protiviti®
Global Business Consulting

EBA Guidelines for AML/CFT Compliance Officers Set Tone for Risk Culture and Governance

An analysis of the European Banking Authority's (EBA) guidelines on policies and procedures in relation to compliance management, and the role and responsibilities of the anti-money laundering and countering the financing of terrorism (AML/CFT) compliance officer.

Two of the most important topics in today's discussions involving enterprise risk management (ERM) are risk culture and risk governance. The Committee of Sponsoring Organizations (COSO) defines *risk culture* as the ethical values, desired behaviors, and understanding of risks in the organization, while *risk governance* sets the organization's tone reinforcing the importance of ERM and establishing roles and responsibilities by which decisions about risks are taken and implemented.[1] An honest look at these two aspects within an organization can shed light on whether they are creating a compliance culture that encourages ethical and informed decision-making on money laundering and financing of terrorism ('ML/FT') risks.

As a response to concerns about the exposure of the European financial sector to ML/FT risks which were highlighted in several high-profile cases of white-collar crimes, the EBA issued guidelines[2] on the role and responsibilities[3] of AML/CFT compliance officers and the management body, and how they interact including at group level in 2022. These guidelines are intended to help credit and financial institutions across the EU to better understand the AML/CFT governance structure, emphasizing the need for a strong risk culture that does not pursue profits at the expense of robust compliance, but encourages a proactive approach to risk management, promotes a compliance culture, and fosters an environment of accountability throughout the organization.

[1] Committee of Sponsoring Organizations of the Treadway Commission (COSO). Enterprise Risk Management, June 2017.

[2] EBA Guidelines on policies and procedures in relation to compliance management and the role and responsibilities of the AML/CTF Compliance Officer under Article 8 and Chapter VI of Directive (EU) 2015/849.

[3] According to the EBA, the provisions set out on this guidance should be applied in a manner that is proportionate to the institution's type, size and internal organization, the nature scope and complexity of its activities, and the ML/TF risks to which the institution is exposed.

The EBA recognizes that, without a strong risk- aware culture, an organization may struggle to implement sound and effective AML/CFT governance since it helps to establish a sense of ownership and accountability within the individuals exposed to ML/FT risks. However, the opposite is also true; sound and effective AML/ CFT governance can help shape the risk culture by establishing clear and defined roles and responsibilities in alignment with the regulatory requirements and good practices. In this sense, the EBA outlined4 the key roles and responsibilities for preventing these risks, where the management body sets the tone at the top. By promoting and ensuring that compliance is integrated into their strategy and operations, organizations are creating a path for the company and its employees to follow.

What are the main provisions laid down in the EBA's recent guidelines?

To ensure a common interpretation and adequate implementation of AML/CFT internal governance arrangement across the EU, by competent authorities and credit or financial institutions, in line with the requirements of the EU Directive 2015/849,[4] the EBA issued these guidelines, which came into effect on December 1, 2022.

By doing this, the EBA not only exercised its legal duty to prevent the use of the EU financial system for ML/FT purposes, and its mandate to lead, monitor and coordinate the EU financial sector's fight against these risks[5], but it also contributed to the development of risk-aware cultures and governance structures within financial institutions, shedding light on the interconnectedness of these elements.

While these measures are primarily designed to address and mitigate financial crime risks, they also have a broader positive impact on an organization's overall risk management capabilities.

The Management Body

The guidelines highlight the crucial role that the management body plays in setting the AML/ CTF strategy, ensuring adequate resources, and fostering a culture of compliance throughout the organization, by outlining the following provisions:

- In its supervisory function, the management body should be responsible for overseeing and monitoring the implementation of the internal governance and internal control framework to ensure compliance with the AML/CFT strategy and applicable requirements in the context of ML/FT.[6]
- In its management function, it should be responsible for implementing the AML/CFT policies and procedures, and the appropriate and effective organizational and operational structure necessary to comply with the AML/ CFT strategy.[7] Furthermore, it should take appropriate steps to ensure remedial measures where necessary.
- It should have access to sufficient, accurate, timely, comprehensive, and up-to-date AML/ CFT data that enable informed decision-making to discharge its AML/CFT functions effectively, such as:
  - the report of the AML/CFT Compliance Officer;
  - the report of the internal audit function;
  - the findings and observations of external auditors, where applicable;
  - the findings of the competent authority, relevant communications with the FIU and supervisory measures and sanctions imposed.
  - moreover, it should be informed of the results of the business-wide ML/FT risk assessments and review the activity report of the AML/CFT Compliance Officer at least once a year.[8]
- On an annual basis, at a minimum, it should assess the effective functioning of the AML/ CFT compliance function, considering the conclusions of any AML/CFT audit that may have been carried out, and the appropriateness of the human and technical resources allocated to the AML/CFT compliance function.[9]

