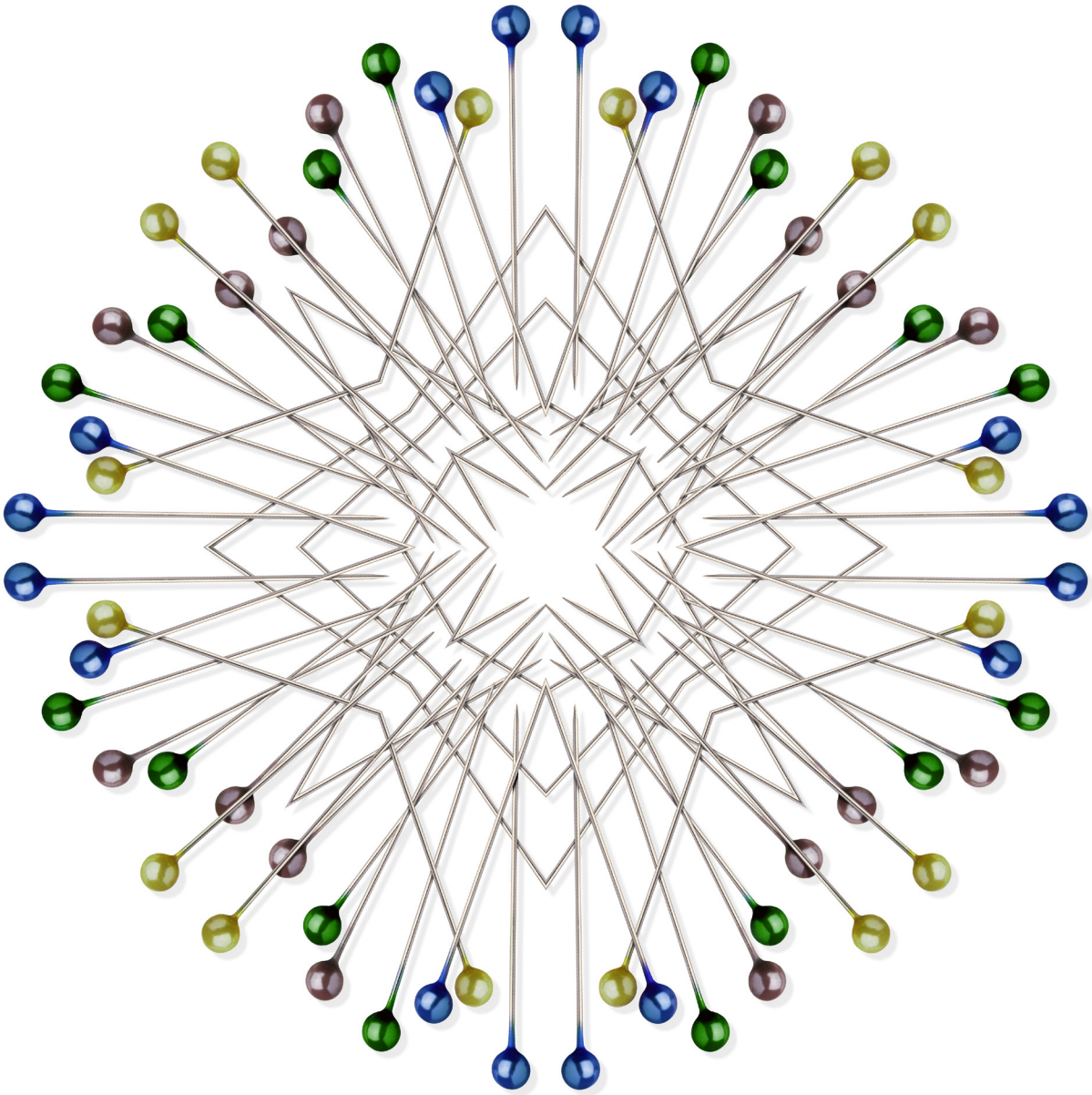
Deloitte.



