Implementing compliance programmes based on a risk-informed approach

Organisations today have access to numerous opportunities across the world and continuously adopt new ways of working to expand their business horizons. These opportunities often come with associated risks. In this regard, regulators not only hold organisations accountable for their action or inaction, but also consider the responsibility of their suppliers and agents, for the non-adherence of laws and regulations.

As per PwC's 26th Annual Global CEO Survey 2023, CEOs across the globe see changes in regulations as the second-biggest threat to their profitability in the next ten years.[1] Business leaders across industries are under increasing pressure to adhere to a complex and increasing set of rules and regulations. Non-compliance can result in significant legal, financial and reputational consequences – not just for organisations but also, in some instances, for business leaders as well.

In this article, we will explore the relevance of risk-informed approach and key steps and considerations involved in designing and implementing compliance programmes for an organisation.

Why is risk-informed approach relevant today?

1. This approach is well-recognised in the industry as well as by enforcement agencies and regulators.
2. Resources at disposal are limited, and risk is ever evolving.
3. All violations are not equal in terms of impact and should not be treated that way.

A risk-informed compliance programme focuses on identifying the highest compliance risks relevant to an organisation and prioritising them for appropriate compliance controls, policies and procedures. This approach will allow organisations to comply with the most relevant and critical compliance risk, better utilise available resources, and adapt to the emerging compliance landscape.

[1] https://www.pwc.in/publications/ceo-survey/ceo-survey-2023.html

Steps to get started with a risk-informed compliance programme

Step 1 Assess your organisation's regulatory risk profile.

Most organisations – especially those with complex organisational structures – across multiple countries are exposed to plethora of laws and regulations at various levels. Based on our experience, most companies (across various functions) are aware of most of their regulatory obligations. However, the compliance function of that same is only aware of about a quarter-portion of applicable laws and regulations. The rest are hidden across the organisation within various business units, functional silos etc. Hence, it is crucial that an organisation identifies all laws and regulations that apply to its industry, region and business operations as the first order of business.

Step 2 Identify business functions, stakeholders and associated processes.

Determine if the responsibilities to comply with various laws and regulations are spread across various functions and business units – secretarial, human capital, finance, marketing, facility management and information technology. Based on the compliance obligations of each organisation, identify appropriate stakeholders based on who is doing what and the impacted current processes.

Step 3 Determine the criticality of the compliances for each functional area and process.

Identify business processes that are most crucial to the ongoing compliances of the organisation. You may take the following into account:

- How important is this business function and the relevant process for the organisation in order to adhere to the compliance required?
- In case of non-compliance, how will it disrupt the business and affect the bottom line, and will it have other penal consequences?
- How important is the function to the continuity of the business and compliance?
- Are there too many silos involved in the process of complying with certain rules and regulations?

Step 4 Identify risks to ongoing compliance and associated vulnerability.

Identify and manage risks that have a good probability of happening. Organisations should create a list of risks, and rank them based on their inherent impact and probability of happening by analysing past trends. For example, if one company official is responsible for reporting to a regulator and he alone coordinates with multiple functions within the organisation to prepare this report, it should be considered as a high-risk task, as the employee may leave or not be available always. Cataloguing risks in advance will help create a regulatory risk register that will reflect the real-time state of the organisation, in terms of potential risks.

Step 5 Create a roadmap to address the identified regulatory risk via a compliance programme.

Once a risk register has been compiled, create a roadmap to address the same via a compliance programme.

The programme should be designed while keeping the following in mind:

Is our programme well-designed?

With a clear understanding of the relevant compliance risk universe, organisations should design a programme that aligns with their goals and objectives. Moreover, they should assess whether all of their resourcing and structural choices are rational. Furthermore, organisations should be able to demonstrate that their programme has evolved with the risk.

Is our programme adequately resourced and empowered to function effectively?

Next comes the ingraining of compliance within the fabric of an organisation. It's important to centralise compliance resources, which will further help focus on the highest risk areas, and highlight how compliance can support the functional team which operates as the first line of defence for most compliance risks. Adequate resourcing will include creation of compliance functions, allocation of adequate budget, empowerment to the function, engagement of a stable service provider and access to technology.

Is our compliance programme actually working?

Whenever required, organisations must be able to demonstrate that the compliance programme is working, and it's not an 'off the shelf' programme that merely exists on paper. Moreover, they must ensure that the programme has sufficient backing with the relevant data and information.

Key elements for robust and effective compliance programmes

Programme governance and resources

Tone at the top and middle is key. It's important that senior leaders, through their words and actions, encourage adherence to compliance. One should be able to demonstrate what concrete actions have they taken to demonstrate leadership in the company's compliance and remediation efforts. Any oversight by the board of directors on compliance programmes can prove to be detrimental to the organisation's reputation.

Policies, procedures and controls

Develop comprehensive compliance policies, procedures and associated controls tailored to your organisation's needs. These documents should outline specific compliance requirements, processes, and responsibilities. Ensure that they are clear, concise and easily accessible to all relevant stakeholders. Periodically review and update your compliance to reflect changes in regulations, industry standards and your organisation's risk profile.

