The evolving role of compliance: How companies need to enforce their three lines of defence to protect the business

Received (in revised form) 5th September, 2019

Renata Hoes*
Chief Compliance Officer, MLRO and Data Protection Officer, MFEX Luxembourg

Karin Gehlert**
Financial Crime Compliance Professional

Renata Hoes

Karin Gehlert

Renata Hoes *joined Generali Investments Luxembourg S.A. as Chief Compliance Officer and Money Laundering Reporting Officer in July 2015. Before moving to Generali Investments Luxembourg S.A., Renata was a member of PwC Luxembourg's Governance, Risk and Controls Department. While at PwC, Renata was a member of PwC's Fight against Financial Crime task force and an expert in general compliance matters with over 18 years of international experience in the insurance and asset management industry. Before joining PwC, Renata was Head of Compliance at a leading management company in Luxembourg where she was in charge of strategic, tactical and operational compliance matters for the company. Prior to this, Renata gained over 12 years of experience in the cross-border life insurance industry as Head of Compliance. In 2000, she joined Luxembourg's largest cross-border life insurance company, and in 2009, Renata joined an international insurance group to set up and develop the Compliance Department in its bancassurance branch in Luxembourg. Renata is the President of the Luxembourg Chapter of the Association of Certified Fraud Examiners (ACFE), member of various working groups of the Association of Luxembourg Fund Industry (ALFI), as well as a member of the Association of Luxembourg Compliance Officers (ALCO). She is also a member of the European Association of Data Protection Professionals, and was admitted to the Institut Luxembourgeois des Administrateurs in June 2018. Renata is a regular speaker at conferences on the topics of anti-money laundering/counter-terrorism financing (AML/CTF), compliance and new regulations.*

Karin Gehlert *led the AML Team of a Central Administrator in Luxembourg before joining a leading management company as Head of AML/CTF in March 2019. Prior to this, she was a member of the Governance, Risk and Controls Department of a Big Four Company in Luxembourg. Karin has more than 10 years of experience in audit and financial crime compliance within the asset management and private banking industry. Karin is a Certified Fraud Examiner and Fellow Chartered Certified Accountant and serves as a Member of the Board of Directors of the Luxembourg Chapter of the ACFE.*

Abstract

Despite the increasing legal and regulatory requirements for financial institutions within the European Union, scandals surrounding compliance and corporate governance failures are continuously being revealed. Apart from significant fines and monetary losses as well as reputational damage for the concerned organisations, such scandals lead to pressure on legislators and international (supervisory) bodies to again further increase regulatory requirements. This paper describes the Three Lines of Defence Model within organisations in connection with the Danske Bank scandal and outlines key principles that can serve as the basis to strengthen the compliance environment and culture within organisations to prevent major scandals.

**Chief Compliance Officer, MFEX Luxembourg S.A., Tèl: +352 661 242109; E-mail: renata.hoes@mfex.com*

***Financial Crime Compliance Professional, 6b Route de Trèves, L-2633 Senningerberg, Luxembourg Tèl: +49 152 098 37 917; E-mail: gehlertkarin@yahoo.de*

Journal of Financial Compliance
Vol. 3, No. 2 2020, pp. 158–170

2398-8053

Keywords: Three Lines of Defence Model, compliance, Danske Bank scandal

INTRODUCTION

Although legal and regulatory requirements have been significantly strengthened and enforced within the financial industry throughout the European Union in the past decade, major international scandals are revealed on a regular basis.

Such scandals, whether centred on money laundering, corruption, bribery, fraud or other criminal activity, always have a significant impact on economies as a whole. After all, trust and credibility play a vital role in any single economy or a system of economies.

The pressure resulting from both regulatory fines and adverse media coverage, that is, measurable monetary damage as well as reputational damage, forces financial institutions to enhance their compliance policies and procedures, related processes including defence mechanisms such as the three lines of defence model, as well as interdepartmental cooperation to prevent further scandals.

THE THREE LINES OF DEFENCE MODEL — CONTROL ASSURANCE

Since the Institute of Internal Auditors (IIA) published a global position paper in 2013,[1] the Three Lines of Defence Model has become accepted as a regulatory framework for the control and mitigation of company risks.