Compliance Risk Management Powers Performance

February 2018

Today's business climate is characterized by disruption and volatility. At Deloitte, we help businesses gain a new view of compliance risk – seeing compliance risk management as a vital performance lever, enabling organizations to take on compliance risks with confidence for competitive advantage.

Compliance Risk Management Powers Performance

The legal landscape is changing very fast and both customer and regulator expectations increase. Financial institutions are exposed to a greater degree of compliance risk than ever before. Specifically, compliance risks are the threat posed to a company's license to operate and which could impact the institution's ability to achieve its strategic objectives. Managing compliance risks has become more and more complex.

To fully understand their compliance risk exposure institutions must strengthen their compliance risk management framework and methodologies. Core compliance fundamentals must be established first before being able to transform to lean compliance. In general, a more dedicated and holistic approach is required. Controlling compliance risks should help to become future proof.

In its *Supervision Outlook* 2018 the Dutch Central Bank (DNB) outlines the priorities it has set and examinations it has planned to conduct as part of its supervisory remit in 2018. Together with this Supervision Outlook the DNB has also published the *Supervisory Strategy for 2018-2022*, which includes the following focus areas:

1. Responding to technological innovation;
2. Emphasizing future orientation and sustainability;
3. A hard stance against financial and economic crime.

The importance of Compliance risk management

Although an improvement of managing compliance risks at financial institutions is already clearly visible, there is still a gap to close. The following trends are closely related to this:

1. Increased regulatory focus;
2. Poor line of sight of compliance risks to senior management;
3. Compliance is often bolt-on not built-into existing business processes and controls;
4. Poor management of business requirements;
5. Too much silo approach;
6. High cost of compliance.

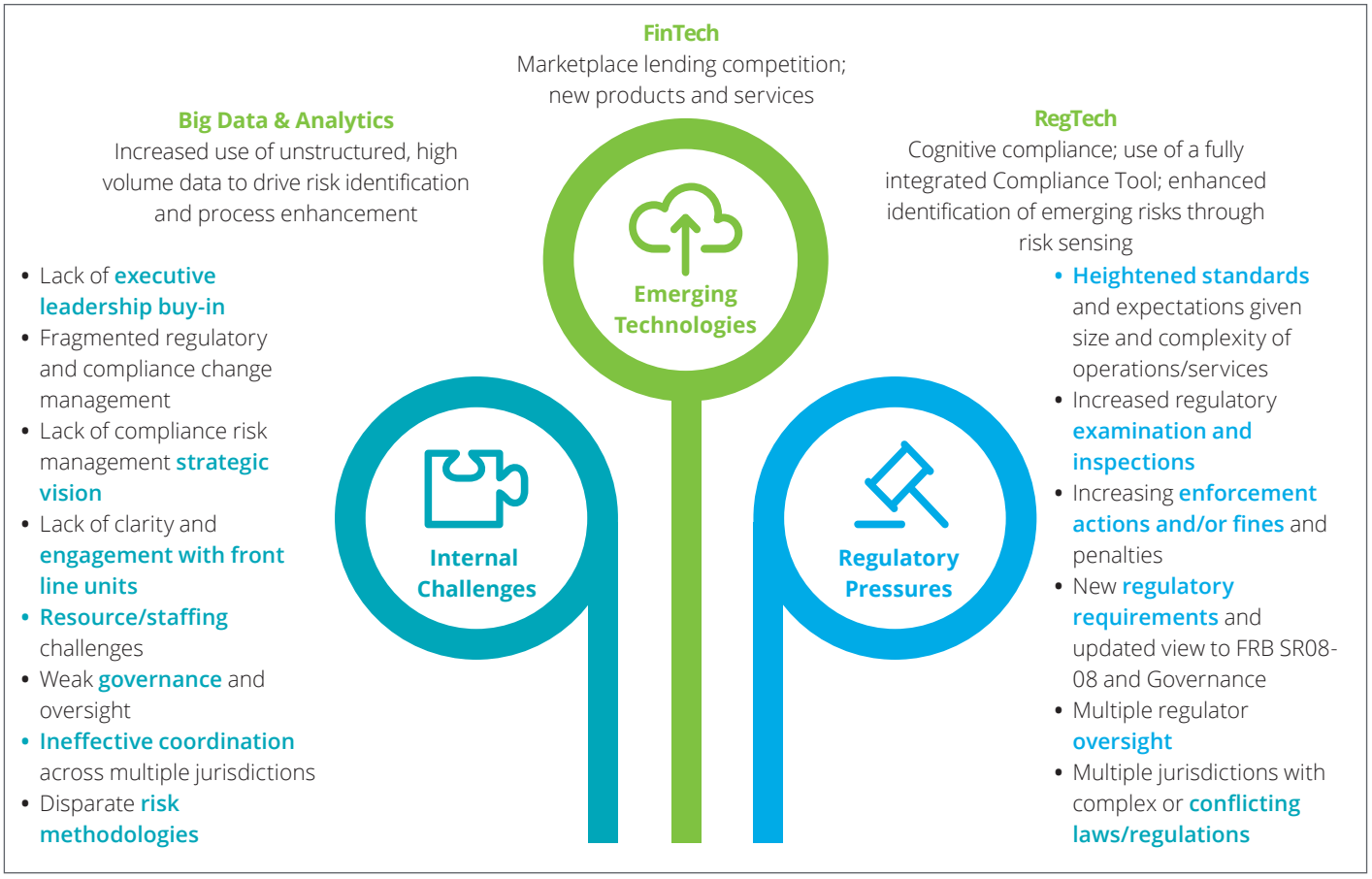
Compliance risk management needs to become more efficient to meet future demands from a regulator and customer, but also society perspective.

