Chartered Institute of Internal Auditors

Tuesday 12 September 2023

David Styles
Director, Corporate Governance and Stewardship
Financial Reporting Council
8th Floor, 125 London Wall
London
EC2Y 5AS

Submitted via email to: codereview@frc.org.uk

Dear David,

Revised UK Corporate Governance Code: consultation response

The Chartered Institute of Internal Auditors (Chartered IIA) welcomes the opportunity to contribute our consolidated views to the Financial Reporting Council (FRC) consultation on the UK Corporate Governance Code.

The Chartered IIA UK and Ireland represents approximately 10,000 internal audit professionals in organisations spanning all sectors of the economy. We are the only professional body dedicated exclusively to training, supporting, and representing internal auditors in the UK and Ireland. Having been awarded our Royal Charter in 2010, over 2000 of our members are now Chartered Internal Auditors and have earned the designation CMIIA. About 1000 of our members hold the position of head of internal audit and the majority of FTSE 100 companies are represented among our membership. We are proud to champion the contribution internal audit makes to good corporate governance, strong risk management and a rigorous internal control environment leading to the long-term success of organisations.

Overall comments

Broadly speaking we welcome the proposed revisions to the UK Corporate Governance Code. We are pleased to see the spotlight on internal control, assurance and resilience and these issues finally getting the attention they deserve. We support the increased focus and strengthening of the principles and provisions on audit, risk and internal control and the ambition to deliver a more robust risk management and internal control framework and the associated systems. This includes supporting the plans for a declaration by the board that the company's risk management and internal control systems have been effective. We are pleased to see that this declaration will go beyond just the material controls related to financial reporting and encompass a broader range of compliance and operational controls related to the material risks of the business.

An internal audit function is a critical element of good corporate governance, being the only independent and objective provider of internal assurance to the board. This means there is a key role for internal audit in supporting the internal controls declaration by providing the board with the additional independent assurance that the internal controls and risk management systems (and the material controls they encompass) have operated effectively. In the associated Code guidance, we would like to see the role that internal audit can play here appropriately recognised. Assurance over the internal controls declaration does not necessarily need to be performed externally, especially where companies have a strong, competently, and adequately resourced internal audit function. For many companies, it will be entirely appropriate for the board to leverage internal assurance and not external assurance. As envisaged in the original White Paper proposal, if material control weaknesses have been reported for two consecutive reporting cycles, then that should trigger external assurance. However, external assurance should not be viewed as the default option.

Chartered Institute of Internal Auditors

We also support the increased focus and strengthening of the Code regarding the responsibilities of the board in relation to corporate culture, diversity and inclusion, as well as climate transition and planning. Similarly, there is a key role for internal audit in providing independent assurance to the board on these matters. Furthermore, we are pleased to see that the updated Code reflects the new reporting requirements due to become law, including the requirement for larger companies to publish an Audit and Assurance Policy and a Resilience Statement.

However, there remains a need for the Code to be explicit, not just implicit, on the need for internal audit. Strengthening the wording by making it crystal clear that the board/audit committee should establish and maintain an internal audit function in accordance with internationally recognised professional standards, would go hand in hand with the need for a more robust risk management and internal controls framework. Prudent and effective risk management and internal controls require strong internal audit functions. While there may not be many publicly listed companies that do not have internal audit capability, this is also about sending a clear message to the market and investors that the presence of internal audit is a critical element of good corporate governance. This change would also bring the UK in line with many of our international peers and help to further enhance the UK's reputation for good corporate governance and a safe place to invest. Being mindful that any change to the wording would still be complied with using a comply or explain approach, and therefore offers flexibility.

We have chosen not to respond to every question, but exclusively to those in which we can offer our expertise, insight, and a valuable contribution. As well as focus our response on the areas of the Code that most relate to and have an impact on the internal audit profession.

The Chartered IIA is happy to discuss any of the comments included in the response. We are also happy for our response to be published and made publicly available on the FRC website.

Yours sincerely,

Chartered Institute of Internal Auditors

Revised UK Corporate Governance Code: Consultation response

1. ESG Reporting (questions covering environmental sustainability, corporate culture, diversity and inclusion, division of responsibilities and board performance)

Q2: Do you think the board should report on the company's climate ambitions and transition planning, in the context of its strategy, as well as the surrounding governance?

