COSMOS
Navigate the Compliance Universe

CEP Magazine - February 2019
So different and so alike: Internal audit and compliance

By Mónica Ramírez Chimal, MBA

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

Let me start with a question: If you work in a compliance area, have you worked with the internal audit area? Do you even speak to them? Do you have frequent meetings?

If the answer is that you at least speak to them (and I do not mean just a greeting), you are on the right path. If your answer is that you have meetings or you have worked together with them, you are in one of the few companies that are doing what should be done. In order for you to understand this, let me introduce the two areas.

Internal audit

The audit has been present since time immemorial. There are different types (according to its objective), but in a generic way, an audit is defined as the objective and independent verification of the adequacy and effectiveness of internal control measures. In other words, audits verify that what is being done is what should be done. This is done by auditing or reviewing numbers.

After the financial scandals that led several companies to bankruptcy (e.g., Enron, WorldCom), most internal audit areas began to use the business risk methodology to perform audits. They were forced to know the company's processes in order to identify risks and the controls that minimize them. Therefore, its scope became global, covering the whole company. But as we know, "watchdog" areas are not very welcome in companies, and after the impact those financial scandals have had, not only in the company itself but in the country's economy, people knew they needed reinforcement. Therefore...

Compliance

Compliance arose as a result of all those financial scandals that had a worldwide effect. It arose as an additional control measure to minimize the risks a company is exposed to, specifically, a new powerful risk: reputational—that is to say, the risk that the company's image will be affected.

Due to financial scandals, regulators decided that in order to protect consumers, market integrity, and stability, the companies that must have a compliance officer were those listed on the stock market exchange and those in the financial sector.

Nowadays, the compliance officer has been included as a key control in anti-money laundering regulation as a powerful control to minimize the risk of money laundering.

The objective of compliance is to ensure adherence to laws, regulations, and commitments made both with third parties (contracts, agreements) and internally (code of conduct and ethics, policies, and procedures). This led to responsibility for three main risks: reputational, regulatory, and legal.

Up until now, it was assumed that those working in the internal audit area needed to be qualified accountants, and those working for compliance needed to be lawyers. Many companies keep these as their requirements for hiring staff for these positions, but the truth is that a compliance officer needs to be much more than a lawyer.

Why? The answer is that to assess reputational risk, a compliance officer must start by knowing the company's processes and use the business risk methodology to understand which processes, products, or services make the company vulnerable to risk and which could affect its image.

An element of compliance is making sure that everyone complies with regulations (regulatory risk) and with contracts and agreements (legal risk). In order to protect the company's image, a compliance officer must be involved in processes and in new products the company wants to launch (before they do), in any kind of suit, and of course, they must know in advance how to protect the company from being used for money laundering.

What companies have learned is that hiring lawyers as compliance officers isn't enough. The compliance officer profile has evolved into a mix of the following skills:

- **An auditor**: to review every detail analytically and ask why this is happening.
- **A policeman**: to obtain the information needed and to preserve or restore order.
- **An investigator**: to be able to corroborate all the information.
- **A psychologist**: to understand the behavior of others and persuade others.
- **A marketer**: to promote compliance and the benefits of its work.
- **A lawyer**: to be able to exercise the right of the "must be."
- **A politician**: to exercise the art of diplomacy.

Commonalities

Many of these abilities coincide with the internal auditor´s profile, because although internal audit has a different scope than compliance, at the end of the day, both areas agree that in order to be effective, they must do the same things

Be objective, ethical, and independent

The staff of both areas must have mental and appearance independence to avoid being considered judge and jury or to be in a conflict of interest. Independence in appearance is what third parties would perceive as being independent. Example: If you audit a company and your spouse is the CEO, you would be perceived as having a conflict of interest. Mental independence refers to your state of mind, your values (ethics), and how you act and would make decisions. Example: If you do not like the person in charge of the area you review, would you increase the scope of your review in comparison to other areas? Or would you indicate that the area is riskier, just because you don't like that person? Both internal auditors and compliance professionals should also conduct audits/reviews in a highly ethical, professional manner. Above all, they must exercise skepticism and be impartial.