In order to begin to understand how the Three Lines of Defence Model can support to protect a business, it is crucial to have a clear understanding about each line of defence.

The first line of defence (business front-line management) is a company's business operations management who owns and manages the risk, inherent in or arising from business processes, and is responsible for having properly designed and effectively operating controls in place to mitigate significant risks, performing ongoing assessments of internal controls and promoting a culture of compliance and control.

To provide quality assurance and testing required from the first line of defence, a degree of expertise is required that can only be maintained through integration with the second and third lines of defence within the business. The more that proximity is lost, the harder it is to perform the function properly. But, while there is a need for expertise on the business side, there is still a tricky balance to be achieved between the three lines of defence. There are several grey areas in terms of the first-line control function's independence and what that means. For example, it can not only find itself operating controls on behalf of the business but also test the effectiveness of the same controls. This creates a risk that the function is effectively grading itself. But, as responsibilities become more clearly defined across the three lines, the industry reaches towards a balance, where, rather than grading its own homework, the first line of defence can demonstrate to the second line that it has been done. The current status quo of semi-independence is not a bad thing as will be described further in the paper. An ideal setup is one where, rather than being directed by the business, the assurance function develops its own plan that is based on a risk hierarchy agreed together with the business.

The second line of defence (control functions) is the independent mandate of an organisation's control functions. This generally includes compliance and risk but may also include other support functions such as finance and legal. Second line of defence functions typically include setting standards related to the expectations associated with managing and overseeing risks,

including compliance with applicable laws, regulatory requirements, policies, procedures and standards of ethical conduct. In addition, the control functions provide advice and training to the first line of defence and establish tools, methodologies, processes and monitoring of controls used by businesses to foster a culture of compliance to satisfy those standards.

The third line of defence is the internal audit function that independently reviews the activities of the first two lines of defence supported by a risk-based audit plan and methodology generally approved by the senior management. The third line's independent assessment of controls is produced with an overall rating by the audit unit and individual ratings for specific findings, which form the basis for regular reporting to the senior management.

THE DANSKE BANK SCANDAL

Although the Danske Bank scandal is very recent, a complex matter and still under investigation with all details yet to be revealed, it serves this paper well as an example to see the various perspectives on compliance failures, as well as the advantages of all three lines of defence to fully cooperate together.

In the 'Report on the Non-Resident Portfolio at Danske Bank's Estonian branch' published in September 2018, one of the key takeaways stated:

> *In early 2014, following a whistle-blower and new reporting from Group Internal Audit, Danske Bank Group realised that there had been a historical misconception. It was now realised at Group level that AML procedures at the Estonian branch involving the Non-Resident Portfolio had been manifestly insufficient and inadequate. It was also realised that all control functions (or lines of defence) had failed, both within the branch and at Group level. This included business functions as well as Group Compliance & AML and Group Internal Audit.*[2]

To understand which events led to such a statement, it is vital to understand the chronology of the scandal as far as it has been made public.

The reporting released by Danske Bank itself, as well as independent media, indicates that the scandal ultimately reaches back to 2007 when Danske Bank effectively established its Estonian unit by taking over Sampo Bank, which had an Estonian branch. During the period 2007 to 2013, approximately 10,000 of the branch's customers, accounting for 44 per cent of all deposits, were non-residents of Estonia. Moreover, these customers made around 7.5 million transactions with external parties (not including transfers between customers). In total, that flow of money added up to approximately €200bn. As the Estonian branch had its own information technology (IT) platform and many documents were written in Estonian or Russian, Danske Bank Group did not seem to have the same amount of insight into the branch's activity.[3,4]

According to news reports, in 2007 and in 2013, Russia's central bank sent warnings to both the Estonian branch of Danske Bank and the Estonian and Danish financial supervisors over suspect transactions worth billions of dollars, alleging that former Sampo Bank clients resided mostly in offshore jurisdictions and were receiving transfers from Russian shell companies that were not justified by real exchanges of goods or services but instead were likely concealing widespread tax evasion and money laundering.[5]

