Appendix 1

KIRKLEES COUNCIL
INTERNAL AUDIT
REPORT TO THE CORPORATE GOVERNANCE & AUDIT COMMITTEE

OBTAINING ASSURANCE.

1. **Summary**

This report sets out information about the theory of assurance, the ways in which it can be obtained, the current arrangements for gaining that assurance, and how these might be enhanced.

2. **Information and Theory**

2.1 The term "Assurance" is defined in the dictionary as
A positive declaration intended to give confidence, a promise
Certainty about something
A strong and definite statement that something will happen or that something is true

2.2 The Institute of Chartered Accountants considers that in the context of the commercial world assurance is so that
Owners, management, investors, governments, regulators and other stakeholders …. rely on the successful conduct of business activities, sound internal processes and the production of credible information

2.3 The councils Local Code of Corporate Governance does include reference to elements of business assurance in the context of accountability, internal control, risk management and audit, (appendix 1A) and whilst the role of the Corporate Governance & Audit Committee does not specifically include "assurance", it does include reference to the responsibilities for accounting, audit and corporate governance (appendix 1B).

2.4 An external audit and internal audit expectation have been long founded elements of local authority governance (much longer than some other parts of the public sector). The past emphasis of this work was on the accuracy of financial information, (External auditor), and the avoidance of error and fraud (Internal audit).

2.5 Through the wider remit of the Audit Commission there was greater consideration of elements of value for money and business strategy (although still a substantial interest in material accuracy of accounts) by the external auditor for 25 years from the 1980s- through to their abolition circa 10 years ago. The external auditors still certify a vfm statement- which has been enhanced somewhat in recent years- but concentrate on material accuracy of financial statements.

2.6 For internal auditors, the (international) Institute of Internal Auditors (IIA) has become more influential and has recommended that internal audit focus is shifted from detailed financial accuracy, error and fraud to a wider remit of assurance based around entity risk.

2.7 The logic of this is that a successful organisation needs to be sure that all its business arrangements perform effectively- whether they be financial or non-financial - because ultimately non-financial issues will tend to become financial.

2.8 This is easiest to understand in the context of a purely commercial business. For example, poor quality or unreliable products, will lead to customer

dissatisfaction and a loss of sales, potentially affecting the viability of the business. If selling something in fixed quantities- inaccurate under-weighing could lead to allegations of dishonesty and fines (and reputation); Over-weight product would be wasteful, and so equally affect profitability. Supply chain risk is often seen as a key risk in the private sector.

2.9 In the context of a public sector (statutory) service provider wider business assurance provides greater certainty that the organisation is fulfilling its statutory and chosen objectives. These are set down in various places but would include the Councils Corporate Plan. In the more detailed context, whilst fraud and error may be still seen as a concern, other issues create potential threats; Cyber security, and the disruption or destruction of information for international, political or other reasons rank as potential risk and threats that ostensibly are not directly financial but so severely affect the ability of an organisation to operate effectively that they create reputational damage, disruption (and if service provision is to be maintained probably higher cost). Cyber ransom has the same effects, potentially, but with a wider context of appropriateness.

2.10 It is notable that the IIA considers that most internal audit plans (in all sectors) over emphasise concerns about the risks of financial information (and thus financial statement error risk), and fraud, and underestimate the entity risk from aspects, such as supply chain, IT and cyber, staffing, legislative change, environmental and climate.

2.11 The emphasis of internal audit has thus moved to an extent to the wider understanding of the assurance processes the organisation has in place.

2.12 The IIA considers that an appropriate corporate structure to deliver this wider assurance understanding is the "Three Lines of Defence" Model. This considers internal assurance at three levels, direct operational control, oversight controls, and internal audit. Other defences exist through the external auditor and external regulators where applicable.

2.13 A description of the arrangement is included as Appendix 2. The chart below though summarises the model.

GOVERNING BODY/AUDIT COMMITTEE								
SENIOR MANAGEMENT								
1st line of defence		2nd line of defence		3rd line of defence			External Audit	Regulators
Management Controls		Financial controls		Internal Audit				
		Security						
Internal Controls		Risk management						
		Quality control						
		Inspection						
		Compliance						

2.14 The arrangement should emphasise the importance of management taking responsibility to deliver sound assurance but provides other ways for those charged with governance to understand organisational risk and quality.

