Three lines of defence — is it the right model?

Received: 29th October, 2021

Donna Turner
Senior Consultant, Sciens Consulting, UK

Donna Turner *is a highly capable Risk, Compliance and Financial Crime professional with 22 years of experience in the financial services industry. Donna is now a senior consultant incorporating her wide-ranging experience into strategy, business development and problem solving to help firms with their governance, risk and compliance challenges. Donna holds two International Compliance Association (ICA) Diplomas, the first in Anti Money Laundering and secondly in Governance, Risk and Compliance. She has been an invited speaker at a number of events including the annual industry forum on Retail Conduct Risk, the Compliance Monitoring & Assurance Strategy industry forum and the International Compliance Association, Big Compliance Festival.*

Abstract

Despite the plethora of legislation, regulatory requirements and industry guidance that financial institutions need to follow, there is an ever-increasing number of scandals involving risk management, governance and compliance failings. Each time a scandal hits the headlines, supervisory bodies, and organisations themselves, consider how to respond and further strengthen the control environment and enhance policies and the related procedures to prevent the same or similar instances occurring. This paper describes the Three Lines of Defence model within financial organisations, considers the Wells Fargo customer account fraud scandal and the departure of Citigroup's Chief Risk Officer and debates whether the revisions to the Three Lines of Defence model proposed by the Institute of Internal Auditors will strengthen the risk and compliance frameworks within organisations and provide a more robust system of corporate checks and balances, endorsed by both the industry and the regulators.

Keywords: Three lines of defence, wells fargo, citigroup, institute of internal auditors

Donna Turner

INTRODUCTION

Where does the three lines of defence model come from? Many people believed it originated from military strategy or from sport but that's not the case, and the answer is nobody really knows. What we do know is that the concept has been around for a long time. The Financial Services Authority (FSA) first referred to the three lines of defence in a policy statement on operational risk systems and controls issued in 2003[1] which stated, 'A number of firms had adopted a three lines of defence approach, where business line management provided the first line, risk functions the second line, and internal audit a third line (each of which reported into different executive management)'. Despite the lack of clarity as to its origins, this statement reveals that firms were adopting the three lines of defence model even in the absence of regulatory stipulation.

Since the Institute of Internal Auditors (IIA) published its position paper in 2013,[2] the three lines of defence model has been formalised, adopted and even promoted by the financial services industry including regulators and industry organisations as best business practice for coordinating risk management within an organisation. During a speech by Clive Adamson, the then Director of Supervision at the Financial Conduct Authority (FCA) in 2014, he stated, 'while I support a strong three lines of defence model, it seems to me that the

E-mail: donna@riskshapes.com

Journal of Financial Compliance
Vol. 5, No. 3 2022, pp. 237–247

2398-8053

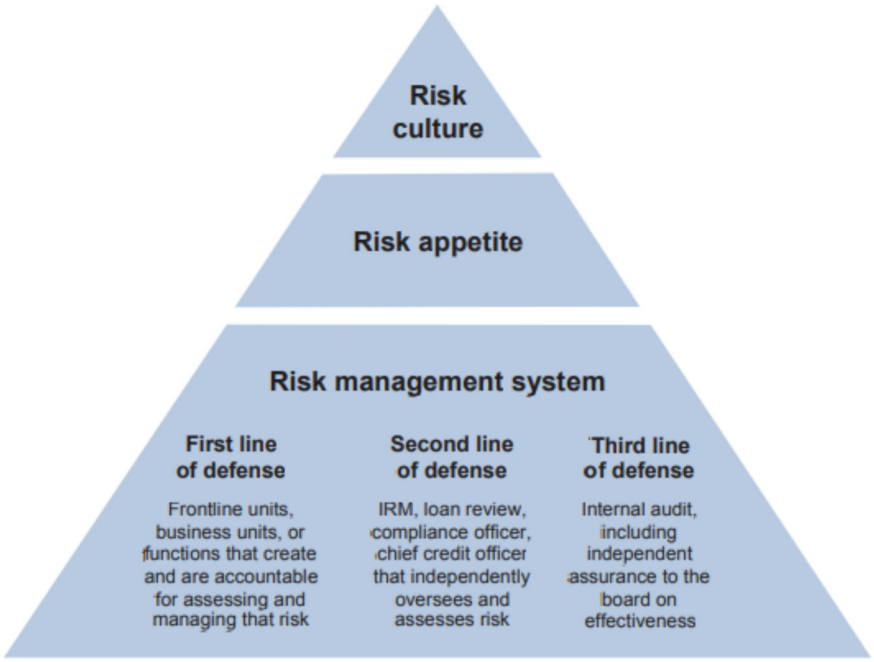

Figure 1 A visualisation of the risk governance framework
Source: The Office of the Comptroller of the Currency's (OCC), Comptroller's Handbook booklet, 'Corporate and Risk Governance'.

conduct question is more a business model and cultural challenge and therefore should be firmly rooted in the first line'.