We support the strengthening of the Code regarding company directors' responsibilities for reporting on climate ambitions and transition planning, in the context of its strategy, as well as the surrounding governance.

In addition to this, we support the strengthening of the Code regarding company directors' responsibilities for the corporate culture, including responsibility for monitoring and assessing the corporate culture, as well as how effectively it has been embedded. In a survey of over one hundred senior internal audit executives as part of the research that supported our 'Cultivating a healthy culture' report published in March 2022, two-thirds of those surveyed supported strengthening the Code regarding the responsibility of the board to promote, monitor, and assess the desired corporate culture, and only 10% were against.

The FRC's own report 'Creating Positive Culture' and the Chartered IIA's report 'Cultivating a healthy culture' also clearly demonstrate that corporate culture can be monitored, assessed and measured, and we stand ready to continue to collaborate with the FRC on this important issue. Not least given that the root cause of many recent corporate collapses can all be linked back to a poor, weak, or unhealthy culture emanating from the wrong tone at the top.

Q6: Do you consider that the proposals outlined effectively strengthen and support existing regulations in this area, without introducing duplication?

By and large, the proposals do strengthen and support existing regulations and standards in this area, without duplication. The wording is complementary to and reinforces regulations and standards in this area, without being unduly repetitive and ensuring a joined-up approach. However, in the interests of strengthening and supporting existing regulations and for greater clarity, we are recommending that Principle I be amended to more closely align with the protected characteristics specified in the Equality Act 2010 (see below).

Q7: Do you support the changes to Principle I moving away from a list of diversity characteristics to the proposed approach which aims to capture wider characteristics of diversity?

While there are clearly good intentions behind this proposed change by attempting to encompass wider characteristics of diversity, we believe in the interests of being consistent with relevant regulation and legislation there would be merit in also including a list of legally recognised protected characteristics. This would ensure that the Code wording is consistent with the Equality Act 2010, the specific protected characteristics of which include: age, disability, gender reassignment, marriage and civil partnership, pregnancy and maternity, race, religion and belief, sex and sexual orientation. This would provide greater clarity as to what exactly is meant and ensure the terms are clearly defined in the Code. We would suggest changing the wording in Principle I of the Code to the following:

I. Appointments to the board should be subject to a formal, rigorous and transparent procedure, and an effective succession plan for the board and senior management should be maintained. Both appointments and succession plans should be based on merit and objective criteria. They should

Chartered Institute of Internal Auditors

promote equal opportunity, and diversity and inclusion of protected characteristics (including age, disability, gender reassignment, marriage and civil partnership, pregnancy and maternity, race, religion and belief, sex and sexual orientation) and non-protected characteristics (including cognitive and personal strengths).

Q9. Do you support the proposed adoption of the CGI recommendations as set out above, and are there particular areas you would like to see covered in guidance in addition to those set out by CGI?

We support the proposed adoption of the Chartered Governance Institute recommendations as part of the Government commissioned review of the effectiveness of independent board evaluation in the UK listed sector.

In addition to this, in section 2 of the Code on division of responsibilities, we would also support the Chartered Governance Institute's recommendation to strengthen provision 16 to make clear that the Company Secretary should have a primary reporting line to the Chair of the Board. Similarly, for internal audit, the Chartered IIA recommends that the Chief Audit Executive should have a primary reporting line to the Audit Committee Chair, and a secondary or administrative reporting line to the Chief Executive (or someone who protects internal audit's independent and objective voice). So, it makes sense for there to be similar board-level reporting line arrangements in place for the Company Secretary.

Q12: Do you agree that the remit of audit committees should be expanded to include narrative reporting, including sustainability reporting, and where appropriate ESG metrics, where such matters are not reserved for the board?