2.15 This arrangement should work in any type of organisation- but see section 2.16 below. The arrangement though is not without risk, as analysis of problems in organisations (based on financial services c 15 years ago), identifies issues of management being driven by goals (and personal incentive), so ignoring assurance controls, a lack of independence of functions and skill in the second line of defence; and the failure by internal audit to identify high-risk areas or processes will lead to audits focussing on the wrong areas.

2.16 The model is stated as applicable to all types of business. Local authorities separate their service provision- much of which is free at the point of delivery, from the funding – much of which is statutory tax. The principles apply, but the non-monetary aspects of some activity mean that different assurance forms may sometimes be applicable. Regulatory intervention in local authority activity can also, in some respects take place at a more detailed level than would be typical of the private sector- examples being Ofsted, CQC. Ombudsman, Planning Inspectorate, Regulator of Social Housing. This regulatory involvement is often reactive or retrospective. In addition, the nature of the council acting in partnership with other parts of the public sector (sometimes as a regulator) also needs to be recognised.

2.17 Whilst all types of businesses use customer complaints as a way of understanding their client base, in the commercial sector unhappy customers often cease to be customers. For a local authority, customer complaint may be a more direct form of assurance, or lack thereof. Customer dissatisfaction may also be a route to regulatory intervention, routinely or otherwise. For example, applicants for planning permission do have the ability to appeal through the Planning Inspectorate. Many successful appeals may suggest a failure of process (and would come with some cost). Planning though is a one direction only appeal process; Persons unhappy that an application was granted do not have a routine ability to challenge the decision (though they have the theoretical right of injunction if legal or administrative processes were not correctly followed).

2.18 A further area of theory is that of “assurance maps”. In some respects, these are a tool to implement the 3 lines of defence model, as understanding what assurance already exists in an organisation is an important part of determining gaps and hence risks.

2.19 Assurance maps do not provide an answer, they are part of knowledge. At a high level, they are relatively easy to draw up and determine scope and issue. At a detail level though, like system, process and control maps, the complexity and costs of creation, analysis and regular updating (whenever a process or system is modified) may not justify the continuous support work, and it may be better to leave routine management assessment (defence 1), oversight (defence 2) or routine internal audit (defence 3), to identify and address any detailed control assurance issues.

2.20 Control risk self-assessment is a form of assurance used, sometimes, by auditors. The external auditor asks for certain statements from specific officers

and members about their satisfaction with arrangements. This can only though be a supplement to the need for the auditor to gain assurance on key risk areas themselves. Similarly, internal auditors, including in some local authorities, use this approach to seek an element of assurance about operational activities. This can include the seeking of an annual certification (say from directors) that all activity is subject to internal check or internal control, or it can go further to a diagnosis and training philosophy that looks to discuss an arrangement or process, identify risks, agree controls, and seek to get commitment from those operating the arrangement to execute the appropriate control arrangements.

2.21 Ideally maximum assurance is obtained by knowing as much about arrangements as possible. Risk management can be about knowing what is not known. But there are also unknown unknowns (as often attributed to Donald Rumsfeld, a past USA defence secretary, but having been referenced in historical texts). Assurance must be about knowing as much as reasonably practical, but it must be within the context of resource, skill, knowledge, and openness.

3. Applicability of Assurance for Kirklees Council, and Kirklees Corporate Governance & Audit Committee. What does this mean for our arrangements?

3.1 At the present we have an internal audit team that focuses on a combination of traditional financial risks, and some areas of high risk in other areas. This is based on an audit plan drawn up against a theoretical list of entity risks (sometimes called the “audit universe”). The work of internal audit is dealt with in detail by officers, with summary reports of outcomes being presented to this Committee in the Quarterly Report, and Annual Report.

3.2 We also have arrangements which bring some reports from other internal assurance functions to the Corporate Governance & Audit Committee and some regulatory reports, but not all. Some other Council Committees- such as Scrutiny, or Cabinet receive or review other assurance and regulatory reports.

3.3 Almost all council activities have administrative processes that have some degree of quality check or intervention, although at the lowest levels the amounts of checking may be minimal or may depend on a system or computer-based system restrictions. The amount of intervention tends to rise as officer-based decisions become more important. For example, delegated planning decisions, where supervisors would read and consider the analysis of each team members proposed determination. In care-based cases, detailed work is done by individuals, teams or specialists, with both direct staff supervision and panel-based case decisions.