The Basel Committee on Banking Supervision (BCBS) reaffirmed[4] that risk governance frameworks 'should include well-defined organisational responsibilities for risk management, typically referred to as the three lines of defence'.

The Office of the Comptroller of the Currency's (OCC), Comptroller's Handbook booklet, 'Corporate and Risk Governance',[5] is used by OCC examiners in connection with their examination and supervision of national banks, federal savings associations and federal branches and agencies of foreign banking organisations. It defines a risk governance framework as an essential component in effectively managing enterprise-wide risks and the means by which the board and management, in their respective roles 'establish a risk management system with three lines of defence to identify, measure, monitor, and control risks'. They represent this graphically in Figure 1.

In theory, it is a simple construct where the first line of defence is expected to own and manage risks by maintaining effective internal controls and executing risk and control procedures on a day-to-day basis. The second line of defence consists of risk management and compliance functions who support the first line by facilitating and monitoring the implementation and adherence to risk management standards and practices. The third line of defence provides an organisation's governing body and senior management with assurance on the effectiveness of risk management and internal controls, based on a level of independence and objectivity that is not available in the second line of defence. In summary,

- The 1st line of defence owns and manages the risks.

- The 2nd line of defence includes functions that oversee the risks.
- The 3rd line of defence provides independent assurance.

Given the theoretical simplicity and the fact that there is very little, if anything, in the way of alternative risk management frameworks in use, why does it get such a perfunctory response from industry practitioners and is often cited as the point of failure in many scandals?

THE THREE LINES OF DEFENCE MODEL

Good intentions

The model is intended to promote risk ownership and a stronger risk management culture while eliminating inefficiencies, gaps and overlaps that can occur in the management of risk and compliance by multiple functions. The IIA's position paper[6] states in its introduction that 'The Three Lines of Defence model provides a simple and effective way to enhance communications on risk management and control by clarifying essential roles and duties'. It is not uncommon particularly in larger organisations for duties related to risk management and control to be split across multiple departments and teams such as internal auditors, risk management specialists and compliance officers, so it makes sense that those duties are well defined, articulated and understood to assure that risk and control processes operate as intended.

In an article by Oliver Wyman defending the three lines of defence,[7] the features of an effective model include:

- Incorporating a process-by-process view.
- Fully embedded and consistently understood.
- Periodic testing with focused deep dives on areas of complexity or observed issues.
- Regularly updated to reflect changes in the business.
- Evidence of debate and challenge.

Other factors also need to be in place if the intentions of a three lines of defence model are to be successfully achieved. Specifically defining and documenting which risks are covered by the framework and those that are not and expressing the objective of the second line and its relationship with the first (eg partnership or trusted advisor versus policy and policing).

Criticisms

But rather than providing a cohesive and coordinated approach to deploying resources to manage risks appropriately and effectively, does the three lines of defence model actually get in the way?

Some have criticised the three lines of defence model as being too focused on defence, rather than creating value, based on the impression that risk, compliance and audit teams are more focused on satisfying the regulator rather than enabling and supporting the business to deliver their strategic plans. With the introduction of the Senior Managers & Certification Regime (SMCR)[8] and the focus on and restructuring of staff remuneration, unsurprisingly, senior managers have prioritised achieving clean audit reports. Managers are often held accountable for just the number of findings appearing in an audit report and not the overall risk performance — all of which contributes to an adversarial or a 'them and us' relationship between the three lines.

The model expresses each line as being distinct and separates responsibilities for executing, advising and reviewing control activities, but there is no consistency across firms in its interpretation, and instead significant divergence its implementation within firms. The Basel Committee noted in 2014 that 'banks have inappropriately classified responsibilities across each of the three lines of defence' in its review of the management of operational risk.[9] More recently in 2019, the Association of Chartered Certified Accountants (ACCA) noted in its report on

embedding risk management[10] that organisations 'struggle to reconcile the theoretical idea of a three lines approach with the practical realities of implementing one'.