According to the Financial Times, in 2010, a meeting of Danske's Executive Board noted the high level of suspicious activity reported from Estonia, but later that same year, managers agreed they

were 'comfortable' with 'substantial Russian deposits'. Meanwhile, the share of the Estonian branch's profits coming from foreign money began to increase significantly. In 2011, despite only accounting for 0.5 per cent of the bank's assets, the Estonian branch generated 11 per cent of Danske Bank's total profits before tax that year. The Financial Times furthermore stated that Lars Morch, at that time the new executive ultimately responsible for Estonia, said in 2013 that the non-resident business needed to be 'reviewed and potentially reduced'. In minutes from an internal meeting at Danske Bank that were first revealed by the Financial Times, Mr Borgen, then Chief Executive Officer of Danske Bank, apparently referred to 'the need for a middle ground'.[6]

In 2013 and 2014, an internal whistleblower, who headed the trading unit in the Baltics from 2007 to 2014, warned Danske Bank's Executive Board about suspicious activities at the Estonian branch.[7,8] In reaction to these increasing allegations of wrongdoing, it is reported that Danske Bank's Internal Auditors produced a critical report on non-resident business.[9]

According to the Financial Times, a board meeting heard the recommendation of one Executive Director to exit the 'offshore business', but Mr Borgen (ex-Chief Executive Officer of Danske Bank) 'found it unwise to speed up an exit strategy as this might significantly impact any sales price'.[10]

After these allegations, the Bank made a thorough review of its clients and all transactions between 2007 and 2014. An investigation of the events was carried out, including whether staff or senior management, including the Executive Board and Board of Directors, sufficiently carried out their obligations. In the conclusion of the report, the Chairman of the Board of Directors stated that:

> *The Bank has clearly failed to live up to its responsibility in this matter. This is disappointing and unacceptable and we offer our apologies to all of our stakeholders — not least our customers, investors, employees and society in general. We acknowledge that we have a task ahead of us in regaining their trust.*
>
> *There is no doubt that the problems related to the Estonian branch were much bigger than anticipated when we initiated the investigations. The findings of the investigations point to some very unacceptable and unpleasant matters at our Estonian branch, and they also point to the fact that a number of controls at the Group level were inadequate in relation to Estonia.*[11]

This message from the Chairman of the Board indicates that the failings of the bank were due to inadequate controls at Group level, which is supported by the key findings published by Danske Bank in the same report:

- a series of major deficiencies in the bank's governance and control systems made it possible to use Danske Bank's branch in Estonia for suspicious transactions
- in general, the Estonian branch had insufficient focus on the risk of money laundering, and branch management was more concerned with procedures than with identifying actual risk
- there were a number of more or less serious indications during the years, that were not identified or reacted on or escalated as could have been expected by the Group[12]

The Bank reported in a press release in September 2018 that the following measures had been taken in regard to the specific issues raised:

- Governance and oversight in relation to the Baltics have been strengthened with the introduction of a new pan-Baltic management.

- The independence of control functions in the Baltics has been strengthened and processes and controls have been raised to Group level to ensure the same level of risk management and control as in other parts of the Group.
- Initiated a comprehensive AML programme, which has led to major changes in the form of new organisational structures, new routines and procedures, as well as the implementation of new IT systems.
- Strengthened and will continue to strengthen the compliance knowledge and culture across the organisation, among other things through a strong management focus and extensive mandatory training. Over the past twelve months alone, internal and external training service providers provided almost 70 different AML training courses across the organisation. Approximately 20,000 employees have been given training.
- Implemented risk management and compliance in performance agreements of all members of the Executive Board and senior managers.
- Generally strengthened the three lines of defence, which also includes ensuring increased independence of control functions and making sure that whistleblower reports and correspondence with supervisory authorities form part of the reporting to the Board of Directors.[13]

SOUND COMPLIANCE CULTURE

The evolution of best practice, sometimes as a result of negative experience, is linked to the growing awareness by financial players of their responsibilities towards investors and stakeholders in general. In the background lies a continuously evolving regulatory context among European Union directives and recommendation reforms of other international and domestic legislation in the fields applicable to the financial services players' multinational dimension.