3.4 Most corporate activity is controlled through specialist teams (Finance, IT, Legal, HR), although most other aspects of activity are controlled at a directorate or Service level. An ambitious investment programme has led to some implementation of more specialist project control and assessment for complex capital projects.

3.5 The assurance schedule (rather than a detailed “map”) can be considered to include the following, listed in the table below.

Appendix 1

A. Sources of Independent internal and external assurance (Third Defence [+}) & selected internal (Second Defence)

Source of assurance	Methodology	Scope	CGAC report	Internal or external
Internal Audit (Risk based plan)	individual project assessment	Routine financial. Some business processes. Some other areas	Yes Summary Quarterly/ Annual	Internal
Internal Audit Investigations	individual project assessment	Various (mainly financial/ governance) areas	Yes As arising	Internal
Customer Complaints	individual project assessment (& some advisory)	All areas, at third stage. Prepares cases for Ombudsman/ responds	Yes Twice per year	Internal
Health & Safety	Routine monitoring /advice and individual project assessment	All areas of health and safety Carries out some internal investigations into incidents and near misses. Assist HSE with external cases	Yes Twice per year	Internal
Information Governance	Routine monitoring /advice and individual project assessment	All areas of information governance. Both provider and oversee-er. Prepares cases for Information commissioner/ responds	Yes Twice per year	Internal
Grant Thornton (External Auditor)	Assessment of presented financial statements against required standards, vfm reporting	All financial information. Some supplementary/ related information. Assessment of quality of internal controls	Yes Once formally (Intermediate reporting)	External
Local Government Ombudsman	Individual project assessment (& some advisory)	Considers cases referred by customers/service users who are unhappy. Case reports. Annual report	Summary information reported as Customer Complaints (as above). Certain specific	External
Ofsted	Individual school performance. Performance of Childrens Services functions	All areas of school performance (except finance/admin) All areas of Childrens services performance	No Some reporting to Executive Team, Cabinet	External
CQC	Individual care provider performance.	All areas of provider performance	No Some reporting to Executive Team, Cabinet	External
Planning Inspectorate	Individual project assessment	Considers cases referred by applicants who are unhappy. Case reports. Annual report	No. Some reports to	External

Appendix 1

			Planning Committee	
Regulator of Social Housing	Social Housing (HRA) operational oversight	Activity areas- such as safety (Role and authority likely to be extended by legislation)	Case specific reporting to date	External
Peer Review (Occasional)	As commissioned, topics typically in scope are Governance and operating models	Understanding how the organisation identifies, relates, and functions as an effective democratic organisation	Case specific reporting to cabinet/ council	External

B Other sources of Potential Assurance

Source of assurance	Methodology	Scope	CGAC report	Internal or external
Budget Monitoring	Routine detailed comparison by Accountancy officers. Strategic analysis of position by Chief Financial Officer	All council budgets in scope; Regular monitoring of all variances, with frequent review of larger items which are seen as control risks	No But reported routinely to ET, Cabinet Scrutiny & Council	Internal
Legal & Governance	Routine consideration of all decision related material	All activities within scope. Includes advisory and legal completions (e.g., contracts, conveyances)	No	Internal
Contract Procedure Rules	Enforcement of significant procurements by Procurement Team	In theory, everything; low value items, grants and certain others can avoid the process	No (other than when in scope of IA)	Internal
Financial Procedure Rules	Mainly self-enforcement. SAP (and certain other systems enforce parts of obligations) Finance officers (Accountancy & IA)	In theory, everything. Some rules can be ignored	No (other than when in scope of IA)	Internal
HR	Compliance with legislation, Employee Handbook Achieving the People Strategy	Requirement to appoint only in accordance with approved structures, and grades. Some processes designed to achieve PS objective (e.g., re recruiting)	No	Internal
Payroll	Compliance with legislation, Employee Handbook	Employee payments controlled through SAP.	No	Internal
Information Technology	Largely integrated, consistently control systems within a virtual private network	All IT devices. All software. Controlled network. Automated- but as per criteria establishes by council	No	Automated
Information Technology	Consultants commissioned to	As determined by council or outside obligatory processes.	No	External