The IIA position paper[11] states that the three lines should exist within every firm, regardless of its size and complexity and should not be combined unless exceptional circumstances arise but the reality is that some smaller or newer organisations may lack the resources and personnel to implement three wholly separate lines. Others who have adopted the model lack specificity, or create additional lines (1.5, 2b etc) to try and fit the model to the organisational structure and processes. While one bank may be integrating risk and compliance teams to achieve operational synergies, another will be separating functions and responsibilities to give each a distinct voice at the executive and Board tables. Some banks will move staff from the second line into the first to assist with control implementation and to review control effectiveness. This can be a useful way to get business units to buy into the risk framework, but for some this may be undesirable as the relationship between the business units and the risk function may become too 'pally' or familiar, leading to things falling through the gaps because they are missed or ignored. It may also allow business management to pass on the responsibility for risk management and therefore not take ownership of the risks, so others may prefer to have two parts to the 2nd line to review control effectiveness and to own risk policies and framework. In addition, separate assurance teams are created across the lines to provide further comfort where the wider model is not trusted.

The model also introduces other areas of ambiguity when considering the role and accountabilities of the Board and its committees which are not technically part of the three lines of defence structure and other functions such as Human Resources which is commonly the owner of the employee remuneration policy, which in theory gives them control over risk behaviour and incentives but is rarely considered to be a core component of a firm's risk management framework.

The IIA position paper[12] states: 'in the worst cases, communications among the various risk and control groups may devolve to little more than an ongoing debate about whose job it is to accomplish specific tasks'. But for many firms, the three lines of defence model seems to create this very specific problem that it was intended to prevent especially where control over resources and funding are not aligned to the model accountabilities.

The three lines of defence approach is widely implemented and for many organisations staffing and financial resources devoted to it have increased significantly but it seems that few place real confidence in it, instead believing it to be a rigid model by placing everyone in a box with a defined role and assuming that the execution of risk management and controls is vertical and linear. Although intended to be a framework to define risk and control responsibilities and deploy resources effectively, the three lines approach has the potential to limit a firm's ability to manage risks in an integrated manner, constrain sensible behaviour, generate workload and create artificial barriers and silos. With all these types of challenges, the question is — does having a three lines of defence framework really help firms to manage risk better than not having it or having something different.

If the three lines of defence worked well, in theory most issues should be detected almost immediately by the first line, so given its long standing and widespread use, why is it perceived to be failing to prevent so many of the financial services scandals?

Wells Fargo: A few bad apples?

The well-documented and heavily reported customer account fraud scandal at Wells

Fargo is an interesting case study to reflect on, particularly considering its reputation at the time for having a robust risk culture.[13]

Under significant pressure to meet business quotas and a remuneration system based heavily on bonuses, the bank's employees opened accounts in the names of customers, without their knowledge or consent. Once opened the employees transferred money to temporarily fund the new accounts which allowed them to meet sales goals and earn extra compensation. Some employees decided not to engage in the unethical sales practices and left, others were fired for reporting the misconduct. The former CEO, John Stumpf claimed that the scandal was the result of a few bad apples who did not honour the company's values and that there were no incentives to commit unethical behaviour. A bold statement considering the action by Wells Fargo to subsequently fire over 5,300 employees (estimated to be around 2% of the workforce) related to the fraudulent sales practices. Considering what happened it is not unreasonable to conclude that business senior management, risk management and compliance functions and finally internal audit, ie, all three lines of defence, failed to prevent, identify or stop the large scale and long running fraudulent activity.

But was it really a three lines of defence model failure? The Board of Directors commissioned an independent investigation[14] that identified cultural, structural and leadership issues as the root causes of the improper sales practices. The report cites: the wayward sales culture and performance management system; the decentralised corporate structure that gave too much autonomy to the division's leaders; and the unwillingness of leadership to evaluate the sales model, given its success for the company.

When a firm's incentives motivate and drive employees on a mass scale to engage in unethical behaviour and the career opportunities and livelihood of those who raise concerns is threatened then the culture of the organisation set and evidenced by the Board and senior management is massively flawed. Could any variant of a three lines of defence model be expected to identify and successfully mitigate this type of senior governance failing. Should the culture of an organisation and its ethical compass be part of the risk taxonomy covered by a three lines of defence framework? Who do risk, compliance and audit employees turn to when undesirable behaviours are encouraged, supported or just ignored by those at the very top of the organisation? The three lines of defence is an internal risk governance framework but how well can it work when deficiencies exist at the highest levels? In these instances, it is the external auditors and regulators who provide the next layer of defence against imprudent behaviour.