We do support widening the remit of audit committees to include narrative reporting, including sustainability reporting and where appropriate ESG metrics where such matters are not reserved for the board. As reporting on ESG matters is becoming increasingly important in decisions by investors we believe this to be an appropriate role for audit committees and draws on their relevant skills and experience. For example, audit committees are familiar with reviewing and challenging disclosures as well as narrative content in the annual report and accounts. Based on our engagement and consultation with our members, including Chief Audit Executives of publicly listed companies, we would observe that it is already common practice for audit committees to engage in the outcomes of ESG-related matters and audits. This is especially true since the introduction of mandatory climate-related financial reporting in line with the TCFD framework that became a regulatory requirement for larger companies in April 2022.

Some stakeholders have raised concerns about the unintended consequence of overloading the audit committee, which could then divert the audit committee's time and resources away from focusing on the financial and risk aspects of the business. However, this can be addressed by focusing audit committees on the assurance of narrative and sustainability reporting where there is a material risk to the business. For example, assuring ESG metrics where there could be a material risk exposure linked to greenwashing or inaccurate data. This is an area that would benefit from specific guidance on what narrative reporting should be within the scope of the audit committee. Concerns have also been raised about the issue of duplication. For example, the potential for the audit committee to duplicate the work of the risk committee, or where there is one the sustainability committee. Widening the remit of the audit committee will therefore require even closer coordination, communication, and delegation of work by the board and its sub-committees to ensure such duplication is avoided.

Widening the remit of audit committees also brings into question the capabilities, knowledge, and skills required of committee members. There is currently a requirement for committee members to be

financially qualified. Going forward audit committees will also need members with appropriate experience in non-financial processes, controls, and reporting, as well as in assurance that is broader than just external audit, meaning that the composition of Audit Committees may need to change under a widened remit. Those with experience working in senior internal audit roles are well placed in this enhanced role. The internal audit profession can help provide a pipeline of new audit committee talent, with the capabilities, knowledge and skills that are now required.

Furthermore, the ongoing focus by regulators, investors, and the public on ESG matters means that audit plans are likely to already encompass ESG-related assurance. Indeed, internal audit functions are already routinely engaged in supporting the audit committee's work in this area, including supporting ESG-related assurance and governance. This includes engaging closely with the business on its ESG strategy and commitments. Examples of key internal audit assurance and advisory activities on ESG include:

- Supporting the business's understanding and knowledge of the ESG regulatory landscape and assessing the applicability of regulations to the operating environment.
- Assessing and monitoring ESG-related goals and targets.
- Providing assurance on risk management, internal controls and governance around narrative and sustainability reporting. Including making sure that all mandatory and optional internal and external reporting processes (and the data that supports them) are in place and operating effectively to ensure ESG metrics are calculated correctly and on time.

We would like the role of internal audit in supporting the audit committee on the assurance and governance of narrative reporting, sustainability and other ESG matters to be reflected in the associated Code guidance.

2. Audit and Assurance Policy

Q10: Do you agree that all Code companies should prepare an Audit and Assurance Policy, on a 'comply or explain' basis?

We agree that all Code companies should be expected to prepare an Audit and Assurance Policy on a 'comply or explain' basis. While the new legislative reporting requirement for companies to produce an Audit and Assurance Policy is only intended to apply to both private and public companies with at least 750 employees and a turnover of £750m or more, it should be viewed as good practice for all publicly listed companies to have one. This will help to support high-quality and comparable reporting across all publicly listed companies for investors and stakeholders, while still giving smaller publicly listed companies the option of choosing to explain why they have not produced one – therefore providing flexibility. However, given the growth trajectory of most publicly traded companies and their overall importance to investors and the economy, we don't see why any publicly listed company would not want to produce an Audit and Assurance Policy; it should be viewed as essential for good governance.

We also support the audit committee being responsible for developing the Audit and Assurance Policy and welcome this being made clear in the revised Code. In the associated Code guidance, the audit committee should be made aware that they can seek support from their internal audit functions to act as the facilitators and coordinators of the drafting of the policy. Internal audit will be able to work on this in collaboration with other key business functions such as finance, legal and risk management. This is because internal audit's unique position in the business means it has a 'helicopter view' of the entire audit, risk, and assurance landscape, helping to weave the policy together by working closely with other assurance providers. We look forward to further engaging on this in more detail as part of the forthcoming public consultation on the Audit and Assurance Policy guidance.

