Paracas-Advisors

Risks seen as a CAE and then as a COO: any difference?

May 11th, 2024

In my career, I have been a CAE, and then a CCO. Along one of my recent posts, I got a great question from Georgiana Sinescu: is there a different approach or perception of risks between the Chief Audit Executive (CAE) and the Chief Compliance Officer (CCO)? To answer this, it is useful to clarify what a compliance function does, explain the role of other functions in owning certain compliance risks and processes, to finally discuss the respective CCO and CAE approaches on the risk of non-compliance.

A "Compliance Management System" (CMS) or Corporate Compliance Program (CCP)

A solid CMS or CCP contributes to the strength of the Internal Control System. As per the US DOJ, a CCP must be a) well designed (risk assessment, policies and procedures, training and communications, confidential reporting structure and investigation process, investigation response, etc.), b) adequately resourced and empowered to function effectively, and c) work in practice.

A standard solution is to create a compliance function that is responsible for running this CMS, with four activities:

- Legal change monitoring. Observe and analyze developments in the legal environment, evaluate the potential impact of legal changes on the enterprise,
- Monitoring and overseeing whether compliance with requirements across the organization is ensured based on appropriate and effective internal procedures,
- Advisory: advise senior management and Boards on compliance with legal requirements and the consequences of legal changes,
- Identification and assessment of risks that can result from a failure to comply with legal requirements.

Compliance risk and process owners: the importance of regulatory compliance

Many functions "own" specific compliance risks and processes, as part of the CMS. For example:

- the Human Resources function is responsible for complying with labor laws (health and safety, social charges and taxes calculation and payment, etc.),
- a Tax function in addition to its operational responsibilities needs to make sure that the enterprise complies with all tax obligations,
- Accounting ensures that it complies with accounting rules (local GAAP, IFRS, etc.)

The compliance function does NOT own these risks and processes: it monitors and oversees them! This core activity of monitoring and oversight is also called regulatory compliance. Together with the compliance risk mapping and assessment, the regulatory compliance activity is in my view a "real" Second Line activity.

The compliance function often owns itself some compliance risks and processes:

- classically: Anti-Financial Crime (AML-CTF anti-money laundering and counter-terrorism financing, sanctions, anti-fraud and internal investigations, corruption, and bribery, FATCA, conflict of interest, etc.)
- often: Customer protection (consumer duty, data privacy, etc.),
- sometimes: Financial Markets obligations (for listed organizations).

These activities in the compliance function, similarly to other functions, are quite operational: I see them more as first Line or "1.5" Line activities. It is not uncommon that some are performed by other functions (when there is no conflict of interest) or are even outsourced.

The risk of non-compliance

In my experience, the outcome of the CAE risk assessment is close to the CCO one. However, there are differences:

The CAE has a holistic perspective:

- The risk of non-compliance (or partial compliance) with rules and regulations is part of the overall enterprise risk assessment regularly performed and updated by the CAE. This will lead the CAE to decide if compliance risks and processes, and which ones, need to be put under review.
- The CAE has also in scope the overarching design and effectiveness of the CMS/CCP, in addition to individual non-compliance risks

The CCO has a specific focus on risks:

- Scope. The "risk universe" of a CCO is partial compared to the CAE, since IA assesses the totality of the risks of the enterprise. Further, when the compliance function "owns" directly certain risks and processes, it can only self-assess itself.
- Granularity. With a comprehensive and monitoring activity, the compliance function has a transversal view of the CMS. I have found that the risk universe for the COO is often more detailed than for IA. When the compliance performs second line reviews, it may include compliance risks and processes that would not be assessed as material enough by IA. The CAE can usefully place a certain level of reliance on the monitoring and oversight activity of compliance. The CAE, while having an independent assessment of the non-compliance risk, still can leverage the assessment made by the CCO.
- Early warning. Monitoring legal changes is a strong component of a compliance function. Upcoming rules and regulations must be anticipated by the CCO, and the risk of non-compliance with upcoming rules must be assessed early, so that the compliance function can advise leadership and the business on measures to be taken (design and effectiveness) to have the organization ready to comply when a new rule is enforced. Internal audit is not necessarily at the forefront of regulatory or legal changes. But when auditing the compliance function, one task for IA will be to assess the quality of the legal change monitoring by compliance.

For the same risks, my experience is that the CCO and CAE mostly conclude in the same way. It is a good idea for the CAE, when a compliance function exists, to leverage the regulatory compliance job done by compliance if this activity is performing well.

But beyond individual non-compliance risks, IA needs to assess the risk of a poor CMS as well as the risks managed by compliance itself.