Monitoring and auditing

Transform the data to work for you. Use cutting-edge analytics, machine learning and advanced monitoring technology to help see across the compliance spectrum, so as to intelligently predict and manage risk. By aggregating information across disparate data sets, systems and business units, organisations will have a cohesive view that can help them take proactive preventative action or respond and remediate with speed and confidence.

Risk assessment

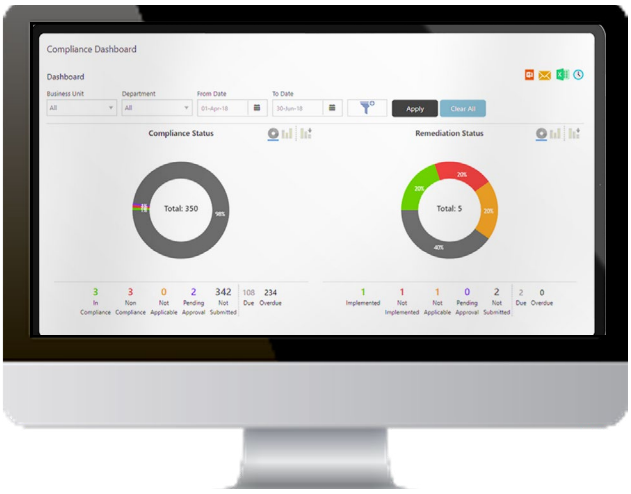
Adapt your compliance programme based on the insights gained from industry benchmarking, emerging laws and regulations, and internal evaluations, as only performing a risk assessment and moving on will no longer suffice. Revisit it often and get value out of your data. A compliance programme that recognises the need for ongoing risk identification, coverage and mitigation when business models or operations change, helps to protect and accelerate your competitive advantage.

Communication and training

Appropriate and adequate communication and training is the hallmark for a well-designed compliance programme. The programme should be tailored to the purpose by considering the risk register. Training should not only be limited to educating organisations about the importance of compliance and adhering to established policies and procedures, but also help the workforce embrace emerging compliance risks. Along with the compliance function, enabling departments that function as the first line of defence for most compliance risks should have access to the required guidance, including external advisors, whenever required.

How is PwC helping organisations manage their compliances efficiently?

PwC has been helping clients across various sectors for over 16 years to strengthen their corporate compliance programmes. More than 200 organisations, including many fortune 500 companies, have been using our cutting-edge SaaS product 'Compliance Insights' for their compliance programmes.



Compliance Dashboard

Dashboard

Business Unit: All
Department: All
From Date: 01-Apr-18
To Date: 30-Jun-18

3	3	0	2	342	108	234
In Compliance	Non Compliance	Not Applicable	Pending Approval	Not Submitted	Due	Overdue

1	1	1	0	2	2	0
Implemented	Not Implemented	Not Applicable	Pending Approval	Not Submitted	Due	Overdue

Benefits of using Compliance Insights

Centralised data management

Compliance insights streamline data access and ensures data integrity, making it easier for an organisation to track compliance activities, audits and regulatory changes.

Automated workflows

Automated workflows reduce the risk of manual errors and ensure that compliance activities are completed on time.

Real-time monitoring and alerts

Organisations can stay up-to-date with the changing regulations and reduce the risk of non-compliance.

Audit trail and documentation

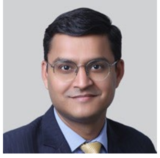
Organisations can demonstrate compliance during audits and reduce the risk of regulatory fines and penalties.

About PwC

At PwC, our purpose is to build trust in society and solve important problems. We're a network of firms in 152 countries with over 328,000 people who are committed to delivering quality in assurance, advisory and tax services. Find out more and tell us what matters to you by visiting us at www.pwc.com.

PwC refers to the PwC network and/or one or more of its member firms, each of which is a separate legal entity. Please see www.pwc.com/structure for further details.

Contact us



Lokesh Gulati

Partner, Contracting & Compliance, PwC India
lokesh.gulati@pwc.com

Ravinder Saini

Director, Contracting & Compliance, PwC India
saini.ravinder@pwc.com

Aman Goel

Managing Director, Digital Products Leader, PwC India
aman.goel@pwc.com

Harsh Kumar

Associate Director, Contracting & Compliance, PwC India
harsh.k@pwc.com

pwc.in

Data Classification: DC0 (Public)

In this document, PwC refers to PricewaterhouseCoopers Private Limited (a limited liability company in India having Corporate Identity Number or CIN : U74140WB1983PTC036093), which is a member firm of PricewaterhouseCoopers International Limited (PwCIL), each member firm of which is a separate legal entity.

This document does not constitute professional advice. The information in this document has been obtained or derived from sources believed by PricewaterhouseCoopers Private Limited (PwCPL) to be reliable but PwCPL does not represent that this information is accurate or complete. Any opinions or estimates contained in this document represent the judgment of PwCPL at this time and are subject to change without notice. Readers of this publication are advised to seek their own professional advice before taking any course of action or decision, for which they are entirely responsible, based on the contents of this publication. PwCPL neither accepts or assumes any responsibility or liability to any reader of this publication in respect of the information contained within it or for any decisions readers may take or decide not to or fail to take.

SG/November 2023-M&C 33360