[4] EU Directive 2015/849 of 20 May 2015 on the prevention of the use of the financial system for the purposes of ML/TF

[5] item 10 of the Executive summary of the aforementioned EBA Guidelines

[6] 4.1.1.12 The role of management body in its supervisory function in the AML/CFT framework

[7] 4.1.2.16 (a and b) The role of management body in its management function in the AML/CFT framework

[8] 4.1.1.13 (a and c) and 15 The role of management body in its supervisory function in the AML/CFT framework

[9] 4.1.1.13 (d) The role of management body in its supervisory function in the AML/CFT framework

- It should designate a member of the management body[10] in charge of the AML/CFT compliance function, and ensure that this person has:
  - the necessary knowledge, skills, and experience with regard to ML/FT risks to which the organization is exposed, and the implementation of AML/CFT policies, controls, and procedures;
  - a good understanding of the credit or financial institution's business model and the sector in which it operates;
  - and a good understanding of the extent to which this business model exposes the credit or financial institution to ML/FT risks.[11]
- It should designate an AML/CFT Compliance Officer considering the scale and complexity of the credit or financial institutions operations, and its exposure to the risks indicated above.[12]

The AML/CFT Compliance Officer ('CO')

To promote and ensure that compliance is integrated into the strategy and operations of the organization, the EBA guidelines also establish clear and defined roles and responsibilities for the CO, as follows:

- The CO should have sufficient authority to propose all necessary or appropriate measures to ensure the compliance and effectiveness of the internal AML/CFT measures to the management body in its supervisory and management function.[13] Furthermore, the credit or financial institution should have the necessary systems and controls in place to ensure that the AML/CFT CO has access to all the necessary information and systems required to perform the compliance officer tasks.[14]
- As part of the second line, the CO should be independent from the business lines and perform its function autonomously, having unrestricted and direct access to all information that is necessary to the performance the CO function. In the case of a significant incident, the CO should be able to report and have direct access to the management body in its supervisory function or to the senior management where no management body is in place.[15]
- The CO should have the necessary AML/CFT knowledge, skills, expertise and seniority, as well as a good understanding of the ML/FT risks associated with the credit or financial institution's business model to perform the CO function effectively. They should also have relevant experience regarding the identification, assessment and management of these risks, and the implementation of AML/CFT policies, controls and procedures.[16]
- The CO should be responsible for, among others, the following main tasks which should be clearly defined and documented:[17]
  - to develop and maintain a risk assessment framework, as well as to report the results and propose mitigated measures of the identified risks to the management body;[18]
  - to set up, keep up to date, and ensure the proper implementation and review of AML/CFT policies, procedures, systems and controls;[19]
  - to provide advice before a final decision is taken by senior management on onboarding new high-risk customers or maintaining a business relationship with them, in line with the risk-based internal AML/CFT policies of the credit or financial institutions, and in particular in situations where the senior management's approval is required;[20]
  - to monitor whether measures, policies, controls and procedures implemented by the aforementioned institutions comply with their AML/CFT regulatory framework. The CO should also oversee the effective application of these controls applied by the first line of defense;[21]

[10] Or the senior manager where no management body is in place. 4.1.4 Identification of a senior manager responsible for AML/CFT where no management body is in place.

[11] 4.1.1.14 The role of management body in its supervisory function in the AML/CFT framework