The three lines of defence framework is based on the principle that specific roles are assigned to the various risk and control functions so that each area understands the boundaries of their responsibilities and how their positions fit into the organisation's overall risk and control structure. A recent governance, risk and compliance benchmark report[15] conducted by Compliance Week in partnership with Riskonnect polled 113 compliance, risk and audit executives from around the world to assess the state of organisations' risk management capabilities; and how effective they are at mapping risks. The results are concerning, 65 per cent indicated they are only 'somewhat confident' in their organisation's ability to map each control it has to a given risk or requirement while 14 per cent said they are 'not confident'. When asked how confident they are in their organisation's ability 'to map ownership of each risk, requirement and control to a specific individual or role', 61 per cent said they are only 'somewhat confident', while another 15 per cent said they are 'not confident' at all. Furthermore, most respondents (64 per

cent) expressed just mediocre confidence in their organisation's ability to map risks to the risk drivers across functions, while 19 per cent said they are 'not confident'. How can a three lines of defence model operate effectively if risks and controls are not mapped to an appropriate function or designated owner.

Citigroup: Failure to establish and implement

How the three lines of defence model is implemented has a direct impact on its efficacy. The US$400m fine levied by the Office of the Comptroller of the Currency (OCC) on Citigroup — and the subsequent enforcement action ordering the firm to overhaul its risk management and compliance programmes — is a good case in point.[16] The OCC and the Federal Reserve each issued orders outlining steps the bank should take to rectify weaknesses and deficiencies in its risk management programmes and internal controls. In its consent order[17] the OCC stated that 'For several years, the Bank has failed to implement and maintain an enterprise-wide risk management and compliance risk management programme, internal controls, or a data governance programme commensurate with the Bank's size, complexity, and risk profile'. The OCC 'identified unsafe or unsound practices with respect to the Bank's internal controls, including, among other things, an absence of clearly defined roles and responsibilities and noncompliance with multiple laws and regulations' and 'failure to establish effective front-line units, independent risk management, internal audit, and control functions'.

The OCC remediation requirements defined within Article VI of the consent order[18] included 'The establishment and documentation of the responsibility and accountability for risk management related functions in each front-line unit and independent risk management unit including the establishment of procedures and processes that clearly define risk management related roles and responsibilities for each unit, and that ensures compliance with enterprise-wide corporate policies, and laws and regulations'. In response to the orders, Citigroup pledged to spend US$1bn over several years to transform its risk and control environment.[19]

How is a three lines of defence model expected to function when it is not implemented properly? Is the outcome for Citigroup really a surprise when the thoroughness of implementation is absent? As evidenced by this case, a poorly implemented three lines of defence model only provides a false sense of security and very little real management of risks.

A NEW APPROACH

Despite the theoretical principles, the focus of attention for many is on finding ways of making the system more effective and technology enabled to respond to criticisms articulated by practitioners, legislators and regulators.

Add more lines

A common suggestion is to add more lines of defence, in particular regulators or external auditors as the fourth line that builds on the work of the other three, to provide specialist support to organisations and protect stakeholders by setting standards, supervising and monitoring control issues.

The Financial Stability Institute published a paper[20] which provided a root cause analysis of how the implementation of the lines of defence model failed in practice during significant banking scandals with the following key findings:

- Misaligned incentives for risk takers in the first line of defence — management put greater emphasis on and set compensation based on the achievement of financial

objectives rather than control-orientated objectives.
- Lack of organisational independence of functions in the second line of defence — control functions might lose their independence by being embedded in the organisation through engagement and exchange of information with other functions of the first and second line of defence. Lack of skills and expertise in second line functions — remuneration and experience in first line functions are still considerably higher and more senior than in second line functions.
- Inadequate and subjective risk assessment performed by internal audit — failure to identify high-risk areas lead to audits focussing on the wrong areas therefore undermining the effectiveness of the third line of defence.

It proposed a four lines of defence model that assigns supervisors and external auditors with a specific role in the organisational structure of the internal control system.

