www.pwc.ch

# *How can your organisation perform effective and efficient compliance testing?*

Véronique Besson, Thought Leadership, April 2018

pwc

# Effective compliance testing

- How is compliance testing defined, and what are its objectives?
- What are the elements of an effective second line of defence testing process?
- How can a company increase efficiency by aligning its compliance testing activities across the three lines of defence?

Compliance testing is one element of an effective compliance programme. The notion of a compliance programme, which has developed largely since the mid-nineties, can be defined as the entirety of the strategic, organisational and process-related measures that aim at establishing ethical and compliant behaviours within a company.

Many companies struggle to establish compliance testing across their compliance universe, in particular because of a lack of resources. Nevertheless, the regulatory pressure to do so is increasing. Under these circumstances, how can companies find a balance between establishing a lean compliance and meeting the legal requirements for compliance testing?

# 1. Definition and objective of compliance testing

Compliance testing is part of the broader notion of compliance programme evaluation. It is one of the instruments used to assess whether the compliance programme effectively and efficiently reduces compliance risks to an acceptable level for the organisation. In other words, it is one of the key instruments for assessing whether a company's efforts to ensure compliance with laws and regulations are bearing fruit.

Compliance testing can be defined as a periodic, independent and objective assessment of compliance-related processes and/or controls. The aim of compliance testing is to assess whether the elements, processes and controls of the compliance programme are designed appropriately and are operating as designed. Compliance testing follows an established process and plan as well as, according to best practices, a risk-based approach.

In general, compliance testing activities are performed, in some form or other, within all three lines of defence (business, compliance and internal audit; see below under 3.1 for a proposed definition of the three lines of defence).

Some of the testing activities are conducted by independent functions within the business, some are performed by compliance personnel, and others by the internal audit function. Nevertheless, the main responsibility for the management of the compliance programme and the performance of compliance testing usually lies with the second line of defence, the compliance function itself.

For further definitions and descriptions of evaluation, monitoring and testing activities, see for example Internal Control – Integrated Framework, May 2013 (COSO 2013) or the ISO standard ISO 19600 – Compliance Management Systems (ISO 19600).

# 2. Compliance testing process

Compliance testing is usually performed by all three lines of defence. This section describes an effective compliance testing process within the second line of defence, the compliance function.

Elements of the compliance testing process:

## 2.1 Establish annual risk-based compliance testing plan

The compliance testing plan is one of the key elements of the annual compliance plan. It is based on the compliance risk universe, which is derived from all the relevant regulatory requirements and could be documented, for example, within a risk and controls matrix.

The compliance testing plan should ideally cover all elements of the compliance programme: compliance strategy, governance and key compliance processes.

The specific risks, and the elements of the compliance programme that will be tested in a given year, should be identified on the basis of a risk assessment in conjunction with the results of previous testing, the number of incidents and other metrics used by the company to evaluate inherent and residual risks.

Finally, compliance testing should be prioritised on the basis of available resources. In other words, the plan can – and should – be scaled according to availability, also taking account of multi-year planning, depending on the inherent and residual risks at stake.

The resulting compliance testing plan should be approved by key stakeholders and decision-making bodies.

## 2.2 Execute plan

Testing activities should be scheduled to take place over the year, based on available resources of testers and stakeholders, as well as on other factors such as dependencies between the various testing activities.

Testing should be performed on the basis of testing methodologies including sample methodologies, documentation standards, as well as standards and procedures for assessing and classifying findings. Alongside an assessment of the findings and their ratings, a root cause analysis and an assessment of severity must also be performed. The company should also develop a methodology allowing it to perform an overall assessment of the effectiveness of the compliance programme.

## 2.3 Inform and report

Regular reporting to management should be performed in accordance with predefined reporting standards and procedures. In particular, meaningful indicators have to be developed. These are linked with the potential measures defined for senior management to take.