	advise of integrity and risk on systems and arrangements such as network security. Obligatory review requirement (e.g., for use of BACS)	Examples are general cyber security or specific cyber risks (E.g., extremist use of public IT)		(Occasionally internal)
General	Reviews of current activity. -compliance /assurance	As established by the review (e.g., building safety in public housing)	No	External
General	Reviews of current activity. -service, HR, objectives, change	As established by the review (e.g., SEND)	No	External (Occasionally internal)
Risk Management	Corporate collection of risk information to understand entity risk	In theory all activities and projects, but dependent on risk awareness and reporting. Limited corporate enforcement	Yes (annual) Quarterly to Executive Team and (informally) Cabinet, Scrutiny	internal
Performance Management	Activity metrics compared with targets, demonstrating trends and comparison and narratives	All activities theoretically within scope but dependent on information. Should be a key tool to focus on "important" activity, and linked with finance and risk information should demonstrate likelihood of success of organisation	Quarterly to Executive Team and (informally) Cabinet	Internal
Council Plan Monitoring	Review of progress to achieving the Council Plan	Detailed analysis of progress to specific objectives in Council Plan	ET, Cabinet	Internal
Project Management Office	Formal project management disciplines	Should provide structured approach to developing and progressing projects- see below		Internal
Gateway assessment	Formal assessment of significant capital project.	To achieve greater certainty & vfm on approved projects following HM Treasury & other guidance	ET. Cabinet	Internal
Annual Governance Statement monitoring	Review of progress to addressing issues in the Annual governance Statement	Detailed analysis of progress to specific objectives in Annual Governance Statement	Yes (though not done in 21/2)	internal
Reviews by Government or Funding Agencies	A closed set of objectives set by the Inspecting party. It may be linked to a statutory obligation, or grant	As established by the regime- e.g., Home Office review of Channel activity re extremism /terrorism	No	External

3.6 In addition, there is corporate assurance provided less formally by requiring other types of work and activity to be carried out only through in house specialists. This would include
- Building Services
- Property Services
- Transport Services

3.7 As note previously most service areas have at least elements of internal quality control and internal activity assessment.

3.8 As noted at 2.20 control risk self-certification requirements are used in some organisations, but they have not been used at Kirklees. The basic logic behind this is that as the organisation has an internal audit function, and that team ought to satisfy itself, on a priority basis, of the quality of any internal controls. It is noted that most internal auditors have a financial background, and so tend to be strong on reviewing financial compliance, and that others have knowledge of areas such as governance and procurement (that may be seen as areas of core risk). The use of generic auditing skills (the word auditing coming originally from Latin- *audite*) ought to be able to gain a level of assurance on any topic. Some by their nature may be complex (IT) or require a base knowledge of acceptable practice and practices (care). This thus routes back to the issue about the problem of using the third line of defence approach, although gaining assurance in any specialist area is always going to be difficult or complex, especially where the decisions are judgemental.

3.9 The objective of assurance arrangements is to understand the risk that the organisation will not achieve its overall objectives. Accordingly, it might be seen as good practice to work from these to identify if there are any assurance gaps.

3.10 A part of the obligatory governance processes is the production of an Annual Governance Statement (AGS); this is also a part of the assurance process; in that it is intended to schedule those areas where the organisation has identified potential concerns. The route to an AGS should be either identified failure, or gaps and uncertainty in assurance arrangements.

3.11 It will be noted that Risk Management arrangements are also a part of the assurance framework. Whilst at a strategic level the risk management process probably effectively identifies key areas of risk, the system may not be as effective in demonstrating potentially medium cost or medium service delivery impact (or high reputational impacts).

3.12 Good practice creates an internal audit plan in part from the risk information, and partly from an understanding of the quality of other forms of first line and second line of defence assurance arrangements.

4. Strategic, operational and broad assurance.

4.1 It is important to remember and acknowledge the different roles for various parts of the Council in relation to assurance, linked to their roles in the organisation

Council- setting the policy direction and budget of the Council
Cabinet- implementing the policies and budget of the Council
Officers- operationally fulfilling the decisions of Council and Cabinet

4.2 In this context, officers ought to have awareness of all assurance areas, and Cabinet ought to oversee the assurance of the achievement of policy, projects and finances at a strategic level.