Be open and accessible

If both areas are in charge of risks, they should be able to develop internal alliances. The only way to achieve that is by ensuring that employees see them as someone who is available to talk—they are open, accessible, and

humble. Most importantly, they protect their whistleblowers, and they do what they say they are going to do.

Report appropriately

There should be a direct report sent to committees that are made up of people who are independent of the company (at least half of the total number) in order to maintain the independence of these areas. Reports shouldn't be sent only to the CEO or general manager. Committees also help to supervise their work on a recurring basis to ensure the objectives, scope, and work are carried out appropriately.

Have the support of senior management

Internal audit and compliance need support from shareholders, members of the board, committees, and the CEO. All employees need to see that they have support and that the audits and revisions can be carried out by the appropriate department when needed—without anyone's influence.

Be up to date on the relevant issues that affect the company

This implies being trained and up to date in risk management, fraud prevention, money laundering, data protection, etc. In addition to having knowledge of new regulations, they need to be aware of the emergence of new risks and news in vogue. For a compliance officer, being up to date on news is also a must.

Carry out follow-ups on detected observations

There is no point in carrying out an excellent review if there is no follow-up on how and when implementation is done to reduce vulnerability.

Have the same authority as the other leaders

If, hierarchically, operations, marketing, human resources, legal, systems, etc. follow the CEO or general manager, then internal audit and compliance must be on the same level.

Have sufficient budget

Both the internal audit and compliance areas need to integrate their team and carry out reviews of other departments or other companies in the group (if any) or in other locations where the company has presence. Additionally, a sufficient budget is needed for the technology tools that facilitate their work.

Have the same risk methodology and definition of risk types

Keep in mind that both manage risk, so having the same risk methodology leads to another benefit: a common language of risk and control. It is also ideal that both areas have a common technology solution in order to be consistent and efficient.

Write their own policies, not all the policies for the company

This is important to note, because many companies confuse these roles. Yes, internal audit and compliance supervise the different scopes of what employees do, but they can't be tasked with writing policies for other areas. Why? Because if that were the case, they would be implementing controls and acting as the first line of defense—thereby losing independence.

Differences

However there are two important differences between the areas:

1. Internal audit considers what has already happened (i.e., it is the detective). Compliance is preventive. Before the launch of new products, services, or contractual agreement, compliance must be present. It must review and verify the data, check if the company has adhered to the regulation, ensure there are no legal breaches, and, above all, prevent reputational risk.

2. Internal audit must audit or review compliance just like any other area within the company. This is included in the Basel Committee on Banking Supervision regulation,[1] which specifically states that compliance and internal audit duties should be separate. The reason: to ensure that the activities of the compliance function are subject to independent review and, in this way, to check its effectiveness. Hence, in risk management, compliance is considered the second line of defense and internal audit as the third.[2]

This is the reason why both areas should be in close communication. Even though they have different scopes, both areas ensure that the "must be" is met. Although compliance can prevent "before it happens" and internal audit detects "when it happened," by cooperating, they can achieve more. They can add more value to the company and, of course, be the best gatekeepers to protect it. As you can see, they aren't so different after all.

Takeaways

- Internal audit considers past events for its reviews, while compliance must be involved before a new product-service or agreement occurs.
- Internal audit is responsible for global risk management of the company, while compliance is in charge of three main risks: reputational, regulatory, and legal.
- Both areas have to be objective, ethical, and independent, and they need to establish internal alliances for their benefit.
- Both areas must be up to date on the relevant issues that affect the company (e.g., news, emerging risks) and follow up on observations issued from audits and reviews.
- Despite their different approaches, it's important that they work together. The company is more protected, and a better and more accurate added value is provided.

1 Base Committee on Banking Supervision, "Corporate governance principles for banks," July 2015, http://bit.ly/2QM7zg9
2 Institute of Internal Auditors, "The three lines of defense in effective risk management and control," January 2013, http://bit.ly/2eHvpUw