

## CEP Magazine – May 2020

# The importance of a comprehensive, risk-based approach to compliance

---

By Mujo Vilasevic, MA

**Mujo Vilasevic** ([mujo.vilasevic@gmail.com](mailto:mujo.vilasevic@gmail.com); [mujo.vilasevic@raiffeisengroup.ba](mailto:mujo.vilasevic@raiffeisengroup.ba)) is Company Secretary & Compliance Officer at Raiffeisen Invest JSC in Bosnia and Herzegovina.

It is fair to say that most of us are accustomed to relying on written laws. Use of “good practices” is also very known, but one cannot conclude that they are primarily depended upon in most cases. In day-to-day business, individuals and corporations prefer to rely on written rules. Not only is this a very practical and stable solution, but it also provides certainty in one’s behavior, which is ultimately part of a collective conscience. So with the wider introduction of the compliance function within organizations—the conscience of the organization itself—it has become very difficult for compliance professionals to provide the basis for certain rules that aren’t based on law, especially when elaborating and explaining their decision-making or opinion-drafting processes.

### Why is this the case?

Most certainly, communication of compliance matters suffers because no other function within the organization gets so personal, with its constant rules of behavior, ethics and integrity standards, what to do and what not to do, how to behave, what to avoid, etc. Without the compliance function, people were familiar with these issues, but they were obviously not properly or systematically governed by organizations. Additionally, compliance enforces the behavior of all “in accordance to the laws” and to be “in compliance with the laws.” These obligations can be made very clearly, and so they are understandable; they are written by lawmakers themselves in a large number of cases. But to demand integrity in decision-making, avoid conflicts of interest, and rely on ethics principles in everyday job operations—that is difficult for all sides involved. In addition, it turns out that such rules are not so easy to find in written laws, bylaws, or regulations.

This can create a stigma for compliance professionals that their decisions are simply based on their own (personal or emotional) judgment, with no strict rules to rely on; that they have a “mysterious way” of figuring out resolutions in individual compliance-related matters; and that their assessments are very interpretative.

Let’s break that stigma.

Many organizations across continental Europe, led by Basel compliance standards,<sup>[1]</sup> have introduced various risk-based approaches when assessing compliance issues, as no compliance professional can rely on their own judgment when there are rules to follow, many of which have matrices and mathematics as supportive evidence.

This is no problem when it comes to regulatory compliance issues, because laws define behavior and respective fines in case of noncompliance. But how can compliance be gained in cases such as conflicts of interest or integrity-related situations? One solution is a comprehensive compliance risk-based approach.

### Achieving compliance with a risk-based approach

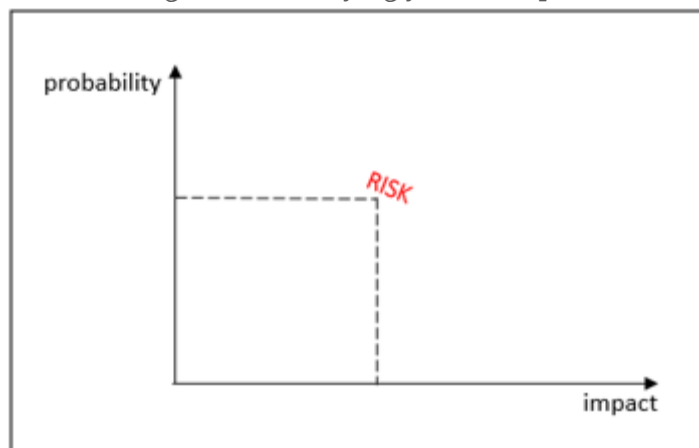
There are obligatory steps that need to be satisfied in any risk management system:

---

1. Define the rules.
2. Have benchmarks.
3. Document the rules.
4. Introduce the rules to the employees, not just by sending mail. Give rules their own life: present them, organize workshops, and make sure that you have employees' attention.
5. Explain to your organization how the rules, compliance function, and everything you do make the entire organization function better.
6. Make yourself approachable and build trust among your colleagues.
7. Ask for feedback.
8. Monitor and control the implementation of rules.
9. Report, analyze, and search for weak spots so you can put them in perspective of the implemented rules.
10. Propose measures and control their implementation.

A large number of organizations have, in this respect, transformed internationally adopted risk standards and matrices with the simple *impact and probability* formula.<sup>[2]</sup> For example, it is not difficult to set up rules that can define, "If [event] happens, the *impact* on us as an organization will be [impact]." (Common examples are financial penalties, loss of clients, and reputational harm). In the same way, the *probability* of an event can be given in length of time (e.g., in three–five years). The intersection between the assessed impact and assessed probability is the *risk spot*, the point to be observed and avoided by establishing rules (Figure 1).