4.3 To support this there are other oversight arrangements already in place; some are detailed, or activity specific, others are more general. In the most part they do not seek specific overall assurance, and activity is likely to be either specific or strategic.

Group	Role	Scope	CGAC report	Internal or external
Specific Boards	Established to provide assurance on specific aspects of council operations	e.g., Housing Assurance Board (a mix of tenants and specialist advisors to oversee housing HRA operations, particularly in the context of housing safety and advise Cabinet)	No	External mainly-internally supported
Scrutiny Committees	Although the objective of Scrutiny is to understand and assess policy initiatives, aspects of their work will provide assurance about activity	Some scrutiny will have, limited assurance content, but other work may involve assessment of the quality of decision making, or a review of (specific or generic) advice from regulators, or other third parties	No, but much activity is in the public domain and in minutes	Internal (External advice occasionally taken)
Cabinet (LMT) Assurance Board (new)	To provide assurance to cabinet at a strategic level of the areas of activity which are important and those which create potential risk	Still to be fully developed but will include Financial Performance Risk Management Projects	No	Internal

4.4 It is important that arrangements for assessment of assurance are not duplicated, but they are sufficiently holistic to cover all aspects of the organisation- without gaps.

4.5 An aspect of most local authority (and many other public organisations) that have had adverse reporting from external auditors, regulators or commissioners is that they often feature poor internal relationships, with dysfunctional officer management teams, poor relationships amongst corporate statutory officers, fixed mindsets, limited challenge amongst politicians and ineffective challenge of politicians by officers.

4.6 It is important that in constructing assurance arrangements, the Council does so in a way that achieves the entire entity assurance, creating positive relationships, and welcoming constructive challenge.

5. Adequacy of Assurance Arrangements.

5.1 The analysis above has provided the current arrangements for gaining assurance.

5.2 There are a lot of assurance structures, but there needs to be corporate thought about how these can be joined together, reflecting the responsibilities (at a political level) of the Council, Cabinet, Scrutiny and Corporate Governance & Audit Committee, and at an officer level of the statutory officers (Chief Executive, Chief Finance Officer and Monitoring Officer)

5.3 Aspects that need to be considered are

(a) How much assurance is appropriate?
(b) How should this be balanced between officers and members?
(c) How should this be balanced between Council, Cabinet, and the corporate Committees- Scrutiny and the Corporate Governance & Audit Committee?
(d) How do we achieve positive assurance on the entire entity?
(e) How do we achieve this without duplication?
(f) Are there any concerning gaps in assurance knowledge at present?

5.4 There needs to be a full understanding of the issue, prior to reaching a decision on the allocation of responsibilities.

5.5 When this understanding is more complete, it may be appropriate for the Council generally, or Corporate Governance & Audit Committee specifically, to assess if gaps in assurance knowledge are areas where Internal Audit should concentrate, or where specific advisory studies should be commissioned from others.

Martin Dearnley
Head of Risk (& Internal Audit)
April 2022

Appendix 1A.
Extract from Local Code of Corporate Governance

Good corporate governance is based on openness, inclusiveness, integrity and accountability and is demonstrated through the systems by which a local authority directs and controls its functions and relates to its communities.
It is about the leadership of communities and developing confidence, through the way that councillors and officers establish strategies, objectives and policies measure their achievement and operate the business of the council.
Delivering these objectives involves both community focus and service provision, in the context of establishing standards of conduct for those involved, business structures and processes and internal control and risk management. These standards are dealt with in more detail in the sections below.
In addition to the overarching requirements for acting in the public interest in principles …., achieving good governance also requires a commitment to and effective arrangements for:
F- Managing risks and performance through robust internal control and strong public financial management +Managing risk + Managing Performance + Managing Data + Robust Internal control + Strong Public Financial Management
G. Implementing good practices in transparency, reporting and audit to deliver effective accountability + Implementing good practice in transparency + Implementing good practices in reporting + Assurance and effective accountability
<u>Service Delivery Arrangements</u> Kirklees Council will monitor the implementation of its agreed policies and decisions and aim to achieve continuous improvement in the procurement and delivery of services by maintaining arrangements which: • Demonstrate accountability for service delivery. • Ensure effectiveness through measurement of performance. • Prioritise the use of resources. • Demonstrate integrity in its dealings with service users and partnerships to ensure the "right" provision of services locally. • Work with partners to specify, and monitor delivery of services which are effective. • Demonstrate openness and inclusiveness through its consultation with key stakeholders, including service users. • Are flexible and can be kept up to date, and adapted to accommodate change and meet user wishes. • Investigate any complaints fairly, and openly, and address any shortcomings.
<u>Internal Control and Risk Management</u> Kirklees Council will establish and maintain effective business control systems and an effective strategy, framework and processes for managing risk which: • Establish mechanisms to monitor and review effectiveness against agreed standards and targets and the operation of controls in practice through internal