Chartered Institute of Internal Auditors

3. Audit, Risk and Internal Control

Q13: Do you agree that the proposed amendments to the Code strike the right balance in terms of strengthening risk management and internal controls systems in a proportionate way?

Broadly speaking we agree that the proposed amendments to the Code do strike the right balance in terms of strengthening risk management and internal controls systems in a proportionate way. The Code remains principles-based, enabling companies to meet the requirements according to their size, complexity, and risk profile.

We support the introduction of the internal controls declaration and are pleased that this goes beyond the material controls related to financial reporting and encompasses other operational, reporting and compliance controls of material concern. This reflects a trend of companies facing material risk exposures in other (non-financial) operational, reporting and compliance areas.

Based on our engagement and consultation with members and stakeholders, including the Chief Audit Executives of publicly listed companies, some have expressed concerns about the need for the Code to emphasise and be clearer on the importance of materiality in relation to the scope of the internal controls declaration. Some have even suggested it might be helpful to provide some parameters around this by including examples of the core areas and types of material controls one might expect to see included as part of the declaration e.g. IT and cybersecurity controls. The importance of including IT and cybersecurity risk and mitigating controls as part of the internal controls declaration was a key theme in the consultation with our members.

However, it could be challenging to provide a list of material controls that apply to all companies, as all companies have different risk profiles, and therefore the material and non-material controls can differ greatly. We suggest that underlining and emphasising in the Code that it is the material operational, reporting and compliance controls deployed to mitigate material risk exposures may be the most pragmatic way of addressing this. As things stand there are concerns that the current wording could lead to a disproportionate response by companies, which in turn could lead to a disproportionate compliance burden. Greater clarity is therefore required to emphasise materiality and make clear that not all operational, reporting and compliance controls are expected to be within the scope of the declaration.

While the Financial Reporting Council has tried in all its communications to make expectations clear and clarify that this is not ‘SOX-lite’ being delivered through the backdoor, there is still a concern amongst many stakeholders that it is. Linked to this, there is a concern that external assurance will be either preferred or required over the internal controls declaration for the board to get the level of assurance they need to sign off on it. In many cases seeking internal assurance over the internal controls declaration should be entirely sufficient and appropriate, particularly where strong, competently, and adequately resourced internal audit functions are present. As set out in the original White Paper proposal, if material control weaknesses have been identified and reported for two reporting cycles, then that should trigger external assurance. But in most instances seeking internal assurance, especially from internal audit should be sufficient.

The boards/audit committees of publicly listed firms should be encouraged to engage internal audit and other internal assurance providers in providing additional assurance over the internal controls declaration. Indeed, many internal audit functions are already engaged in providing reasonable assurance of the effectiveness of the internal controls and risk management systems. This can include providing an annual Internal Control Report to provide the board with an overarching view of how the Three Lines of Assurance have operated the material controls including associated evidence.

The work also involves evaluating and assessing the processes undertaken by the first and second lines. This supports the board in carrying out its annual review of the effectiveness of the internal controls and risk management systems. So, in many respects internal audit is already doing significant work in this area, which in turn can help support the board's internal controls declaration.

However, it would be counterproductive for all the additional work associated with producing the internal controls declaration, to sit entirely with the internal audit function. This often happened in the USA after Sarbanes Oxley was introduced, with the resulting unintended consequence that this diverted internal audit time and resources away from auditing new and emerging risk areas, to having to spend significantly more time and work on the internal controls and risk management systems, along with the associated attestation. Roles and responsibilities regarding the internal controls declaration need to be made crystal clear. Internal audit does have an important role to play – but it is there to independently review and provide assurance on the effectiveness of the internal controls and risk management systems and should not own or be responsible for the entirety of the process. This additional work for internal audit functions should not result in entire audit plans being shifted to devote significant time and resources in this area, assurance on other risk areas is still vital. As per the Chartered IIA's internal audit codes of practice, the audit committee has a responsibility to ensure that the internal audit function has sufficient resources to carry out all its work. So, if internal audit needs more resources to carry out this additional work this should be provided.