"Solid and comprehensive compliance risk management will ultimately reduce the likelihood of a major non-compliance event or ethics failure"

DNB Supervision Outlook 2018

The following elements will devote extra attention in 2018, both in specific sectors and across sectors:

- Effective data-analysis
- Excluding boxticking exercises
- Strengthening lines of defence
- Use of innovating technologies
- More effective and efficient ethical operational management
- Complying with the 4th AML Directive requirements
- Preventing paper SIRAs
- On-site research on actual effectiveness of controls
- Adequate transaction monitoring system
- Preventing money laundering, terrorist financing and evasion of financial sanctions
- Reporting of relevant compliance risks
- Effectiveness of the compliance function
- Effectiveness of Systematic Integrity Risk Analysis in practice



Given the information model above, institutions may be better able to develop an effective compliance risk management framework, which is strongly embedded into its day-to-day business and operations. Combining and aligning compliance risk management elements contributes to an improved insight and control of all compliance risks the institution is exposed to. It allows associated functions to prioritize on mitigating compliance risks and monitoring. A solid and comprehensive compliance risk management will ultimately reduce the likelihood of a major non-compliance event or ethics failure. It shall increase the quality of business processes and customer satisfaction, which enables the institution to set itself apart in the marketplace from their competitors.

Holistic approach required

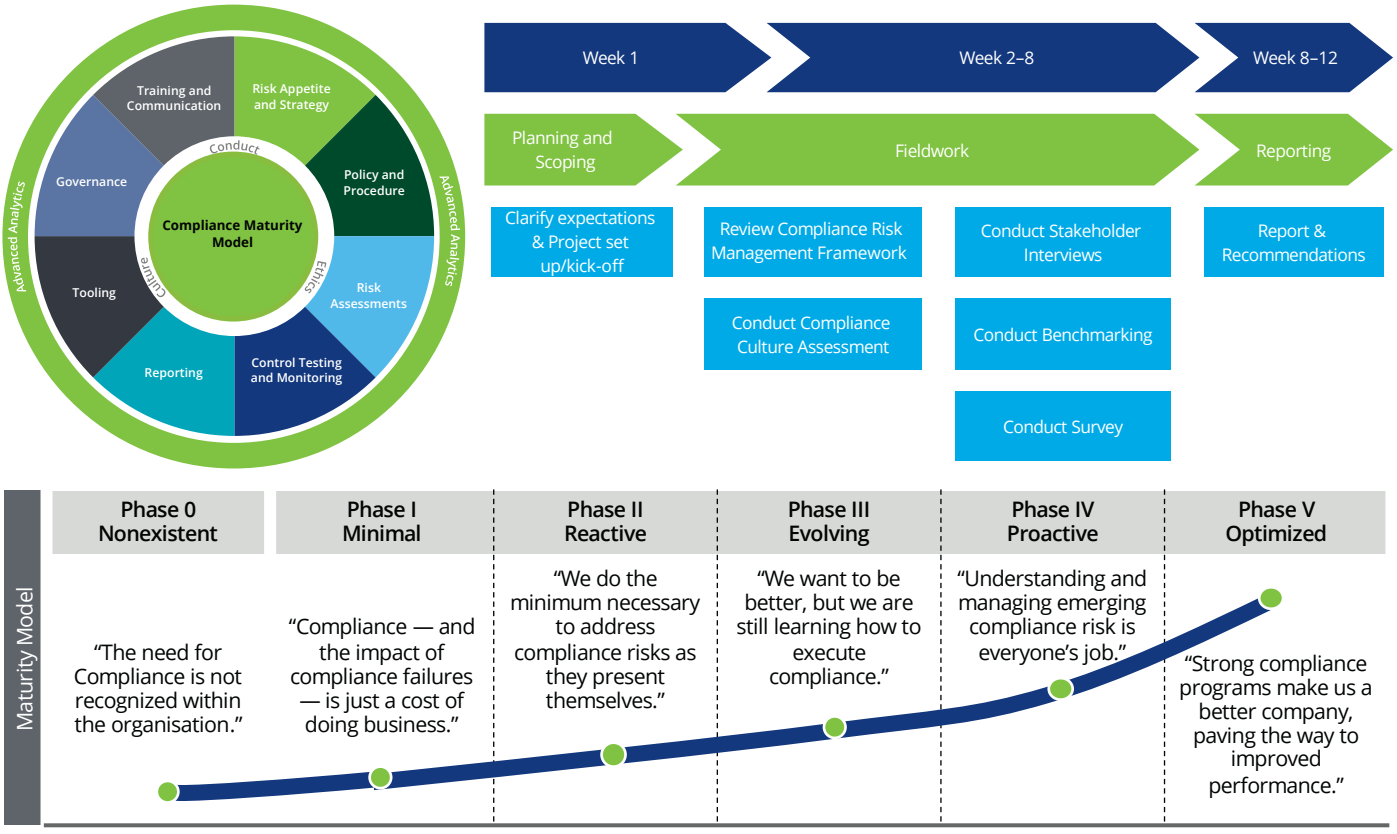
A solid compliance risk management requires a holistic approach which ultimately combines and aligns all elements in the compliance risk management framework as stated in the figure below.

Compliance risk management is part of the day-to-day business and operations. It should be on the agenda of the risk management function, compliance function and internal audit as safeguards of the organization. But the business is as control owner, risk owner and customer owner ultimately responsible for being in control over compliance risks. Compliance risk management should therefore be a recurring agenda item in the board meeting.

Measuring the maturity of the compliance risk management framework

Eager to find out what the level of maturity is of your compliance risk management framework and how to enhance it? Deloitte's Maturity Model for compliance risk management can provide you with this insight. This model has been developed by our global team of compliance experts based on the knowledge and experience of leading organisations and compliance practices we have seen across leading organisations around the globe.

The framework is underpinned by eight key organisational compliance elements. Through desk research, surveys and interviews we will map your current state for each element. We will report on the improvement areas of your organisation and suggest a course of action to increase the maturity level to the desirable state.