External audit and regulators are indeed additional defences against undesirable outcomes, but they are outside the control of firms themselves. This approach conflicts with the concept of the three lines of defence as an *internal* governance framework to prevent breaches of a firm's risk appetite. If risk appetite is clearly defined and measured and monitored appropriately it becomes far easier to define the roles of the three lines and allows risk and compliance managers to have influence over business decisions. Those opposed to the concept of an external fourth line argue firms should not need to rely on regulators to ensure that they are remaining within their own risk appetite.

Although senior management are outside the construct of the three lines, they have the responsibility for setting the organisation's objectives, defining strategies to achieve those objectives and establishing governance structures and processes to best manage the risks in accomplishing those objectives. As an alternative to the inclusion of external supervisory bodies, can senior management roles and accountabilities be formalised and incorporated within the three lines of defence model to ensure it is robustly implemented?

Since the financial crisis and with the introduction of SMCR, UK regulators are now very focussed on the role of senior management, exerting direct influence on the composition and functioning of boards of directors. Individuals in positions which exercise significant influence over the business of the firm are interviewed before their appointment by regulators, questioned as to their competence and experience. They are given detailed job descriptions and required to undertake specific training.

Other countries' financial regulators have not gone so far but are still increasing their level of focus on boards. The German regulator, BaFin, has powers[21] to replace a poorly functioning supervisory board, stating that 'If senior management lack the sufficient qualifications or personal reliability, BaFin may require of the supervisory board that they be removed from office and may replace them with a special commissioner. BaFin may also dismiss members of supervisory boards who lack the necessary expertise or reliability and transfer the supervisory powers to a special commissioner'. US regulators do not currently pre-vet directors, but Federal Reserve bank examiners do now attend board meetings regularly to offer their views, and privately meet the chairs of audit and risk committees.

So, with the external oversight on senior management's competency, character and effectiveness will instances of unethical corporate culture such as that seen at Wells Fargo be picked up and rectified allowing a three lines of defence model to operate successfully or should this level of an organisation sit in the first line with the business and have full accountability for owning and managing the risks?

Implement a principles-based approach

Last year the Institute of Internal Auditors finalised revisions to its three lines of defence model for risk management and it is now referred to as the 'Three Lines Model'.[22] These are the first changes to the IIA's three lines of defence model since it was formally adopted in 2013.

The word 'Defence' has been removed from the title to emphasise the new focus on the creation as well as the protection of value to shareholders and stakeholders. Something that will be welcomed by many and especially by those that criticised the previous model for its over-cautious view of risk.

Perhaps to mirror the transition away from rules-based regulation and supervision, the biggest change is the adoption of a principles-based approach. The revised model sets out the following six principles:

- Principle 1 confirms that the governance of an organisation requires appropriate structures and processes that enable accountability, action and assurance.
- Principle 2 stipulates it is the role of the governing body to ensure appropriate structures and processes are in place for effective governance and that organisational objectives and activities are aligned with the prioritised interests of stakeholders.
- Principle 3 states that Management's responsibility to achieve organisational objectives comprises both first and second line roles. First line roles are most directly aligned with the delivery of products and/or services to clients of the organisation and include the roles of support functions. Second-line roles provide assistance with managing risk.
- Principle 4 requires that in its third-line role, internal audit provides independent and objective assurance and advice on the adequacy and effectiveness of governance and risk management.
- Principle 5 reiterates that the independence of internal audit from the responsibilities of management is critical to its objectivity, authority and credibility.
- Principle 6 recognises that all roles working collectively contribute to the creation and protection of value when they are aligned with each other and with the prioritised interests of stakeholders.

This should provide greater flexibility in applying the model and recognise that in practice, governing bodies, management and internal audit do not simply fit into the rigid lines and roles that the original model suggested. The emphasis is upon collaboration and communication across the lines with the collective aim of the achievement of business objectives.

Is independence or integration more important?

In fact, the new model explicitly states that 'independence does not imply isolation' and that there is an expectation that there will be regular interaction and communication between first and second lines and internal audit to ensure that the work of internal audit is aligned to the objectives of the organisation and that duplication, overlap and gaps in assurance are minimised. But does this compromise second and third line independence? Can those individuals playing a challenger role still be legitimately independent?

Regulators have historically expressed concerns as to the appropriate levels of independence for each line, arguing that the second line may be too close to the business and remunerated in a similar way, or alternatively be too remote to be effective. Some employees in second or third line roles may consider their next career move to be in the business itself, so may be unwilling to be critical of the senior management whom their future careers might depend. Regulators as well as a firm's senior management will have to get comfortable with the second and third lines taking a more integrated

approach and being engaged and providing their perspective while controls are being designed and implemented.