## 2.4 Track agreed remediation actions

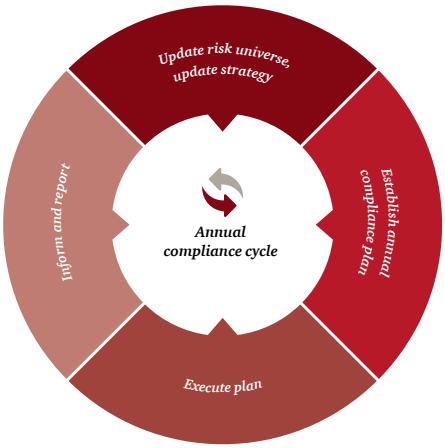
A process has to be put in place to ensure remediation actions are tracked and validated once the issue has been resolved.

## 2.5 Perform testing quality assessment

To ensure effectiveness, testing, reporting and remediation activities should be assessed to ensure that they are appropriate and are performed according to the defined standards. Any improvement measures should be defined if relevant and reported to management.

The quality standard programme also has to include training measures to ensure that sufficient expertise exists within the testing team.

The compliance testing process is part of the annual compliance risk management cycle, which comprises of the following elements:



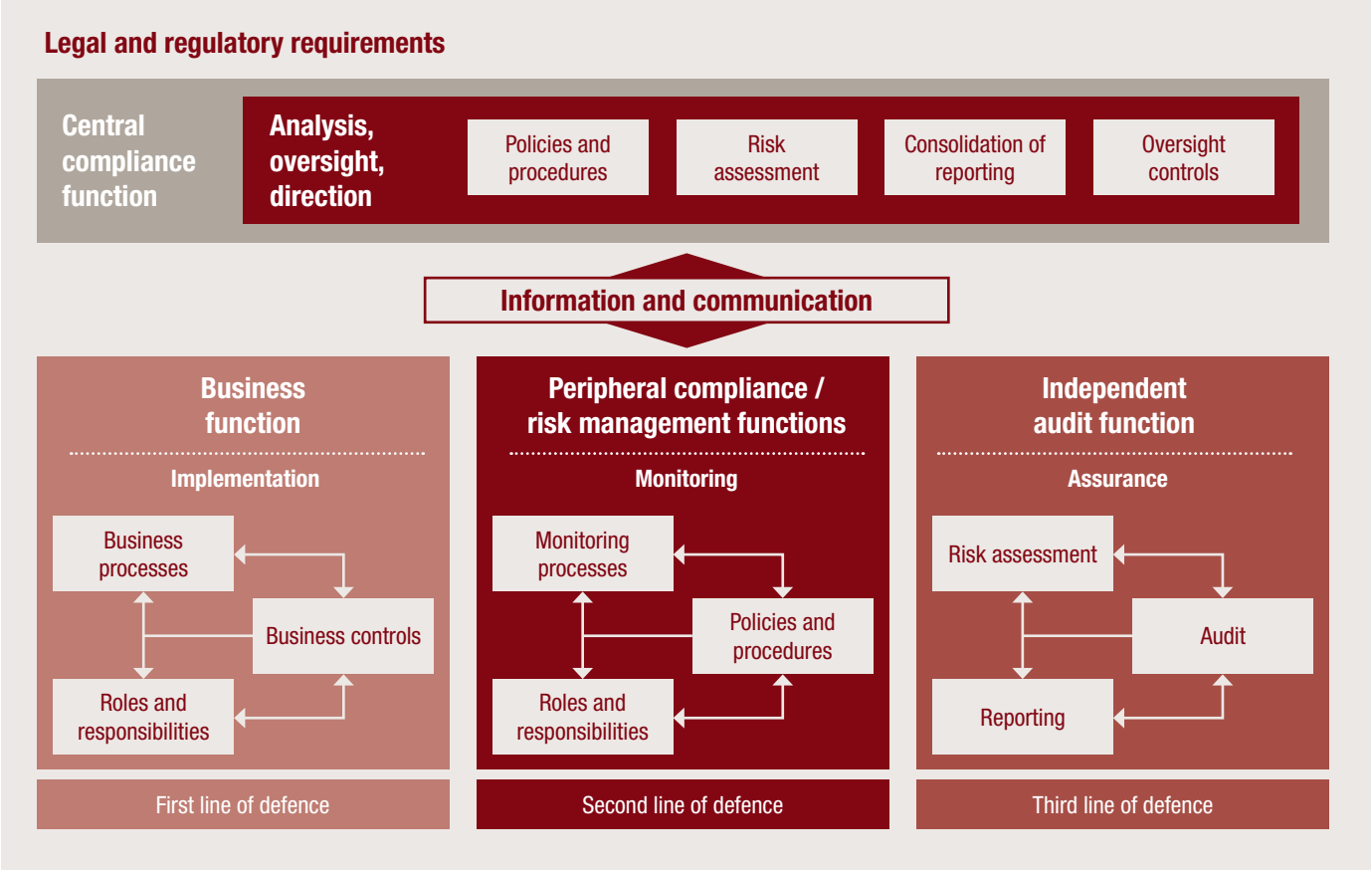
# 3. Aligning compliance testing across the three lines of defence