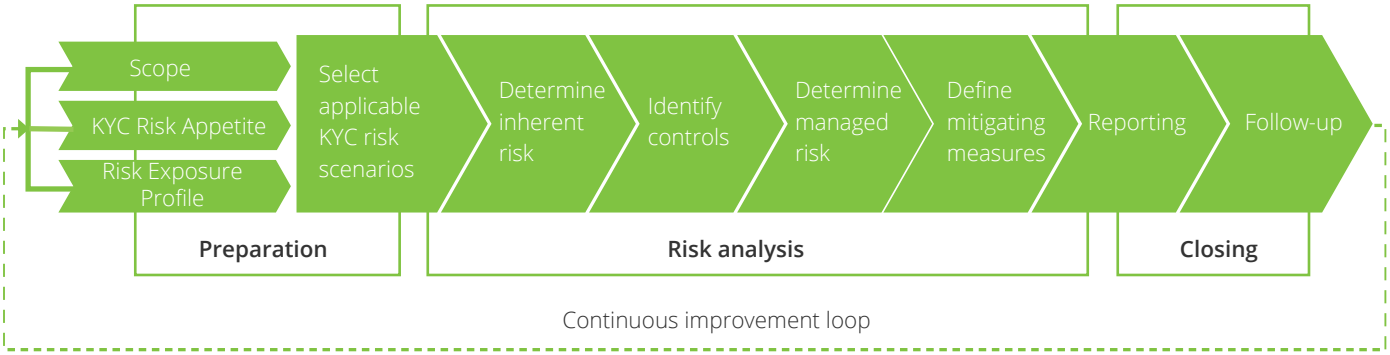
Advanced Analytics

Compliance Risk Management is also about interpretation of data through analytics. Advanced analytics is about applying state-of-the-art techniques like machine learning, predictive modelling, statistics, and advanced visualization to large volumes of data in order to gain actionable insights and achieve competitive advantages. Some examples:

- Recognizing specific client type behavior which is considered as being unacceptable according to the risk appetite & policies;
- Real-time insight into unusual transaction behavior by applying self-improving transaction monitoring scenarios;
- Real-time insight in actual product risks by monitoring financial products and the way they are actually used;
- Monitoring, predicting and improving workforce performance.

Compliance Risk Management sub-elements

Systematic Integrity Risk Analysis (SIRA)



Deloitte has developed a (DNB proof) SIRA methodology that consists of a tailor made approach covering all relevant integrity risks for your organization and industry. This approach also meets the risk assessment requirements as outlined in the 4th AML Directive. The SIRA allows insight into vulnerabilities existing in the organization. The implementation of this risk assessment methodology may also require a roll-out through your entire global organization. This methodology can be delivered as a service or a technology enabled solution.

The SIRA has a specific focus for the following elements for which Deloitte can provide with a structural solution:

- A solid risk appetite statement;
- Data-driven approach and (advanced) data-analytics;
- External trends and developments;
- Inherent risk score;
- Control effectiveness;
- Scoring and proper mitigation of residual risks;
- Monitoring and adequate follow-up;
- A systematic implementation;
- Solid risk analysis governance (roles and responsibilities between first and second line of defence);
- Solid documentation of decision-making process;
- Having a clear SIRA policy and standards in place applicable for the entire organization.

Robotics Process Automation (RPA)
Costs of compliance are increasing. The need for quality, control, reliable and compliant processes in accordance with regulation is crucial. RPA can be the structural solution for this need.

RPA tools are delivered through software that can be configured to undertake repetitive rule-based tasks which are normally executed (manually) by humans. This can help businesses to improve the efficiency and effectiveness of their operations in a cost-effective way. This enables Compliance officers to spend more time on strategic, relevant and high-priority tasks. Some RPA examples within Compliance Risk Management:

- Control Testing & Monitoring: automation of manual first line and second line compliance checks;
- Know Your Customer:
  - Extracting data from internal and external sources;
  - Automation of KYC processes;
  - Filing Suspicious Activity Reports (SAR).

Product Risk Assessment (PRA)

Financial institutions are required to have a solid understanding and insight into integrity risks related to their broad product portfolio and financial services. A proper analysis of these integrity risks should be systematically executed for which the SIRA is an ideal methodology. We have seen that the SIRA approach for a product risk assessment can uncover latent integrity risks. This has already helped some financials to strengthen their controls and/or redesign their product portfolio.

Do you as a financial, know to what specific money laundering, sanction, tax evasion, cybercrime or fraud risk your products and services are exposed to? A sound understanding of these integrity risks allows financials to enhance their core business and customer satisfaction.