To address these concerns the roles and responsibilities for developing and supporting the Internal Controls Declaration should be set out clearly in the associated guidance. Including in relation to testing and retesting the controls, as well as the role of internal audit as an independent assurance provider.

Q14: Should the board's declaration be based on continuous monitoring throughout the reporting period up to the date of the annual report, or should it be based on the date of the balance sheet?

The board's declaration should reference that the controls have worked throughout the year not just at one point in time. This underlines the essential role of independent assurance throughout the year - not just an annual opinion, this should also link back to the Audit and Assurance Policy.

It would be optimal for the declaration to be based on continuous monitoring throughout the reporting period, but not on controls having always worked throughout the year. It is important to have a mechanism that provides the capability to detect any weaknesses that emerge swiftly and to remediate or put in place compensating control activities at pace. This capability is vital to prevent a weakness that can be easily fixed, escalating into a more serious issue and then becoming a material weakness that is a threat to the business and needs to be reported. It is not good enough to have a control failure arise and then go unreported for several months. So, continuous monitoring on a frequency that is appropriate to the risk, is key to preventing and detecting material control weaknesses.

Q15: Where controls are referenced in the Code, should 'financial' be changed to 'reporting' to capture controls on narrative as well as financial reporting, or should reporting be limited to controls over financial reporting?

We support controls referenced in the Code being changed from 'financial' to 'reporting' to capture controls on narrative as well as financial reporting. This is entirely consistent with other changes in the revised Code, including the internal controls declaration covering financial and non-financial material controls, as well as the widened remit for the audit committee to cover narrative and sustainability reporting. With the expansion of the Code to include an additional focus on narrative controls,

changing the wording to ‘reporting’ controls is appropriate, ensuring consistency and a joined-up approach.

Q16: To what extent should the guidance set out examples of methodologies or frameworks for the review of the effectiveness of risk management and internal controls systems?

The Code guidance could include good practice examples but not stipulate methodologies or frameworks for the review of the effectiveness of risk management and internal controls systems. This would provide a suitable level of guidance but allow flexibility for an organisation to define and develop its own methodologies or frameworks based on its specific circumstances if required. Such guidance will also help support high-quality and comparable reporting.

One of the most effective models and frameworks used to support effective risk management and internal controls systems is the ‘Three Lines Model’ advocated by the Chartered IIA and our partners. The model was first introduced in 2013 as the ‘Three Lines of Defence Model’ and has been widely adopted by organisations globally since then and is commonly used by UK publicly listed companies. It was recently updated as the ‘Three Lines Model’ in 2020.

Under this model internal audit is shown as the Third Line, providing comprehensive assurance on the effectiveness of internal controls, governance and risk management, with a primary reporting line to the governing body/audit committee. Whereas management and risk management are shown as the First and Second Lines.