[12] 4.2.1.24 The role and responsibilities of the AML/CFT CO

[13] 4.2.1.25 The role and responsibilities of the AML/CFT CO

[14] 4.2.1.27 The role and responsibilities of the AML/CFT

[15] 4.2.1.31 The role and responsibilities of the AML/CFT CO

[16] 4.2.1.36 The role and responsibilities of the AML/CFT CO

[17] 4.2.4.38 Tasks and role of the AML/CFT CO

[18] 4.2.4.(a) Tasks and role of the AML/CFT CO

[19] 4.2.4.(b) Tasks and role of the AML/CFT CO

[20] 4.2.4.(c) Tasks and role of the AML/CFT CO

[21] 4.2.4.(d) Tasks and role of the AML/CFT compliance officer

- to advise and bring to the attention of the management body on measures to be taken to ensure compliance with applicable laws, rules, regulations, and standards, and provide assessment of the possible impact of any changes in the legal or regulatory environment on the institution's activities and compliance framework. Furthermore, the AML/CFT CO should provide an activity report on, at least, an annual basis.;[22]
- to ensure that knowledge or suspicion of ML/FT or of a person's connection with ML/FT are promptly reported to the Financial Intelligence Unit ('FIU'), and prompt and exhaustive response to any request for information made by the FIU;[23]
- to inform staff about the ML/FT risks to which the credit or financial institutions are exposed, including methods, trends and typologies, as well as of the risk-based approach implemented by the institutions to mitigate these risks. The CO should also oversee the preparation and implementation of the ongoing AML/CFT training program. The trainings should be adjusted on a risk-sensitive basis.[24]

AML/CFT Compliance function at group level

- The credit or financial institution should designate a member of its management body, or senior manager responsible for AML/CFT among the senior managers at the level of the parent undertaking, as well as a group AML/CFT compliance officer.[25]
- This institution should set up an organizational and operational coordination structure at group level with sufficient decision-making power for the group AML/CFT management to make this position effective at managing and preventing ML/TF risks, in line with the proportionality principle and applicable legislation.[26]
- The group AML/CFT compliance officer should cooperate with and coordinate the activities of the various local AML/CFT compliance officers in the group's operational entities in order to ensure that they work consistently.[27]

Our Point of View

Although the aim of the EBA guidelines is to ensure a common interpretation and adequate implementation of AML/CTF internal governance arrangements across the EU, the implementation of these guidelines will also influence the behavior of the employees of the credit and financial institutions within EU.

Overall, these institutions are complex organizations that operate based on the interactions and choices made by their employees. The behavior of these individuals is the result, among others, of ethical values and understanding of risks within the institution, as well as the organization's tone and defined roles and responsibilities by which decisions about risks are taken and implemented.

In this case, the EBA guidelines set higher standards and expectations for AML/CTF compliance by establishing clear and defined roles and responsibilities in alignment with the regulatory requirements and good practices, where the management body sets the tone at the top. By promoting and ensuring that compliance is integrated into their strategy and operations, organizations are creating a path for the company and its employees to follow.

It is true that the implementation of these guidelines entails compliance costs, however it will also represent benefits for the institutions mentioned above. The harmonization of AML/CFT governance structures, as well as the development of risk aware culture within the European credit and financial institutions, will help in reducing its vulnerability towards ML/ FT risks.

For instance, these provisions will foster an environment of accountability in the AML/CFT compliance function and prioritize the management body function, setting the tone at the top; behavior that will cascade throughout the organization and strengthen the AML/CFT program.

[22] 4.2.4.(e) Tasks and role of the AML/CFT compliance officer

[23] 4.2.4.(f) Tasks and role of the AML/CFT compliance officer

[24] 4.2.4.(g) Tasks and role of the AML/CFT compliance officer

[25] 4.3.3.79 (a) Organizational requirements at group level

[26] 4.3.3.79 (b) Organizational requirements at group level

[27] 4.2.6 81 (d) Outsourcing of operational functions of the AML/CFT compliance officer

How Protiviti can help your organization to implement the EBA Guidelines?

Protiviti can prepare you to comply with these new EBA Guidelines in a timely and cost-efficient manner. We can help your organization by, among others:

- Performing a quick scan to assess if your organization has implemented all EBA requirements in relation to compliance management and the role and responsibilities of the AML/CTF Compliance Officer; identifying potential gaps and improvements areas; and supporting you to close these gaps;
- Identifying potential gaps and improvements areas; and supporting you to close these gaps;
- Performing a gap analysis of your risk culture and risk governance framework; and Helping with the design and implementation of appropriate governance measures, controls, defined and clear roles and responsibilities; policies and first- and second-line procedures

Moreover, we can also help by turning your information and statistical data into PowerBI dashboards. The latter will give the management body and CO the power to quickly understand and analyze AML/CFT risks; find areas where controls should be implemented or improved; and build informed decisions based on consolidated data.

For more information about our financial crime consulting solutions, visit our solution page or get in contact with us.

Contacts

Laura Benavides
laura.benavides@protiviti.nl

Owen Strijland
owen.strijland@protiviti.nl