organisation truly had a culture of compliance, or was merely doing what it had to, to remain compliant. An organisation will never truly improve its efforts unless it ethically believes in compliance and promotes that throughout the organisation.

**Delgado:** There is no doubt that businesses are more aware of the importance of responsibility assignment – not least because many regulators are now insisting on this being a formal component of being compliant. The real issues come from whether or not these assigned responsibilities are understood

clearly enough by the individuals themselves and others in the wider business and, then, if those with assigned responsibilities are properly held accountable for any failings. As with so many areas of compliance, technology has a key role to play here, not necessarily in assigning responsibilities, but in ensuring communication of these assignments is clear, both within and outside of an organisation.

**R&C: Is it important for companies to start with the right tone at the top to cultivate a culture of compliance? What strategies might be deployed to make a company's commitment to compliance and ethics more than just a box-ticking exercise?**

**Cropper:** It is critical. Compliance has to start at the top; however, that is where the tick-box exercise can creep in. Regulators are highlighting the fact that organisations need to demonstrate 'the tone from the top', and therefore organisations oblige, but miss the true objective. Although creating a culture of compliance needs to start from the top, the end goal is to promote compliance and embed and operationalise it throughout the organisation. In doing so, you actually end up with compliance running throughout every process and procedure and across every function of the business. 'Top-down'

compliance results in a 'bottom-up' compliance. One of the most effective strategies to encourage bottom-up culture is to provide an environment where employees feel comfortable in reporting breaches or near misses of compliance. Demonstrate and reward such activity, and make it easy to do so with tools, technology and processes. After all, it is

**"It is very easy to talk about a culture of compliance, but far harder to define what this means in reality, and even harder to then embed this within an organisation."**

*Mark Delgado,  
Mitrtech*

good business to do so: the cost of non-compliance is known to be almost three times that of remaining compliant.

**Delgado:** It is very easy to talk about a culture of compliance, but far harder to define what this means in reality, and even harder to then embed this within an organisation. Really, it is all about instilling an environment where calling out non-compliance is actively encouraged and practices to gain or improve compliance are actively rewarded. A successful

culture of compliance should result in everyone in the business being able to answer questions like “What does compliance mean to me and how does it relate to my role?” The right tone from the top is certainly vital. Employees need to believe that everyone is held to the same high standards and, importantly, what the repercussions are if those high standards are not met. One important way of helping with this is by ensuring not only that compliance policies are comprehensive, up-to-date and have been read and understood by all relevant employees, but that these policies are referenced directly by relevant operational procedures. These procedures should clearly state what escalation or exception mechanisms are in place for non-adherence and they should be formally affirmed by all employees involved.

**R&C: To what extent do you believe technology can enhance collaboration between the different functional organisations within an enterprise? How common is it for departments or groups to develop a silo-based mentality when it comes to compliance?**

**Cropper:** The risk and compliance technology market is on the rise, and for good reason. Many organisations have managed risk and compliance

as ‘siloed’ functions for a long time, and in creating these silos they are not utilising business critical data. When you look at governance, risk and compliance (GRC) maturity models, the objective is to embed and operationalise GRC initiatives across every function of the organisation, and share the same

**“Many organisations have managed risk and compliance as ‘siloed’ functions for a long time, and in creating these silos they are not utilising business critical data.”**

*Jason Cropper,  
Mitrtech*

knowledge to help make better decisions for the business. This is almost impossible to do without leveraging a technology platform which provides visibility and predictability to the organisation. An example of this is with the increasing collaboration between the legal, risk and compliance functions. The risk function focuses the organisation’s attention on the areas of highest risk, the compliance team implement strategies and processes to help mitigate the highest impact risks and the legal team can use this data to ensure they utilise their legal spend in the areas which provide the most value to the business.



Without a common technology platform, this level of visibility and connectivity is not possible.

**Delgado:** Silos exist more where there is an absence of collective responsibility for compliance or an absence of a common approach to becoming compliant which, to a great extent, is technology-oriented. Very few compliance programmes can be truly executed by a single group or department. Most successful initiatives have cross-functional touch points and many affect a significant proportion of the business. Technology is essential in the efficient implementation of any compliance programme, but can either help eliminate siloed thinking or further embed it. Technology for compliance, like any enterprise wide function, needs to be thought about exactly that way – enterprise wide. A holistic approach to the technology used for management of risk, the management and dissemination of policy and other corporate-wide compliance activities can really help everyone in an organisation look to solve their compliance problems in the same ways, using similar methodologies. Corporate-wide platforms also, of course, ensure that compliance reporting is standard across functions and across initiatives and provide clearer and more consistent compliance health understanding and visibility companywide.