"Financial institutions offer a wide range of financial products, but do they actually know their latent integrity risks?"

Policies and procedures

Clear policies and procedures play a major role to stay compliant, while they also provide overview and awareness. Furthermore, the quality and quantity of these policies and procedures are a reflection of the organizational maturity. Profound analysis and review of the current range of policies and procedures including the underlying risks and controls, will identify gaps and opportunities for improvement. These insights enable the organization to embed the right and required controls in its processes and evolve to an organization which is self-improving and self-controlling.
Important factors for a high-quality set of policies and procedures are:

- Clear understanding of legal the framework and underlying requirements;
- Clear determination of the objectives of the policies and procedures;
- Accessible, understandable and executable for the whole organization;
- Clear policy house (layered policies), taking into account the different levels of the organization;
- Well-supported by the organization's IT systems;
- Consist practical guidance;
- Monitoring service (either internal or external);
- Strengthened by smart solutions like data analytics, robotics and/or artificial intelligence;
- Clear organizational structure with well defined, transparent and consistent lines of responsibility;
- Responsibility and commitment to Integrity Risk Management (e.g. Tone at the top and equally important Tone at the middle).

"A decent policy house, translated into proper procedures, is the platform for consistency and clarity"

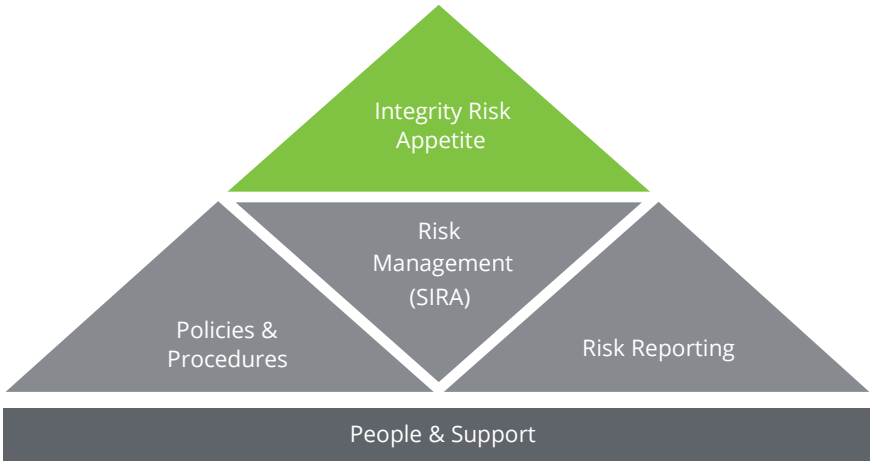
Integrity Risk Appetite

Financial institutions are exposed to many forms of risks, including integrity risks ranging from facilitating money laundering to cybercrime and socially or ethically unacceptable behavior. Integrity Risk Appetite is the level of risk regarding integrity breaches an organization is willing to accept in their pursuit of their strategy and business goals. Without a sophisticated and appropriate integrity risk appetite, a financial is not able to set and demonstrate clear boundaries.

Deloitte uses a six step approach that has proven to be successful in developing, implementing and monitoring the Integrity Risk Appetite, and optimizing integrity risk management:

1. Alignment with strategic goals, value drivers & strategic risks;
2. Definition of tactical risks & tolerances which set a benchmark for actual risks;
3. Identify existing & desired limits which provide actionable input for risk and business managers;
4. Implement limits in business lines so integrity risk appetite is used on an operational level within the organization;
5. Continuous monitoring supported by new and innovative reporting structures;
6. Integrity Risk Appetite should foster board level debate on actionable elements that clearly articulate the organizations intended responses to (reputational) losses caused by integrity risks and breaches in limits.

Implementation of an Integrity Risk Appetite in the business line is the most challenging step in the process and successfully dealing with the challenges is the main driver for the approach as developed by Deloitte.