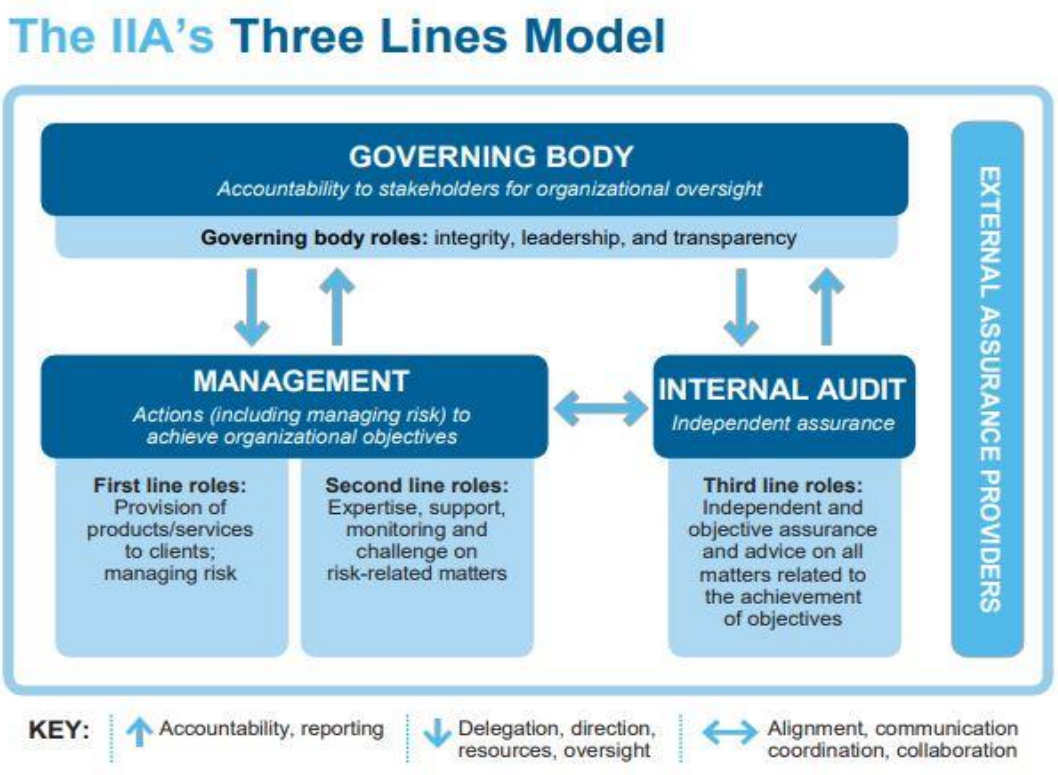
The ‘Three Lines Model’ is designed to show how organisations can mitigate risk and ensure accountability through effective oversight and governance. This model is used to clarify specific roles and responsibilities among an organisation’s leadership to promote strategic and operational alignment, oversight, and independence of the internal audit function.

Governing Body (or Board): Responsible for the strategic direction of the organisation. They maintain accountability of management activities, including compliance with legal, regulatory, and ethical expectations.

Management (First and Second Line Roles): Leads the daily execution of objectives set by the governing body. They establish and maintain appropriate structures and processes for the management of operations and risk.

Internal Audit (Third Line Roles): Maintains accountability to the governing body and independent from management. Works in partnership with management to promote improvement and achievements of organisations objectives.

Chartered Institute of Internal Auditors



We believe there would be significant value in referencing the Three Lines Model in the Code guidance.

Other frameworks that could be used to specifically review or report on the effectiveness of internal controls include COSO or Criteria of Control (COCO).

Q17: Do you have any proposals regarding the definitional issues, e.g. what constitutes an effective risk management and internal controls system or a material weakness?

Broadly speaking we agree with the current definition of what constitutes an effective risk management and internal control framework, and what is considered a material weakness as set out in the existing Code guidance and believe this to be sufficient. However, we question the appropriateness of including the words "or monitor risks". After deleting these words the current definition would then read as follows:

"A fault, deficiency or failure in the design or operation of the risk management and internal control framework, such that there is a reasonable possibility that the company's ability to identify, assess, or respond to its strategic, operational, reporting and compliance objectives is adversely affected."

Our rationale is that monitoring is key in both preventing and identifying a material weakness and so does not sit well in the sentence. In this context, it is worth noting that the Public Company Accounting Oversight Board (PCAOB) makes no mention of the word "monitor".

If the FRC were minded to include some additional narrative in the Code guidance on the definition of a material control weakness specifically, we note that the PCAOB states:

"A material weakness is a deficiency, or a combination of deficiencies, in internal control over financial reporting, such that there is a reasonable possibility that a material misstatement of the company's annual or interim financial statements will not be prevented or detected on a timely basis.

If this wording was adopted in the Code guidance it could be amended, to cover both financial and non-financial reporting, to be consistent with and reflect the revisions to the Code to also cover narrative as well as financial reporting. We suggest it could be amended along the lines of:

"A material weakness is a deficiency, or a combination of deficiencies, in internal control over reporting, such that there is a reasonable possibility that a material misstatement in the company's annual report and accounts, including in relation to the accurate reporting of its principal risks, will not be prevented or detected on a timely basis."

Q18: Are there any other areas in relation to risk management and internal controls which you would like to see covered in guidance?

We have included several suggestions in our responses to the questions above on areas in relation to risk management and internal controls that we would like to see covered in the Code guidance.