According to a press release, the breadth of suspicious activity by customers of the Estonian branch of Danske Bank was vast. Some of the customers had shared addresses or held properties that were suspicious, others seemed to have significant differences between actual revenue and payment activities or were even publicly associated with money laundering, while dozens of Danske Bank's employees are now suspected of collusion as they apparently had been involved in suspicious payments.[14]

Financial players should consider integrity and compliance with external and internal regulations as an essential part of the culture for the entire organisation and as a competitive advantage in doing business. Compliance protects the brand and strengthens the entity's relationship with all its stakeholders and hence should be considered as adding value and not solely as a burden increasing overhead costs. If the employees of the entity are not well-trained on integrity and compliance with external and internal regulations, compliance culture will never be the foundation of the structure, which holds up a company's reputation and values.

To achieve a sound compliance culture, there are several foundational layers and pillars that must underlie, inform and guide the behaviour of all employees within an organisation and form the basis on which the overall company's success rests and leverages from.

THE FOUNDATION

Tone at the top creating a solid foundation to build upon

What is often referred to 'tone at the top' is the foundation every organisation builds its success upon. Compliance is most effective in a corporate culture that emphasises standards of honesty and integrity and in which senior management (for the purposes of this paper shall be defined as the

decision-makers of the business) leads by example. Senior management of the organisation must be firmly committed to the achievement of high standards of compliance throughout the business, as well as promoting the values of correctness and honesty, with the support and advice of its Compliance Officers.

Senior management has the ultimate responsibility for compliance with laws, regulations and administrative provisions applicable to their entities. It is the senior management's responsibility to ensure that both the second and third lines of defence have the necessary authority, resources and expertise to carry out its duties, among which is enforcing the requirements of internal policies.

In the case of Danske Bank, it is reported that recurring warnings about serious misconduct to the Group's senior management, regardless from whom the reporting was made, that is, external or internal, employees or the third line of defence, did not result in thorough investigations, nor in any similar immediate action. What is seen when reading reports about the Danske Bank scandal is the lack of involvement by the second line of defence and their role in identifying, investigating and reporting the misconduct, especially regarding the reporting made to senior management at Branch and Group level and the consequences.

Compliance is every employee's responsibility

Looking at the Danske Bank case, the fact that only one whistle-blower reached out to senior management seems rather surprising given the vast extent the scandal is now known to have reached and the period during which the misconduct took place. At the same time, it is reported that various employees are under investigation for collusion with customers to get around background and security checks. The question that could be asked is whether the fear of retaliation among employees was bigger than the fear of being found guilty of collusion for money laundering.

As one of the responses to the publication of the scandal in 2018, Danske Bank has taken the initiative to strengthen their whistle-blower procedures to transfer the responsibility for receipt, review and investigation of the reports to Group Compliance.[15]

Regardless of their seniority within the organisation, every employee must be required to exercise a strong commitment towards compliance. Compliance must be an integral part of the financial entity's business activities, and each individual must accept responsibility for compliance in their job and pursue it with the spirit and letter of the law as well as all applicable rules and legal requirements. Employees are required to familiarise themselves with their compliance obligations (foremost those stated by the entity's Code of Conduct and Policies) and meet them in their day-to-day business activities, acting with due skill, care and diligence.

Correctness and honesty are key values

Financial players must work in compliance with current legislation, professional ethics and internal rules. The pursuit of each entity's interests cannot justify conduct violating the principles of correctness and honesty. The entity must be focused on maintaining the highest level of integrity and reputation at all times, and hence, must require it to demonstrate a good understanding of applicable laws, regulations and standards in the markets and jurisdictions where they operate and fully comply with them.

If an employee, both at entity and Group level and regardless of seniority and level of assigned responsibility, does not demonstrate ethical behaviour at all times and does not promote the entity's

key values, it has to be questioned whether this could encourage further misconduct on a different level. An organisation should accordingly ask itself to what extent exceptions may be accepted and potentially at what price. At the same time, the question should be raised whether penalising misconduct is a meaningful tool for promoting key values among all staff members.

Simple rules and promotion of such rules can help focus on key risks, as well as develop a guide for the future. Greater trust, increased transparency and less complex risks will ultimately make the overall compliance controls more robust.