The new model also recognises that there is often considerable fluidity between first and second line activities. It is also stressed that activities are not undertaken in linear sequence, but the roles of each line operate concurrently. The updated model now expressly permits a firm to blur its first and second line roles. Whereas in the prior model, the IIA had stated that lines could be combined only in exceptional situations.

The IIA rejected the view that the lines are structural elements of an organisation, and the new model does not explicitly list the departments that sit within each of the three lines. So, there is room for an organisation to interpret and implement an approach to suit its business objectives and circumstances, including placing certain departments outside of the model such as the Legal department. But this could add to confusion over who is in or out of the model and why and what that means in terms of accountability and access to and prioritisation of resources.

Many of the complaints of the previous 'defence' model appear to have been addressed but while offering flexibility, this new, principles based approach may be unworkable for some financial institutions. Many global banking regulators maintain supervisory expectations for high degrees of independence for second and third line roles. It is unclear if regulators would be satisfied with arrangements that may lead to the perceived relaxing of the 'segregation of duties' given that they have for a long time modelled some of their supervisory approach on the three lines of defence. There will need to be dialogue between the regulators and the industry to achieve practical implementation aligned to the three lines model. However, in a speech by the FCA's CEO, Nikhil Rathi, delivered at the FCA's Our Role and Business Plan webinar,[23] he highlighted 'the FCA must continue to become a forward-looking, proactive regulator. One that is tough, assertive, confident, decisive, agile. 'and 'to be more adaptive – constantly learning and always adjusting our approach as consumer choices, markets, services and products evolve'.

So perhaps in the spirit of this intention, the FCA will be open to changes and adaptions of the long-established lines of defence approach or even entirely new approaches that may emerge from modern and innovative firms being regulated for the first time. The adoption of new technology powered by robotics, machine learning, cognitive and predictive analytics, artificial intelligence, and other new supporting technologies will also play a role in adapting and upgrading the model as the importance of data as a strategic asset in the risk and control landscape is realised.

CONCLUSION

Despite the criticisms levelled at it, the three lines of defence model remains conceptually attractive, particularly in the absence of any real alternative approach. It can work if it is well defined, articulated and understood by all employees, effectively implemented and continuously monitored and, most importantly, underpinned by a strong and robust corporate culture. The right risk culture should encourage constructive challenge, ethical decision making, appropriate incentives, openness and transparency. Making sure the tone from the top, business risk appetite, performance management and compensation structures are aligned with company strategies is key.

The three lines of defence model has historically been designed and built around traditional divisional organisational structures or risk disciplines. Risk management and control functions need to continually adapt to changing regulatory requirements,

providing independent challenge, whilst also adopting a collaborative approach to deliver better business outcomes and avoid a 'them and us' divide. A genuinely collaborative, connected, risk-aware organisation is yet to be the norm. A refreshed model needs to focus on ensuring greater accountability of risk by the first line including risk culture while building better coordination within the second line and implementing new technologies to increase effectiveness. The IIAs proposals are catching up to some extent with practice (eg blurring of the lines) but also offer an opportunity to significantly enhance the risk and control environment within an organisation. The inclusion of the two principles relating to governance and the role of the governing body in overseeing the organisation's risk management and control framework and its accountability to stakeholders for ensuring that appropriate structures and processes are in place for effective governance should avert the shortcomings in poor risk management, governance and cultural failures, ineffective controls and unreliable data that are so often the contributing causes to corporate failures and regulatory breaches.

One should not ignore the role middle management have to play in a three lines of defence model either. An essay published by the FCA during 2018[24] notes '… a narrow aspect of ethical culture, but one that desperately needs more attention …' and highlights the importance of the role of the middle manager. The middle management is tasked with translating top management expectations into front-line employee behaviour. When we consider that people spend more time interacting with middle management than top management it is logical to assume that the success or failure of any operating model is almost entirely dependent on the observed behaviours of middle management. If the middle management want the three lines of defence model to work, it will. We get what we focus on, and we focus on what we are incentivised to do.

References

(1) Financial Services Authority, (2003), 'Building a Framework for Operational Risk Management: The FSA's Observations', available at https://www.handbook.fca.org.uk/archive/2003/08/PS142_2.pdf (accessed 23rd August, 2021).