Figure 1: Identifying your risk spot



So, there are specific and countable formulas to determine whether some executive decision within the company would generate certain risks, unfavorable situations, or be so disruptive to business that it is better not to attempt it at all. *The reason behind this is to ensure that both the benefits and risks of each business decision have been weighed.*

In order to comply with the conscience of the European continental system, it is important to document the assessment; have comprehensive, necessary, and detailed information during decision-making; and assess the process in order to properly inform management.

Next, it is very important to communicate the rules to employees and other interested parties. How do you communicate rules, risk assessments, and compliance decisions most effectively? Compliance professionals should explain the solutions they are offering, the problem that they're trying to solve, and why the organization will be better with the application of new compliance rules than it is today.

No one likes change that doesn't bring benefits. A popular argument is, "What's wrong with how things are now?" So to make sure you have the attention of your colleagues and that your compliance methodology or risk assessment (well, the entirety of your compliance rules) are well communicated, it is essential to portray why the current situation (without the compliance rules or if there's a breach) is inadequate. It is not just the financial penalties that justify the need for compliance rules and assessment. Reputational risk and harm come into question for breaches of rules or regulatory demands, as well as because of any integrity risk scandal. It is crucial to try to present this to one's organization in order to get its attention and then move forward with compliance implementation. If you identify the problems with the current state and then offer a solution, you will have the organization's attention, and then you can proceed with a further explanation of the compliance methodology and all related compliance issues. Essentially, you are now free to move forward with the risk-based approach.

Finally, after the rules are communicated, well documented, and made available (via a joint network, a hard copy, etc.), it is important for compliance professionals to monitor implementation and controls, as well as to search for and report weak spots. Of great importance in this step is to not forget that compliance is not internal audit, nor is it a sort of inspector general for each and every process within the institution. It is up to the institution itself to determine the precise scope and methodology of its compliance, as well as the controls it conducts. Such controls are performed on a regular, daily basis through the compliance tasks in general, but they can also be aimed as direct oversight of specific issues, areas, or topics (e.g., third-party assessments). Within this, compliance officers should apply the aforementioned assessment tools, determine weak spots, and introduce necessary preventive and corrective measures in order to achieve compliance. Thus, the full circle of compliance is complete.

If properly documented, communicated, and presented to the organization, these tools can be useful and effective for any compliance-related issue. Compliance professionals will help assess cases of both noncompliance that end up in the media and have mainstream attention and cases that won't stir public interest, so it is important to have a proper methodology that is both well documented and implemented on a daily basis.

## **Marrying compliance with integrity standards**

If an organization wants an individual who will be dedicated to the rules, highest standards, and best practices—no matter whom these practices involve, from bottom to top—then that organization should seek employees with integrity, the highest levels of ethics standards, and impressive personal qualifications. Compliance professionals should be an example of integrity, providing the method of application for rules and standards that are written and need implementation. It is the task of compliance to facilitate this in everyday business for their organizations and to ensure that the decision-making process within the organization is always taking into perspective both the risks and the benefits.

## **Conclusion**

Our efforts on breaking stigmas regarding our decision-making processes for compliance must be continuous. The comprehensive risk-based approach is one tool. However, communication of the rules within organizations, the compliance role itself, and the benefits of compliance have the utmost importance. We must also remember that there is one thing that will keep compliance professionals separate from other risk managers: No compliance professional can ignore the importance of employees' needs in their daily jobs incorporated with the

needs of the organization. One must try to understand the positions of employees, as well as top and middle management, in order to have a comprehensive understanding of each compliance issue. Without this personal approach, it is not possible for an organization to fully comply with necessary rules, and it is impossible to explain to individual employees why they were fined due to a breach of rules and regulations. This approach will help make an organization better over time. It will guide the organization's brand and the organization itself through the simplest and most challenging compliance, ethics, and integrity issues.

## About the author

**Mujo Vilasevic** is a compliance professional with more than six years of experience in the financial sector. He has been published in local and international papers on compliance, corporate governance, and European Union law. Vilasevic currently lives and works in Sarajevo, Bosnia and Herzegovina.

## Takeaways

- Compliance professionals across borders are challenged to identify proper methodologies for compliance decision-making processes.
- The different perspectives of the role of compliance in an organization are highly important for compliance and its implementation.
- Clear communication of compliance-related issues is essential for each organization.
- Ethics and integrity compliance build the basis of a good compliance assessment.
- Compliance professionals must work hard on resolving the stigma regarding their decision-making processes.

<sup>1</sup> "Basel III: international regulatory framework for banks," BIS, accessed February 27, 2020, <http://bit.ly/2TfxwUE>.

<sup>2</sup> Indeed, "How to Use a Risk Assessment Matrix," *Indeed Career Guide*, October 7, 2019, <https://indeedhi.re/385egP4>.

This publication is only available to members. To view all documents, please log in or become a member.

[Become a Member](#) [Login](#)