COOPERATION AND COLLABORATION WITHIN BUSINESS LINES AND FUNCTIONS

For an organisation to be agile and leverage from a sound compliance culture, second and third lines of defence as well as every internal department need to collaborate. As a first step, it is key to understand each other as business partners rather than competitors limiting own opportunities. As a second step, it is crucial to identify overlapping matters between the second and first line of defence departments — we must benefit from reciprocal exchange.

To do so, the following points are critical.

Have a clear business model that is not unduly complex

Not losing sight of the big picture and ensuring that a clear and simple business model, as well as strategy, is defined and communicated to all employees. A streamlined business model can help reduce complexity and control weaknesses, which is especially important in multinational organisations where language and cultural barriers are additionally added to the hurdles to master for all lines of defence.

Another point worth considering is the complexity of reporting lines. The Danske Bank scandal showed that a whistle-blower reached out to senior management at Group level. A question that can be raised is whether a more advanced whistle-blowing process communicated to all employees guaranteeing the review of anonymous reports by more than one addressee could have led to an earlier detection and investigation of the scandal, thus potentially limiting both financial and reputational damage.

Simplify the internal organisation

Having complex internal structures and many management layers can make it more difficult for organisations to respond to external developments, including warnings and risk communication.

A simpler organisation, by contrast, can take decisions more quickly, which enables it to respond more flexibly to new business opportunities, as well as to risks that can arise from future and current developments. It can also help employees feel more involved in, and committed to, change and simply obeying the rules.

Senior management of organisations should determine and provide the resources needed for the establishment, development, implementation, evaluation, maintenance and continual improvement of the Compliance Management System appropriate to their size, complexity, structure and operations.

Resources should be understood in a broader sense and include financial and human resources, as well as access to external advice and specialised skills, organisational infrastructure, contemporary reference material on compliance management and legal obligations, professional development and technology.

Interdepartmental communication

As already indicated, publicly available information regarding the interaction of

all three lines of defence in the Danske Bank scandal is limited. Therefore, questions may be asked about how years of external audits did not spot irregular activities and transactions, and whether respective audit findings were flagged by external auditors.

In the aftermath of the scandal, Danske Bank took the initiative to 'strengthen the whistle-blower setup by transferring the responsibility for investigating reports to Group Compliance and implementing a stronger governance setup to handle reports. Furthermore, we have increased information about the whistle-blower system to all employees and introduced mandatory training'.[16]

Defining relevant departments and bringing them together on a regular basis to ensure responsibilities are clearly defined, and policies are updated regularly and made available to all employees is a critical and elemental step in promoting compliance with policies. This not only involves the first line of defence but can include the Legal department to review policies from a regulatory standpoint, and the Human Resources (HR) department to look at policies to ensure they are easy to read and organise training for all employees regarding the critical points of attention.

Have dedicated policy owners

Policies need to have an owner. Although sometimes there may be multiple parties with input, either a specific individual or a group of individuals need to own a specified policy and ensure that it reflects changes in laws, regulations and company practice at all times while meeting the business needs.

Compliance failures can often stem from outdated policies that have not been reviewed since the date of implementation. Companies can run into trouble when it comes to accountability or disciplinary action if an employee violates an outdated policy.

At the same time, a policy that can affect various departments but has not been reviewed and approved by all relevant departments can be potentially harmful. The key is to combine ownership and collaboration in implementing and keeping policies up to date. A review and approval process that ensures operational efficiency and compliance at the same time must be set up to ensure that policies are updated with laws and regulations and that employees have the means to adhere to the policy.

Has the organisation ensured a minimum of (enforced?) collaboration between departments for the setup and maintenance of policies and procedures?

We refer back to Danske Bank where it may be questioned whether Group standards in terms of know your customer principles were applied and whether there was any exchange between Group and local compliance departments. Multinational organisations need to ensure that there is a reconciliation between local processes and carry out a regular gap analysis between Group and local laws.

Have policies and procedures that are easily accessible and available

Polices are often spread throughout the organisation from HR and IT policies to health and safety policies. Organisations, therefore, need to ensure that policies are not only updated regularly as noted above but are readily available, be it through a policy management software, a company intranet or an HR portal.