control and internal audit.
• Include public statements on its risk management strategy, framework and processes to demonstrate accountability.
• Demonstrate integrity by being based on robust systems for identifying, profiling, controlling and monitoring all significant strategic and operational risks.
• Include mechanisms to ensure the risk management and control process is monitored for compliance and those changes are accommodated.
• Display openness and inclusiveness through the involvement of those associated with the planning and delivering of services, including partners.

Appendix 1B
Extract from Constitution Non-Executive Functions,
Corporate Governance & Audit Committee.

4. To consider the council's arrangement relating to accounts including
(a) the approval of the statement of accounts and any material amendments of the accounts recommended by the auditors
(b) to keep under review the council's financial and management accounts and financial information as it sees fit
5. To consider the council's arrangements relating to the external audit requirements including:
(a) the receipt of the external audit reports so as to.
(i) inform the operation of the council's current or future audit arrangements
(ii) provide a basis for gaining the necessary assurance regarding governance prior to the approval of the council's accounts
6. To consider the council's arrangements relating to internal audit requirements including:
(a) considering the Annual Internal Audit report, reviewing and making recommendations on issues contained therein
(b) monitoring the performance of internal audit
(c) agreeing and reviewing the nature and scope of the Annual Audit Plan
7. To review the adequacy of the council's Corporate Governance arrangements.
This will include (but not be limited to) the following:
7.1. Internal control and risk management.
7.2. Oversight of whistleblowing and the Council's whistleblowing policy.
7.3. Oversight of the complaints process and the role of the Local Government Ombudsman.
7.4. Oversight of Information Governance and the role of the ICO.
7.5. To review and approve the annual statement of Corporate Governance.
8. To agree and update regularly the council's Code of Corporate Governance, monitoring its operation and compliance with it, and using it as a benchmark against performance for the annual Statement of Corporate Governance.

APPENDIX 2
Three Lines of Defence
An Assurance Concept

1. **Key points:**

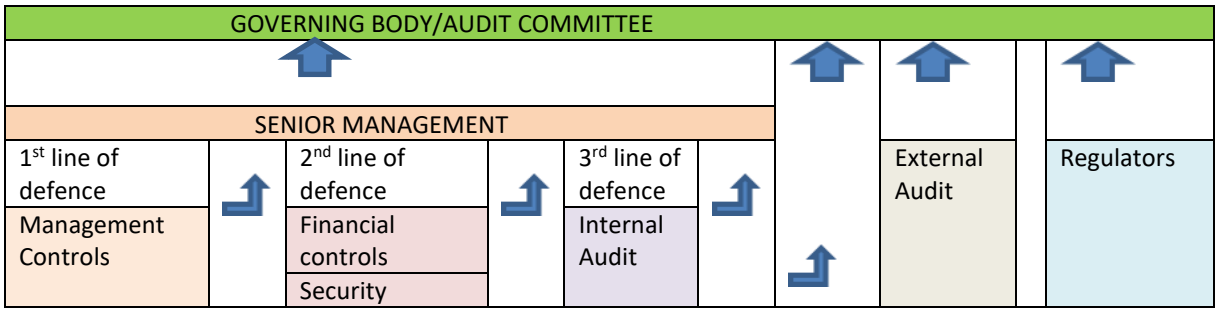
Guidance for Boards, Audit Committees, executive management and Internal Audit on establishing a Three Lines of Defence model for effective and efficient governance, risk management and control has been issued by the Institute of Internal Auditors (IIA).
The model is not simple to implement ideally requiring vision and ongoing support at Board level.
Significant benefit to all type and size of organisation can be achieved by implementing the model although common pitfalls should be considered

2. **The Three Lines of Defence model and the benefits and challenges of implementation.**

The Institute of Internal Auditors (IIA) published a global position paper in 2013, titled: *The Three Lines of Defense in Effective Risk Management and Control. (*Published in USA)
The concept has remained sufficiently important that a further position paper was published in June 2017 by the Chartered Institute of Internal Auditors, titled: The Three Lines of Defence, hereafter the 2017 paper.