**R&C: Do you believe companies need to encourage employees to ask questions of direct managers, human resources, the**

**legal team or other colleagues, to flag potential compliance problems before they snowball into more serious issues?**

**Cropper:** This goes back to creating a culture of compliance – enabling and promoting whistleblowing and incident reporting is a critical component of this. It is also an area that frustrates me as many organisations seem to want to hide compliance breaches, yet evidence proves that it works in your favour to self-report. The US Securities and Exchange Commission (SEC) whistleblowing campaign demonstrates this well, having awarded more than \$162m to whistleblowers since its creation in 2011. These whistleblowing activities resulted in more than \$1bn in fines and penalties to organisations. It just does not pay to be non-compliant, or to hide it. Given that the Federal Sentencing Guidelines for organisations offer up to 95 percent reduction in potential fines if you can demonstrate an effective compliance programme and self-report the breach, such activities should not be overlooked.

**Delgado:** This is a fundamental and significant gauge on how well the culture of compliance initiative is working within an organisation. In many cases, it will be appropriate for employees to be able to voice their concerns anonymously and to have confidence in that process. Indeed, many companies are now taking this one step further and actively

incentivising employees to come forward and flag not only potential compliance breaches, but any operational weak or blind spots they can see. This will help create a real, tangible culture of continuous improvement.

**R&C: What general advice would you offer to companies in terms of establishing an across-the-board attitude to compliance throughout their organisation?**

**Cropper:** I would offer two pieces of advice. The first is to 'mean it'. Organisations that conduct 'tick-box compliance' never truly reap the rewards that a true culture of compliance brings. In order to establish true across-the-board compliance, you need to have an ethical approach to compliance. The second area of advice is to really consider the objective of your compliance programme. Too many people conduct compliance activities to satisfy regulatory requirements. Proving you trained your employees on a subject is a tick-box exercise. Providing the tools and processes that are effective in managing and changing the employee's behaviour to be more ethical and compliant is the goal. Pay more attention to the objectives, and spend time monitoring their true effectiveness, not simply monitoring if they were done.

**Delgado:** Companies must ensure that employees believe and trust that the organisation is serious about compliance and, just as importantly, that behaviour that puts compliance at risk will not be tolerated. I am not talking about finding the occasional scapegoat to publicly name and shame, but an impartial and fair corporate-wide enforcement of adherence to what the company lays down as its compliance guiding principles. There is a great deal to be said for leading from the front here. Leadership at all levels in a business need to run their teams reinforcing the company compliance culture and clearly defining what that means to employees on the ground.

**R&C: How do you envisage the compliance landscape evolving in the months and years ahead? To what extent are the legal and regulatory demands on companies only set to increase, making the corporate compliance function an essential part of any successful business?**

**Cropper:** Compliance is still on the rise, and I do not see this changing anytime soon. There is, however, a perception from the corporate world that as compliance hiring is slowing down, and fines and penalties are stabilising, 'the need to comply' is not as strong anymore. This could not be further from the truth – they are missing some fundamental insight. The reason why penalties are reducing is



precisely because organisations are investing in people and technology to help them, and they are taking compliance more seriously than in previous years. It is not compliance that is on the decline, it is that organisational GRC maturity is on the rise. Organisations are now able to demonstrate their effectiveness, and are conducting themselves more ethically, and, in turn, regulators are allowing for significant reduction in penalties where breaches do occur. The message is clear – it pays to be compliant.

**Delgado:** In many sectors, the corporate compliance function is already an essential part of a successful business. As regulation increase spreads deeper and more broadly into the economy, inevitably, more and more businesses will make that shift. Much is said about the cost of compliance. For

those companies that are already well down the compliance road, the goal will shift from compliance to more efficient compliance. As with all efficiency drives, technology has a significant part to play in achieving these goals. Compliance IT systems will become more sophisticated, will address a broader range of compliance-oriented activities and will be developed to address specific regulations in a way they do not do today. Predictive analytics, for example, is already helping many organisations spot non-compliant behaviour and even predict the likelihood of breaches before they occur in ways that are almost impossible to manage in a manual way. This technology, and technologies like it, will become more complex and reliable, allowing businesses to achieve a higher level of compliance, but at a lower cost than ever before. **RC**