When employees have a question, they need to be able to look at the policy and address their questions to the respective owner or group of owners. If they cannot find an answer to their questions or do not understand the policy, it is difficult to train them. This is where automated solutions at

Group level are key because such policies are housed at a central location. Although SharePoint sites and intranet sites can work, there is still a lack of centralised control. If a policy cannot be made readily available and understandable to the bulk of users, we are not going to have good compliance.

In addition, we need to pay specific attention to just having employees sign off on policies for the sake of an audit trail versus real training. It is worth taking the time to analyse, in the context of a particular business, whether employees can make suggestions to policy amendments or ask for clarifications.

Training all business lines

A policy that has not been presented, explained and made available to all employees cannot be relevant. Processes and responsibilities that are not detailed to relevant employees cannot be crucial.

By doing this with an automated system, it is easy to track who saw the policy, who read it, who acknowledged it, who had training on a new or updated policy and who completed the certification.

A simple confirmation that an employee has read and understood a policy serves well for audit purposes and for the theoretical compliance of regulatory requirements. Will this prevent, however, the organisation from being engulfed by major scandals? Should companies invest in more than a simple confirmation that employees have read a policy?

Compliance costs

Compliance cost refers to all expenses that a company incurs to adhere to industry regulations. Compliance costs are simply the ongoing price for following the rules as they are. Compliance costs include salaries of people working in compliance, time and money spent on reporting, new systems required to meet retention and so on. These costs typically increase as the regulation around an industry increases. For a publicly traded company, compliance costs include all industry-specific compliance — environmental assessments, HR policies and so on — as well as the costs of shareholder votes, quarterly reports, independent audits and so on.

Following the scandal, Danske Bank, in an effort to strengthen the compliance knowledge and culture across the organisation, within 12 months had internal and external training service providers provide 'almost 70 different AML training courses across the organisation. Approximately 20,000 employees have been given training'.[17]

UTILISING FOUNDATION AND PILLARS

Coming back to the initial question of defining responsibilities and coordination with other departments to better support businesses, it is critical to have a sound Compliance Management System, which includes the following activities to be performed as an essential part of business operations.

How would a report with comparably sensitive content as described earlier — regardless of the issuer — be processed within the organisation? Are the respective controls in place to ensure the appropriate individuals and departments would be involved?

Each organisation must systematically identify its compliance obligations and their implications for its activities. The compliance obligations must be considered in establishing, developing, implementing, evaluating, maintaining and improving the Compliance Management System. Compliance obligations should be documented in a manner that is appropriate to the size, complexity, structure and operations of each entity.

Sources of compliance obligations could include documents, such as the code

of conduct, laws and regulations, internal regulations and authorisations, given to financial entities by their supervisory authorities.

Each entity must have processes in place to identify new and changed laws, regulations and other compliance obligations to ensure ongoing compliance; evaluate the impact of the identified changes; and, most importantly, implement any changes in the management of compliance obligations.

Where allowed by the local regulation, the compliance function can share resources with other units/departments, in particular, with Legal/Corporate Affairs. In any case, adequate safeguards must be put in place to ensure the separation of tasks and the prevention of conflicts of interest to guarantee the function's independence. A function is independent when it is objective and free from influences that may compromise its ability to undertake its duties in a fair and independent manner. The separation of the compliance function from other control functions and from operational departments must be guaranteed by expressly defining their respective roles and scope of activities.

To be effective, the compliance function must have a clearly defined mandate that establishes its role within the overall structure of the organisation. The compliance function must be positioned and perceived throughout the organisation as an essential part of the internal control system. It should have a tangible role and work closely with the business while preserving its authority and status as an independent function. Working closely with the business is an opportunity to get across the organisation the values that the compliance function brings, as well as being a chance for the compliance function to better understand the business. Partnering with the business helps to increase the culture of trust, accountability and transparency and to better integrate a good compliance risk management in daily business activities.

The compliance function's role and objectives need to be carefully balanced with those of other functions, such as legal, risk management and internal audit, optimising synergies wherever possible and complementing each other. The control functions are expected to cooperate closely and exchange information to guarantee the cross-disciplinary nature of the information and an efficient and effective Internal Control System.