The 2017 paper stated:
'*Applying the three lines of defence model in an organisation is not a silver bullet for achieving effective internal audit. Much also depends for example on the standing, scope and resourcing of the internal audit function. However, if the positioning and governance structure for internal audit are wrong, its ability to support the board or audit committee in their challenging of management can be fatally undermined'.*

What is the Three Lines of Defence model?
The IIA and the Institute of Directors endorse the 'Three Lines of Defence' model as a way of explaining the relationship between these functions and as a guide to how responsibilities should be divided:



Internal Controls		Risk management Quality control Inspection Compliance							

The three lines of defence

The first line of defence (functions that own and manage risks)
This is formed by managers and staff who are responsible for identifying and managing risk as part of their accountability for achieving objectives. Collectively, they should have the necessary knowledge, skills, information, and authority to operate the relevant policies and procedures of risk control. This requires an understanding of the company, its objectives, the environment in which it operates, and the risks it faces.

The second line of defence (functions that oversee or who specialise in compliance or the management of risk)
This provides the policies, frameworks, tools, techniques and support to enable risk and compliance to be managed in the first line, conducts monitoring to judge how effectively they are doing it and helps ensure consistency of definitions and measurement of risk.

The third line of defence (functions that provide independent assurance)
This is provided by internal audit. Sitting outside the risk management processes of the first two lines of defence, its main roles are to ensure that the first two lines are operating effectively and advise how they could be improved. Tasked by, and reporting to the board / audit committee, it provides an evaluation, through a risk-based approach, on the effectiveness of governance, risk management, and internal control to the organisation's governing body and senior management. It can also give assurance to sector regulators and external auditors that appropriate controls and processes are in place and are operating effectively. Is the model applicable to any organisation?
In short, yes.

The 2013 paper stated that the three lines of defence model is 'appropriate for any organisation – regardless of size or complexity. Even in organizations where a formal risk management framework or system does not exist, the Three Lines of Defence model can enhance clarity regarding risks and controls and help improve the effectiveness of risk management systems'.

The IIA position papers are part of their 'Strongly Recommended' category of guidance and compliance is not mandatory.

3. The key benefits of implementing an effective model

To implement an effective and efficient model across an organisation is not simple and requires vision and ongoing support from the Board and executive management in terms of direction and resources. The benefits are:

(a) Improved coverage of risks and controls by identifying and refining where necessary the population of risks and controls, and appropriately allocating the ownership and performance of these risks and controls across the lines of defence. Consequently, any unintended risks and gaps in controls may be avoided, and unnecessary duplication of work should be avoided by removing layers of redundant controls.
(b) Improved control culture across the organisation by enhancing the understanding of risks and controls. For example, potential conflicts of interest or incompatible responsibilities may be more readily identified and challenged with those risks then either removed or mitigated; and
(c) Improved reporting to the Board and executive management through a coordinated approach to providing timely and insightful reporting avoiding potentially duplicative and irrelevant information.

4. When implementation of the model fails

The Financial Stability Institute published Occasional Paper No 11 'The four lines of defence model' for financial institutions in December 2015. The paper included a root cause analysis of how the implementation of the lines of defence model arguably failed in practice during significant banking scandals with the following key findings:

(a) Misaligned incentives for risk-takers in the first line of defence – management may have put greater emphasis on and set compensation [or career progress] based on the achievement of financial objectives rather than control-orientated objectives.
(b) Lack of organisational independence of functions in second line of defence.
(c) Lack of skills and expertise in second line functions; and
(d) Inadequate and subjective risk assessment performed by internal audit. Failure by Internal Audit to identify high-risk areas or processes will lead to audits focussing on the wrong areas therefore undermining the effectiveness of the third line of defence.

Extract from an article by Steve Bruce CA 6 November 2017, ICAS website