In addition to these suggestions, we would further comment that in the current guidance on Risk Management, Internal Control and Related Financial and Business Reporting 'internal audit' is only referenced twice. This is surprising given the key role that internal audit plays in providing independent assurance on the effectiveness of the risk management and internal control framework and systems within publicly listed companies. The important role of internal audit needs to be better recognised and reflected in the associated guidance, especially in terms of ensuring a joined-up approach. We are happy to continue working closely with Maureen Beresford and Tedi Jorgi on the redrafting of the Code guidance on risk management and internal controls to ensure that the important role of internal audit is reflected appropriately and accurately.

We would also like to use this opportunity to bring to your attention an error in the Code guidance on audit committees. In paragraph 56 it states:

"56. If the external auditor is being considered to undertake aspects of the internal audit function, the audit committee should consider the effect this may have on the effectiveness of the company's overall arrangements for internal control, the effect on the objectivity and independence of the external auditor and the internal audit function and investor perceptions in this regard."

This paragraph is inconsistent with The Statutory Auditors and Third Country Auditors Regulations 2016 which prohibits an external auditor who is providing the statutory audit to a company, to also provide internal audit services. Providing internal audit services, when you are providing statutory external audit services is strictly not permitted in the list of prohibited non-audit services. It is concerning that the Code guidance has not been updated since April 2016 to reflect this. The Financial Reporting Council should be updating its guidance regularly to reflect current legislation, to maintain high regulatory standards.

Finally, throughout the wording of all Code guidance, to provide greater clarity for stakeholders, it would be beneficial if the guidance could wherever appropriate explicitly differentiate and refer to either internal audit/internal auditor or external audit/external auditor. At present throughout the Code guidance, there are several instances where the wording only refers to "audit" or "auditor". This small change will help educate and enhance the understanding of stakeholders on the different and distinct roles of internal audit and external audit.

Chartered Institute of Internal Auditors

4. Provisions 26 and 27: Requirements for publicly listed companies to have an internal audit function

It is disappointing that the provisions in the Code on the need for publicly listed companies to have an internal audit function remain unchanged, with the provisions remaining implicit not explicit that the board/audit committee is responsible for establishing and maintaining an internal audit function. There would be great benefit in making the Code more explicit and clearer on this, which would go hand in hand with the increased focus on ensuring a robust internal control and risk management framework, as well as greater alignment with the requirement for companies to publish an Audit and Assurance Policy. Prudent and effective risk management and internal controls require there to be a strong, competently, and adequately resourced internal audit function.

The Code wording would benefit from aligning more closely with the PRA and FCA requirements for regulated financial services companies, as well as the wording of a significant number of our international peers' corporate governance codes. These all make it explicitly clear that companies should have an internal audit function.

For example, the FCA systems and control handbook states:

"SYSC 6.2 Internal audit

SYSC 6.2.1R01/07/2011

A common platform firm and a management company must, where appropriate and proportionate in view of the nature, scale and complexity of its business and the nature and range of its financial services and activities, undertaken in the course of that business, establish and maintain an internal audit function which is separate and independent from the other functions and activities of the firm and which has the following responsibilities:

(1) to establish, implement and maintain an audit plan to examine and evaluate the adequacy and effectiveness of the firm's systems, internal control mechanisms and arrangements;

(2) to issue recommendations based on the result of work carried out in accordance with (1);

(3) to verify compliance with those recommendations;

(4) to report in relation to internal audit matters in accordance with SYSC 4.3.2 R."

The latest version of the Swiss Corporate Governance Code states:

"31. The internal audit assesses the effectiveness of the internal control system.

– The board of directors should set up an internal audit and, in doing so, be guided by recognised professional standards.

– The internal audit should make an autonomous and independent assessment of the effectiveness of the controls set up by the board of directors and the executive board and of the internal control system.

– The internal audit should be in direct communication with the executive board and the board of directors. It makes reports to the executive board and the board of directors or the audit committee.

– Internal audit should have unrestricted access to all areas and information of the company. Internal audit and the external auditor should coordinate with each other in an appropriate manner."