As mentioned above, business management acts as the first line, ensuring continuous monitoring, which is built into the business processes so that compliance and risk processes, as well as controls, are always performed whenever an overlying business activity is completed. The second line of defence, compliance and risk, monitors and facilitates the implementation of effective compliance and risk management practices by operational management and assists risk owners in reporting adequate risk-related information up and down the organisation. Internal audit will cover how effectively the organisation assesses and manages its risks and will include assurance on the effectiveness of the first and second lines of defence.

Although these distinctions seem reassuringly clear cut, closer examination suggests that there are grey areas, and the ever-increasing regulatory burden has put a growing strain on technology and the business within our organisations.

HOW CAN WE OVERCOME THESE CHALLENGES?

Use compliance to one's advantage

Technological innovations introduced to aid regulatory compliance may be used for better business outcomes. For example,

technologies that are applied for regulatory data collection, protection and reporting can be used to improve data accuracy, help with the single view of the customer and lead to improved customer experience and faster speed to market.

Moreover, is the factoring done in compliance when pitching for a new client? Is the compliance presented as a benefit to share- and stakeholders? Is the appetite of the counterparty assessed for a strong compliance environment in current business? Is a sound compliance environment considered when benchmarking against industry peers or competitors?

Thinking ahead of the game

With regulators putting all three lines under pressure to cover more risks and demonstrate their assurance capability, companies are in danger of engaging in an internal race, with each line developing, for example, expensive data capabilities that they use exclusively but sometimes overlap. To improve efficiency here, companies need to try to develop tools that can be used by all functions, albeit in different ways.

When implementing new technologies and solutions, it is crucial to make sure they will be flexible enough to keep up with the regulatory environment in addition to newer technologies. At the beginning of every digital transformation project, it makes sense to consider the potential regulatory implications. To do this, one must build flexibility into one's own governance strategies, such as automating data retention policies across varied data types and regulatory regimes, so they will be able to adhere to shifting global regulations and avoid penalties.

Referring back to the Danske Bank scandal — has the organisation assessed potential costs and benefits of implementing effective whistle-blower mechanisms in excess of pure legal requirements (if any)?

For global organisations with hundreds of interacting systems, tasks like data tracing represent a huge workload that is almost impossible to undertake manually without sacrificing some of the speed and agility that is necessary for the function to perform effectively. Being able to at least partially automate data testing would similarly free up human talent that could be put to better use. But, while automation can make it easier and faster for humans to perform their role, the function will still require professionals with the right background and skills to interpret data.

Automation undoubtedly brings efficiency to functions like control assurance by freeing manpower from performing repetitive, time-draining tasks and therefore cutting costs. Used best, it also improves a function's effectiveness by maximising human potential. By presenting humans with contextualised information, such technology allows them to make decisions that previously were not possible. For example, by using automation to not only provide information about the performance of controls but also flag how that performance might impact the business, the assurance function can better prioritise.

Focus — do not be distracted by the regulatory environment

Compliance is an ever-moving target that can become overwhelming if organisations allow it. Challenges for legal and compliance functions can seem maddeningly complex as well as time and resource consuming. When new regulations come out, many companies do not feel ready for it and are concerned about their ability to report data to senior management and their respective regulators as well as providing adequate transparency.

Does the organisation view regulatory change not only as a burden but as a chance to assess and introduce additional safeguards that have a potentially reassuring effect for clients and constitute a commercial advantage?

CONCLUSION

Compliance costs can be incurred as a result of local, national and international regulations and generally increase as an organisation operates in more jurisdictions. Global organisations that have operations in jurisdictions all over the world with varying regulatory regimes naturally face much higher compliance costs than an organisation operating solely in one location.

In corporate strategy, the second line of defence provides advice on whether and how strategic and business model considerations are likely to satisfy the regulators' judgments about the fair treatment of customers, market integrity and, in some case, financial soundness. The question is difficult because the costs are concentrated, while the benefits are diffused.