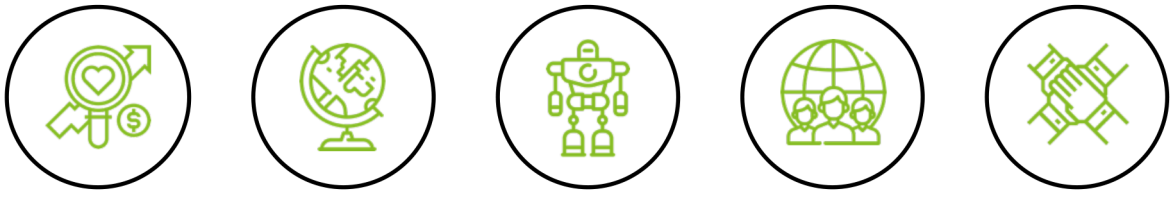
Control testing & monitoring

Controls are a very important element within Compliance Risk Management. Proper functioning and monitoring of these controls is the key to reducing Compliance Risk. However, control requirements change constantly due to new regulations, policies and standards, while control testing activities often remains a manual process, driven by reporting deadlines.

The traditional approach to control testing offers little opportunity to add value, resulting in a "tick the box" exercise with high fixed costs, lack of flexibility and risk of inconsistent quality.

Deloitte can help to improve your control testing and monitoring by using outsourcing (managed services), automation and/or Robotics Process Automation (RPA) for example.

Some advantages that can be reached:



Key success factors

There will never be a successful implementation and conservation of a sound Compliance Risk Management framework without a couple of essential organizational elements, being:

Reporting
Reporting findings, observations, test results and results from risk assessments consequently to the right group of stakeholders

Tooling
Business processes can often be more efficient and effective by using the right tooling, IT infrastructure nd holistic case management system

Governance
Roles and responsibilities must be clearly defined, including mandates, monitoring, KPI setting and accountability, to be able to govern the company effectively

Training & communication
Only by an effective and recurring training program and clear communication people can be encouraged to do the right thing, which is the first step to combat and prevent non-compliant events

Corporate values should be reflected in culture, conduct and ethics

How we can help?
With our broad experience with Compliance Risk Management and knowledge of the financial market, its challenges, developments and trends, we can help to strengthen your Compliance Risk Management framework.

We can support you with:

- **Assessing** your current Compliance Risk Management framework;
- **Implementing** improvements;
- **Transforming** your compliance function;
- Our **managed services** from our Deloitte Managed Services (DMS) team.

Next step – Lean Compliance

Compliance activity has historically worn the badge of "licence to operate" or "the cost of doing business". However, whilst it is mission critical, it does not mean that functions cannot seek to simplify, tech enable and reduce costs. It is possible to "lean compliance".

The compliance function of today misses the following:

- A holistic view
- Simple business requirements
- Clear line of sight
- Key cultural indicators
- Technology enablement

Benefits of simplified compliance are the following:

- Less burden on the business units
- Increased line of sight of risk exposures
- Significant opportunity for FTE savings
- Improved quality and effectiveness

Contact

Please contact us to discuss how we can strengthen your Compliance Risk Management together.

Jeroen Jansen
Partner Risk Advisory/
Financial Services North West Europe Leads
Email: Jerojansen@deloitte.nl
Phone: +31 (0) 6 100 426 56

Martin Eleveld
Partner Risk Advisory/
Financial Services
Email: MEleveld@deloitte.nl
Phone: +31 (0) 6 232 451 59

Tjeerd Wassenaar
Partner Risk Advisory/
Corporates
Email: Twassenaar@deloitte.nl
Phone: +31 (0) 6 129 967 20

Christiaan Visser
Director Risk Advisory/
Lean Compliance
Email: Chvisser@deloitte.nl
Phone: +31 (0) 88 288 54 28

Hassan Bettani
Director Risk Advisory/
Insurance
Email: Hbettani@deloitte.nl
Phone: +31 (0) 6 820 123 60

Joes van Berkel
Manager Risk Advisory/
Compliance risk management
Email: JovanBerkel@deloitte.nl
Phone: +31 (0) 6 109 990 27

Deloitte.