REPRINT

R&C risk & compliance

MANAGING RISKS THROUGH ETHICS, INTEGRITY AND COMPLIANCE

REPRINTED FROM:
RISK & COMPLIANCE MAGAZINE
APR-JUN 2017 ISSUE

www.riskandcompliancemagazine.com

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

NAVEX GLOBAL®
The Ethics and Compliance Experts

Published by Financier Worldwide Ltd
riskandcompliance@financierworldwide.com

ONE-ON-ONE INTERVIEW

MANAGING RISKS THROUGH ETHICS, INTEGRITY AND COMPLIANCE

Carrie Penman
Chief Compliance Officer and Senior Vice President, Advisory Services
NAVEX Global
T: +1 (971) 250 4100
E: cpenman@navexglobal.com

Carrie Penman is the chief compliance officer of NAVEX Global and senior vice president, Advisory Services. She has been with NAVEX Global since 2003 after serving four years as deputy director of the Ethics and Compliance Officer Association (ECOA). Ms Penman was one of the earliest ethics officers in America. She is a scientist who developed and directed the first corporate-wide global ethics programme at Westinghouse Electric Corporation.

RC: In your opinion, how important is it to incorporate robust ethics, integrity and compliance standards into risk management strategies?

Penman: It is very important. Robust ethics, integrity and compliance programmes are critical elements of any enterprise risk management (ERM) strategy. It is clear from all of the best practice guidelines and regulatory guidance that a strong and effective ethics and compliance programme is expected to be built on a foundation of a comprehensive ethics and compliance risk assessment. Compliance programme elements should then be specifically designed to mitigate the key risk areas identified as part of an overarching risk assessment and strategy process. It is also important to recognise that risk management goes beyond ethics and compliance, and gets into areas of operational risk, reputational risk and financial risk. These risks are typically addressed holistically through an ERM process where compliance is one aspect of the review. Today, many organisations are now also appointing chief risk officers (CROs), and if that person is not the CCO, the two of them should be joined at the hip.

RC: How should corporations go about identifying, quantifying and prioritising the risks they face? Moreover, what strategies and policies can then be developed to assist organisations to map their ethics, integrity and compliance standards to their risk profile?

Penman: We recommend that organisations undertake a thoughtful and focused ethics and compliance risk assessment process. This can be standalone or a subset of the organisations' ERM process. One way to approach this process is to review key documents and interview key leaders and subject matter experts to identify the top risks that should be addressed, along with identifying current mitigation strategies and residual gaps. Those strategies can – and should – include training, policy, procedures and auditing. Throughout the assessment, it is extremely important to look for gaps, and also determine the likelihood of risks actually happening and the magnitude of a particular risk if it were to happen. Think about it like this: it is unlikely that a tornado will hit my house, but if it does, the consequences will be extreme. So, what can I reasonably do to protect my family and assets that is commensurate with the likelihood of the risk? Through all of this, organisations need to know that risk levels will never be taken to zero. But there are steps they can take to mitigate risk to reasonable or acceptable levels.

RC: What role should the board play in setting the tone for prioritising ethics, integrity and compliance?

Penman: The board's role is critical. Strong board oversight of risk identification and mitigation is a key part of best practice frameworks. Boards should review the outcome of risk assessments and resulting mitigation strategies, and monitor the implementation of those strategies. It is important to recognise that boards typically focus on ERM, which includes, but is not limited to, ethics and compliance. Other potential operational risks are often considered more threatening. But bribery and corruption risks most often rise to the level of enterprise risk assessment to be reviewed and prioritised by the board. Boards, typically via an audit, risk or compliance committee, need to review and monitor the subset of identified ethics, compliance and reputational risks.

"Boards, typically via an audit, risk or compliance committee, need to review and monitor the subset of identified ethics, compliance and reputational risks."

Carrie Penman, NAVEX Global

RC: How important is staff training when integrating ethics, integrity and compliance standards into company culture? To what extent can this help employees develop a greater understanding of the importance of such standards in creating long-term value?

Penman: Training and education is extremely important. If done well, it should raise employee awareness – which can help them spot risks and avoid doing something that they do not even realise, at first, could be a problem. To be most effective, training should be risk-based and role-relevant. All employees do not need to receive every type of training; just the training that is relevant to the work they do. For example, every international sales executive should receive in-depth training on bribery and corruption, but a line manufacturing employee likely will not. Training employees on everything is overwhelming and will send a message that the organisation is not thoughtful of their time or responsibilities. Organisations should develop a training and communication plan, based on the outcome of the risk assessment, which identifies the key audiences and success points for each high risk area. It is important to understand that training must be combined with an effective culture of compliance, otherwise employees will view training as just

something they have to get through, or worse, see it as something contradictory to their culture and become cynical about the organisation.

Put another way, if management does not impress upon employees that training is important, or if what is covered in the training runs counter to what the employee sees day in and day out, the best training materials in the world will not work.

RC: What impact is increased regulatory scrutiny having on the way corporations manage the risks they face?

Penman: It is certainly an interesting question at this particular moment in time, given the change in leadership in Washington. Regulatory scrutiny in the US, it is safe to say, is in a state of flux. However, regulatory scrutiny outside the US continues to increase. The corporations that really get the importance and value of compliance understand that there is a competitive advantage to having a strong culture. Regardless of the law, it is simply smart to have employees and managers who are trained and aware and comfortable asking questions. Think of increased regulatory scrutiny as a stick, one that should not be ignored, but the carrot is a happier workforce and more engaged clients and business partners. Enlightened organisations emphasise ethics and compliance because they believe doing so is the right, and smart, thing to do.

RC: What overall advice can you offer to corporations on implementing risk management procedures and policies that harness ethics, integrity and compliance standards?

Penman: Organisations should have robust risk assessment processes, either separate from or a subset of the ERM process, that lead to detailed two to three-year ethics and compliance work plans. These work plans need to be living documents with due dates and with accountable parties clearly identified. And the risk assessment and resulting work plan should be reassessed when an organisation changes its business model, its geographic footprint, its lines of business, and so on, because its risk profile may change and alternate mitigation strategies may need to be put in place. And, when looking at acquisition targets, potential buyers need to be especially cautious and include an assessment of the organisation's risk assessment and risk management processes. Lack of documentation for risk management – or a lack of updated documentation – should be a major red flag.

RC: Do you expect corporate ethics, integrity and compliance standards to become a greater part of risk management in the years ahead? Ultimately, what are the hallmarks of an

effective risk management programme in today's market?

Penman: Organisations around the world are recognising that an ERM process is often not sufficient to cover all risks and that ethics and compliance needs to be elevated. Risk management and compliance are increasingly tied together. We are seeing ethics and compliance increasingly become embedded within best practice strategies, including the United States Sentencing Guidelines and the recent ISO 37001 standard. A lot of corporations were already incorporating ethics and compliance, and indeed elevating it within risk management. The most effective organisations already see risk management as a strategic necessity and are recognising the need to link this with their ethics, compliance, reputational and cultural initiatives. R&C