Thinking about some of the cost arguments:

- Chief financial officers (CFOs) grumble about the size of a budget request
- Add up employee hours spent on compliance training
- Fees from the audit firm and outside counsel
- Hours senior management or audit committees spend in meetings talking about compliance

The benefits, on the other hand, 'think of all those regulatory fines and reputational damage we did not have!' is hardly an impressive argument to senior management.

Jesper Berg, Director General of the Danish Financial Regulator, stated that the Estonia case has been extremely damaging to the trust of the public in the financial system and to Denmark's international reputation. It is decisive that the work of rectifying this continues with increased strength. A proposal was published in January 2019 that shall contribute to strengthening the anti-money laundering (AML) supervision and the work of the Danish Financial Supervisory Authority in general. Among the main categories of the proposal are:[18]

- Better and more effective defence lines in the banks
- Obligation to provide information and criminal liability as well as better protection of whistle-blowers
- Fiercer consequences when a bank's management fails to recognise its responsibility

The key takeaway from this paper is that although the rules are complex they must be known. Policies and procedures must be read as a starting point. Maximise the knowledge of all parties and the scope of the internal relationships. Strengthen relationships between compliance and the business and gather important information.

No automated monitoring tool or system is intended to replace staff intuition, experience and the need to remain vigilant. Boost the compliance culture in the company and lead by example.

References and Notes

(1) The Institute of Internal Auditors (2013) 'The Three Lines of Defense in Effective Risk Management and Control', available at: https://na.theiia.org/standards-guidance/Public%20Documents/PP%20The%20Three%20Lines%20of%20Defense%20in%20Effective%20Risk%20Management%20and%20Control.pdf (accessed 2nd October, 2019).

(2) Bruun & Hjejle (2018) 'Report on the non-resident portfolio at Danske Bank's Estonian branch', https://danskebank.com/-/media/danske-bank-com/file-cloud/2018/9/report-on-the-non-resident-portfolio-at-danske-banks-

estonian-branch-.-la=en.pdf (accessed 2nd October, 2019).
(3) Gabriella Gricius (2018) 'The Danske Bank scandal is the tip of the iceberg', available at: https://foreignpolicy.com/2018/10/08/the-danske-bank-scandal-is-the-tip-of-the-iceberg-money-laundering-estonia-denmark-regulation-financial-crime (accessed 2nd October, 2019).
(4) Bruun & Hjejle, see ref. 2 above.
(5) Francesco Guarascio (2019) 'Supervisors ignored Russian warnings over money laundering at Danske: Document', available at: https://www.reuters.com/article/us-danskebank-moneylaundering-eba/supervisors-ignored-russian-warnings-over-money-laundering-at-danske-document-idUSKCN1S60O2 (accessed 2nd October, 2019).
(6) 'Danske: Anatomy of a money laundering scandal', *Financial Times*, available at: https://www.ft.com/content/519ad6ae-bcd8-11e8-94b2-17176fbf93f5 (accessed 2nd October, 2019).
(7) *Financial Times*, see ref. 6 above.
(8) Teis Jensen (2018) 'Danske Bank whistleblower was former Baltics trading head: Denmark's Berlingske', available at: https://www.reuters.com/article/us-danske-bank-moneylaundering/danske-bank-whistleblower-was-former-baltics-trading-head-denmarks-berlingske-idUSKCN1M61KU (accessed 2nd October, 2019).
(9) Bruun & Hjejle, see ref. 2 above.
(10) *Financial Times*, see ref. 6 above.
(11) Danske Bank (2018) 'Findings of the investigations relating to Danske Bank's branch in Estonia', available at: https://danskebank.com/news-and-insights/news-archive/press-releases/2018/pr19092018 (accessed 2nd October, 2019).
(12) Bruun & Hjejle, see ref. 2 above.
(13) Danske Bank, see ref. 11 above.
(14) Gabriella Gricius, see ref. 3 above.
(15) Danske Bank, see ref. 11 above.
(16) *Ibid*.
(17) *Ibid*.
(18) Financial Supervisory Authority (2019) 'Statement on supervision of Danske Bank as regards the Estonia case', available at: https://www.dfsa.dk/en/News/Press-releases/2019/Report-on-the-Danish-FSAs-supervision-of-Danske-Bank-as-regards-the-Estonia-case (accessed 2nd October, 2019).