(2) The Institute of Internal Auditors, (2013), 'The Three Lines of Defence 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 9th August, 2021).

(3) Adamson, C., (2014), 'Speech at the Association of Professional Compliance Consultants' annual conference', available at https://www.fca.org.uk/news/speeches/sustainable-conduct-environment (accessed 12th August, 2021).

(4) Basel Committee on Banking Supervision, (2015), 'Corporate governance principles for banks', available at https://www.bis.org/bcbs/publ/d328.pdf (accessed 27th August, 2021).

(5) The Office of the Comptroller of the Currency's, (OCC), Comptroller's Handbook booklet (2019), 'Corporate and Risk Governance', available at https://www.occ.gov/publications-and-resources/publications/comptrollers-handbook/files/corporate-risk-governance/pub-ch-corporate-risk.pdf (accessed 29th October, 2021).

(6) *Ibid*, ref. 2.

(7) Wyman, O., (2015), 'Whose Line Is It Anyway? Defending the Three Lines of Defence', available at https://www.oliverwyman.com/content/dam/oliver-wyman/global/en/2015/nov/Three_Lines_of_Defence.pdf (accessed 12th August, 2021).

(8) Senior Managers and Certification Regime (2021), available at https://www.fca.org.uk/firms/senior-managers-certification-regime (accessed 12th August, 2021).

(9) Basel Committee on Banking Supervision, (2014), 'Review of the Principles for the Sound Management of Operational Risk', available at https://www.bis.org/publ/bcbs292.pdf (accessed 26th August, 2021).

(10) The Association of Chartered Certified Accountants, (2019), 'Risk and Performance: Embedding Risk Management', available at https://www.accaglobal.com/gb/en/professional-insights/risk/risk-and-performance.html (accessed 26th August, 2021).

(11) *Ibid*, ref. 2.

(12) *Ibid*, ref. 2.

(13) Kelly, J., (2020) Wells Fargo Forced to Pay $3 Billion for the Bank's Fake Account Scandal,

available at https://www.forbes.com/sites/jackkelly/2020/02/24/wells-fargo-forced-to-pay-3-billion-for-the-banks-fake-account-scandal/ (accessed 21st February 2021).
(14) Independent Directors of the Board of Wells Fargo & Company, (2017), 'Sales Practices Investigation Report' available at https://www08.wellsfargomedia.com/assets/pdf/about/investor-relations/presentations/2017/board-report.pdf?%3ca%20href= (accessed 27th August, 2021).
(15) Compliance Week in partnership with Riskonnect, (2019), 'Risk Management Benchmark Survey', available at: https://riskonnect.com/content-library/survey-shows-gaps-in-integrated-risk-management/ (accessed 9th August, 2021).
(16) Armstrong, R., (2020) Citigroup fined $400m over internal controls 'deficiencies', available at https://www.ft.com/content/84c831fb-5088-41cd-bcb6-0f0daf968c43 (accessed 21st February 2021).
(17) Office of the Comptroller of the Currency, (2020), 'Consent Order #2020-056', available at https://www.occ.gov/static/enforcement-actions/ea2020-057.pdf (accessed 17th August, 2021).
(18) *Ibid*.
(19) *Ibid*, ref. 16.
(20) The Financial Stability Institute, (2015), 'Occasional Paper No 11, The four lines of defence model', available at https://www.bis.org/fsi/fsipapers11.pdf (accessed 26th August, 2021).
(21) BaFin, (2017), available at https://www.bafin.de/EN/Aufsicht/BankenFinanzdienstleister/Massnahmen/massnahmen_node_en.html (accessed 26th August, 2021).
(22) The Institute of Internal Auditors, (2020), 'An update of the Three Lines of Defense', available at https://na.theiia.org/about-ia/PublicDocuments/Three-Lines-Model-Updated.pdf (accessed 26th August, 2021).
(23) Nikhil Rathi, (2021), 'speech delivered at the Financial Conduct Authority's Our Role and Business Plan webinar', available at https://www.fca.org.uk/news/speeches/transforming-forward-looking-proactive-regulator (accessed 12th August, 2021).
(24) The Financial Conduct Authority, (2018), 'Discussion Paper (DP 18/2) – Transforming Culture in Financial Services - Essay 3.5 The invisible role of middle management – unethical behaviour and unrealistic expectations', available at https://www.fca.org.uk/publication/discussion/dp18-02.pdf (accessed 27th August, 2021).