The International Corporate Governance Network's global governance principles state:

"8.1 Internal audit
The board should oversee the establishment and maintenance of an effective system of internal control to properly manage risk which should be measured against internationally accepted standards of internal audit and tested annually for its adequacy. Companies should have a dedicated internal audit function with clearly defined oversight and reporting structures. Where such a function has not been established, full reasons for this should be disclosed in the annual report, as well as an explanation of how adequate assurance of the effectiveness of the system of internal controls has been obtained."

The newly published version of the G20/OECD Principles for Corporate Governance states:

"V.D.8. Ensuring the integrity of the corporation's accounting and reporting systems for disclosure, including the independent external audit, and that appropriate control systems are in place, in compliance with the law and relevant standards.

The board should demonstrate a leadership role to ensure that an effective means of risk oversight is in place. Ensuring the integrity of the essential reporting and monitoring systems will require that the board sets and enforces clear lines of responsibility and accountability throughout the organisation. The board will also need to ensure that there is appropriate oversight by senior management.

Normally, this includes the establishment of an internal audit function. This function can play a critical role in providing ongoing support to the audit committee of the board or an equivalent body of its comprehensive oversight of the internal controls and operations of the company. The role and functions of internal audit vary across jurisdictions, but they can include assessment and evaluation of governance, risk management, and internal control processes. It is considered good practice for the internal auditors to report to an independent audit committee of the board or an equivalent body which is also responsible for managing the relationship with the external auditor, thereby allowing a co-ordinated response by the board. Both internal and external audit functions should be clearly articulated so that the board can maximise the quality of assurance it receives. It should also be regarded as good practice for the audit committee, or equivalent body, to review and report to the board the most critical policies which are the basis for financial and other corporate reports. However, the board should retain final responsibility for oversight of the company's risk management system and for ensuring the integrity of the reporting systems. Some jurisdictions have provided for the chair of the board to report on the internal control process. Companies with large or complex risks (financial and non-financial), including company groups, should consider introducing similar reporting systems, including direct reporting to the board, with regard to group-wide risk management and oversight of controls."

These examples are all far more explicit and clearer on the responsibility of the board/audit committee for establishing and maintaining an internal audit function, and the function's role in supporting an effective system of risk management and internal control.

Based on Chartered IIA research conducted in July/August 2023 that examined the corporate governance codes and listing requirements of 46 European Union and G20 countries (along with several additional countries that are regarded as global financial hubs) 53% had an explicit requirement for their publicly traded companies to establish an internal audit function and a further 38% had an implicit requirement. Now is the time for the UK Corporate Governance Code to be updated to align with most of our international peers. The UK needs to maintain its enviable global reputation for good corporate governance underpinned by the presence of strong, competently, and adequately resourced internal audit functions.

Chartered Institute of Internal Auditors

To address this issue, we propose the following change to provision 26 (bullet point 9) of the Code on the main roles and responsibilities of the audit committee:

26. The main roles and responsibilities of the audit committee should include:

• *Establishing and maintaining an internal audit function in accordance with recognised professional standards and Codes of Practice, including ensuring that internal audit has unrestricted access to all areas and information of the company, as well as monitoring and reviewing the independence, objectivity and effectiveness of the function. Or, where there is not an internal audit function, considering annually whether there is a need for one and making a recommendation to the board;*

A small amendment to the current wording would provide greater clarity and make crystal clear that the presence of internal audit is viewed as a critical component of good corporate governance, while at the same time maintaining flexibility for publicly listed companies to explain why they don't comply/do not have one.

We would also like to propose a further small change to provision 27 (bullet point 10) on the work of the audit committee in the annual report:

27. The annual report should describe the work of the audit committee, including:

• *a summary of the main activities of the internal audit function, or where there is not a function, an explanation for the absence, how internal assurance is achieved, and how this affects the work of external audit; and*

While it is relatively common to find some narrative on the work of internal audit in audit committee reports in the Annual Report and Accounts of publicly listed companies, it is not uncommon to find no dedicated summary of the main activities or internal assurance work carried out by internal audit. In the interest of good corporate governance, publicly listed companies should be encouraged in the Code to provide some narrative on the key activities and programme of work carried out by their internal audit function in their Annual Report and Accounts. This also reflects and reinforces the proposed change to provision 26.