

CEP Magazine – January 2018 Key compliance concerns for 2018

By Mónica Ramírez Chimal, MBA

Mónica Ramírez Chimal (mramirez@asserto.com.mx) is Partner and Founder of her own consultant firm, Asserto RSC in Mexico City.

Abracadabra, alakazam...what will 2018 make compliance officers be worried about?

Good news! World Bank has forecasted a growing economy in many countries. But, as the countries grow, there will also be scarcity of things such as water and intensive changes in weather, driving migration and natural disasters. This will raise new risks and new issues to comply with.

In a general overview (compiled from various sources and my own opinion), the key compliance concerns for 2018 are as follows.

External to the company

1. Cybersecurity: So many new technologies are arising so quickly, and so much depends on social networks that the compliance officer will have to deal with a new requirement: being an expert in technology. Ransomware, data breaches, engineering attacks—how do you protect the company if you don't know what is going on in the real world?

Cybersecurity also covers the control mechanisms a company has to face cyberattacks, not only for their website, but also for the information sent and received by employees and safeguarded in their servers. How can a company control and face what their employees are posting in social networks? In some countries, the companies are not allowed to check their employees' emails or posts. Meanwhile, others companies can easily block their employees' electronic devices from being used for social media. The dilemma is, how to separate the employee's personal post from a statement on behalf of the company.

Is the company launching a new technological product? If so, has the compliance officer been involved to check the risks that the company could face? Because in so many companies, the compliance officer is the last one to participate.

2. Virtual currencies: The International Monetary Fund has already acknowledged^[1] the bitcoin technology by saying it is effective; it is now analyzed by several large international banks. No matter your position on the subject, there are many countries that have already welcomed virtual currencies as a method of payment. If the company you are working for wants to have a competitive advantage, allowing payments with virtual currencies is one. Again, the compliance officer should have more knowledge. Know what a virtual currency is, how it works, and get involved in the regulation (this will vary by the country). With that, the compliance officer could start assessing the risks the company may face.

3. Terrorism: Let's divide it into two. One, how the company is making sure it is not financing, directly or indirectly, terrorism and, second, the terrorist attacks that may affect it. For the first, what are the key controls the company has to ensure where the payments go and for what purpose? Does the company know its customers,

employees, and third parties? Keep in mind that their actions can affect the company, its image, and its reputation.

For the terrorist attacks: Where does the company do business? Is it a country that is known to support rebel groups, weapons of mass destruction, or terrorism? If so, keep in mind that any facility that the company has there can be destroyed or be used by terrorists. Or, if the company uses that country's port, its products can be easily used to be mixed with explosives or, depending on what the material is, to be used as dual-use goods. (Dual-use items are goods, software, technology, documents, and diagrams that can be used for both civil and military applications. But they can present an extra safety threat because of the risk of terrorism and illicit drug production.) Check if you are at risk and, if so, implement other kinds of controls.

4. Money laundering: The Financial Action Task Force, World Bank, and the International Monetary Fund have included this issue in their agendas. Why? Because it keeps growing internationally and in different forms. "Willful blindness" is a key concept in anti-money laundering regulation that is being used to refer to a person who knows that the crime is being committed but who allows it—in other words, lets it happen...like it has not been seen. The compliance officer shouldn't have willful blindness and should be aware that money laundering is not only happening in the financial sector, but also has expanded to several non-financial businesses, such as restaurants, gas stations, hospitals, malls, agriculture, pawn shops, etc. So many industries that I can't mention one business line that has not been used by a criminal. What are the controls the company has in place to minimize being used by a criminal to launder money? Which areas are more vulnerable to it?

Note: For both terrorist financing and money laundering, has the company trained the compliance officer and personnel vulnerable to the risk on the matter? If they don't understand what money laundering and terrorism and what the characteristics and differences are, how can the company be protected?

5. Modern slavery: We've all heard several times "know your third parties." Know them, because what they do can affect the company you work for. All right. They can operate without a license, they can be a shell company, the owners can be criminals, they can pay their workers an inferior wage, they can hire illegals, but there is also the possibility of an outrageous crime: that they could be forcing people to work in deplorable conditions, as in not having the proper lighting, temperature, or even equipment—yes, in lower conditions than what the laws says—or threaten them, extort them, or even exploit them sexually. How can the compliance officer protect the company from this risk? Do surprise visits. Yes, no matter where the facilities are, just go there without telling them. That's the advantage of Compliance: It can audit as well, whenever it wants to.

6. Corruption: The cancer continues spreading worldwide. So many people think that it is a "harmless crime." Nobody gets hurt, right? Wrong! They do. According to what the company does, the compliance officer should analyze which are the vulnerable areas either to give or receive a bribe and, for those, implement internal controls that help to minimize the risk of corruption. An anti-corruption policy as training will help to do it. Remember: a scandal that the company you work for has been involved in, either by helping or being used to finance terrorism, to launder money, to exploit people, or to be corrupted, could damage the company's image and reputation so severely that the impact cannot be measured—in money and in the consequences of fines, loss of licenses, and even imprisonment. So, take it seriously.

7. Climate change and natural disasters: Let's get real. Very few companies are complying with environmental regulation. Add to this, most of the large companies outsource their workforce in another country that is too far from them. So, they don't pay the attention required to care if indirectly they are contributing to pollution. As we have evolved in technology, producing so many products at a large scale, we have also affected the environment by not paying attention to the waste/residues. We are forgetting that sometimes all that is thrown into the ocean—or left in a field—if not handled as it should be, could become a threat to us. No wonder why the climate is

changing so quickly, and in 2018, we should expect that everything becomes more severe—rains that become floods, cyclones, earthquakes, and other effects such as new or stronger diseases, lack of water supply, and migration all around the world. The compliance officer should have at the top of the list: Make sure that the company is complying with environmental, safety, and hygienic regulations. Not only on paper—test them. Proving the company is really doing it for the benefit, not only of the law, but for all us.

8. Competition: Who would have thought that companies were going to diversify so much, that a supermarket would be the competition to different types of restaurants (e.g., sushi, baguettes and pizzas, roasted chicken) or of a bank or a hospital (in some supermarkets they offer check-ups with a doctor)? Well here is a tough one for a compliance officer: Analyze which businesses can be the direct and indirect competition of the company. And which of those are more positioned in the market. How do you do it? Knowing the key products/services the company offers, its strengths and weaknesses, report it so the company can improve them. Why? You don't want your company to get into bankruptcy; the compliance officer should anticipate any potential risk the company may face! That's their difference with internal or external audit.

This document is only available to members. Please log in or become a member.

[Become a Member Login](#)