As described above, compliance testing is usually performed not only by the compliance function (second line of defence), but also by the business (first line of defence) and internal audit (third line of defence).

In our experience, compliance testing is not always optimally aligned across the three lines of defence. Moreover, many companies are unable to perform all the testing that would be necessary or cannot complete the planned testing consistently.[1] One way to improve the efficiency of testing activities is to align compliance testing across the three lines of defence.

## 3.1. Definition of the three lines of defence concept

Figure 1 below illustrates the functions and their roles within the three lines of defence. In summary, under this model the first line of defence (the operational units) has the primary responsibility of managing compliance risks. The second line of defence (the compliance and risk functions) has the responsibility of providing tools to manage risks and monitor compliance. The third line of defence (the internal audit function) has the responsibility of conducting independent testing to assess, in particular, compliance.




[1] See in particular PwC's publication 'Making the grade: How financial institutions can improve compliance testing', November 2015.

## 3.2. Aligning compliance testing activities across the three lines of defence

Frequently, all three lines of defence perform testing activities: independent functions within the first line perform independent testing of business processes, the second line of defence plans and executes compliance testing, and the third line of defence, within its yearly testing plan, performs compliance-related testing activities.

These testing activities are often performed in silos. Senior management fails to communicate about the testing activities of the different lines of defence, and there is no function formally tasked with coordinating activities between the three lines of defence to ensure no duplication of testing, consistency in the reporting of results as well as the alignment of remediation and improvement measures.

Moreover, employees often have insufficient knowledge and understanding of their roles and responsibilities within the company's compliance programme.

As a result, organisations experience drains on their resources, a lack of appropriate resources and duplication of effort, which leads to productivity losses and ultimately has a negative impact on customers.

One solution to this problem could be to adopt the following approach:

| 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|
| Roles and responsibilities are communicated | Testing tools, methodologies and procedures are standardised across the three lines of defence | Activities are coordinated across the three lines of defence | Business is informed about testing activities of the two other lines of defence | Reporting is consolidated across all three lines of defence |
| Ensure that the roles and responsibilities of each line of defence with regard to compliance testing are clearly defined and communicated, and that people are trained accordingly. | Consider how tools, methodologies and procedures that are applied for testing by the different lines of defence can be aligned and leveraged to improve effectiveness and efficiency. | Integrate coordination activities within the yearly compliance process and the yearly audit process to ensure second line and third line of defence testing activities are aligned at all stages (planning, execution, reporting and remediation). | Inform the business to enable them to plan their own activities accordingly. | Consolidate all reporting activities of the three lines of defence |

## 3.3. Conclusion and outlook

A clearly defined compliance testing process as well as the alignment of testing activities between the 3 lines of defence are key to lean and effective compliance testing.

In parallel, companies can further enhance efficiency by introducing more technology-based compliance testing, such as data analytics, robotics or natural language processing[2].

[2] See also related to internal audit: "Revolution, not evolution. Breaking through internal audit analytics' arrested development", January 2018. www.pwc.com/us/en/services/risk-assurance/library/internalauditanalyticsrevolution.html

# Authors and contacts


**Robert Borja**
Assurance Partner

PwC
Birchstrasse 160
8050 Zurich

+41 58 792 29 56
robert.borja@ch.pwc.com



**Véronique Besson**
Assurance Director

PwC
Birchstrasse 160
8050 Zurich

+41 58 792 23 68
veronique.besson@ch.pwc.com



**Karin Kirkpatrick**
Assurance Senior Manager

PwC
Birchstrasse 160
8050 Zurich

+41 58 792 24 70
karin.kirkpatrick@ch.pwc.com