ISACA Response
FRC Corporate Governance Code Consultation

About ISACA

ISACA is an independent, non-for-profit, global professional association, engaging in digital trust and the development, adoption and use of globally accepted, industry-leading knowledge and practices for the effective and safe, business and personal use of technology. ISACA has been established in the UK for over 35 years with over 140,000 professional members worldwide in over 180 countries.

We have deep experience advising on technology auditing, transparency and regulatory oversight regimes in the UK private and public sectors, and we hope we can contribute to the ongoing development of reforms to the UK's Corporate Governance Code, outlined here. In recent years, ISACA has worked with HM Government (including the FRC, BEIS (now-DBT), DCMS (now-DSIT), NCSC, ICO, and the CDEI on cyber security skills and workforce development, and on wider corporate governance issues relating to trust in the digital age, especially relating to internal controls and assurance processes.

In addition, we are a founding member of the UK Cyber Security Council and take an active leadership role in key workstreams, including on qualifications and standards, career pathways and professional ethics. In February 2023, the UK Cyber Security Council and ISACA announced a partnership to co-develop new national standards for cyber auditing, with ISACA becoming the official awarding body for Audit and Assurance Professional Titles.

We have welcomed the opportunity to work with the FRC, DSIT and DBT in supporting the development of plans to reform the UK's corporate governance regime, particularly around electing the correct cyber governance guidance, standards, framework, and metrics, for a number of years. We would be pleased to discuss the contents of our response further with the relevant teams involved and look forward to future opportunities to support government policy development in this area.

Executive Summary

ISACA welcomes this consultation from the FRC on proposed amendments to the UK's Corporate Governance Code. The core amendments suggested in the draft version of the new Code, foremost the introduction of mandatory Resilience Statements and Audit and Assurance Policies for Public Interest Entities (PIEs), are an encouraging step toward improving the quality of corporate stewardship in the UK and addressing the evolving challenges in today's business landscape.

In our response, we outline ISACA's perspective on whether the proposed amendments to the Code will do enough to foster a culture of prudent and effective risk management. We provide suggestions for immediate and longer-term policy developments that reflect on the experiences of our membership working in a variety of Code-adherent large organisations, as well as the continual evolution of business practices. In particular, our suggestions for the longer-term evolution of the Code are founded on our membership's analysis that the trend toward delegation of governance duties to digital solutions is destined to grow and compound, especially as artificial intelligence systems become more mature and readily available to businesses of varying sizes.

We have summarised the key elements of our feedback, below:

- **Broadening the scope of mandatory compliance:** ISACA welcomes recognition that all Code-compliant firms – including those outside of the PIE bracket - could benefit from the introduction of APPs and agrees that encouraging this approach will result in greater consistency and more comparable reporting, across the economy. To further encourage compliance and ensure this consistency is realised, and in recognition of the growing risks posed to corporate resilience by firms' increasing adoption of emerging technologies and the potential future systemic importance of many of these new systems, as a next step, ISACA encourages the Government to consider drafting a timeline for the gradual expansion of the definition of PIEs to broaden the scope of mandatory compliance with APPs and Resilience Statement requirements.
- **Inclusion of methodologies and frameworks within guidance:** ISACA is a firm believer in the value of integrated risk management frameworks and suggests the inclusion of case studies displaying suggested best practice methodologies and frameworks would have the benefit of ensuring consistency across the economy. Moreover, ISACA encourages the Government to consider creating portfolios of best practice that can be hosted on the Government's website as a reference point for firms. This model could replicate existing Government models, such as the Centre for Data Ethics and Innovation's recently established portfolio of case studies displaying a variety of best practice techniques for building AI assurance within organisations. Such portfolios are effective in promoting engagement with affected firms, as well as underlining best practice.

- **Incentivise cultural resilience:** ISACA encourages the Government to ensure the language used in its corporate governance guidance reflects on the variable evolution of different technologies and encourages firms to think about their resilience holistically, and in terms of maturity relative to the risks of the day. Per the above answer, this should be supplemented with direction toward suitable frameworks to measure their maturity against and case studies demonstrating best practice.

- **Support for continuous monitoring:** ISACA believes declarations are more valuable if they reflect continuous monitoring up to the date of the annual report. A declaration based on a single point in time is a one-dimensional statement. A declaration based on, for example, KPIs measured at regular points throughout the year which reflect performance during the year, would be much more informative. Mandating this approach is more likely to encourage closer scrutiny of and diligence to risks and their management throughout the year.

- **Outcome-based reporting:** ISACA endorses the benefit of outcomes-based reporting particularly in instances of departing from the code

ISACA responses to consultation questions

Q1: Do you agree that the changes to Principle D in Section 1 of the Code will deliver more outcomes-based reporting?

ISACA shares the proposed outcome-based approach when demonstrating the impact of governance practices and how the Code has been applied. ISACA believes that this approach should be followed also for the case of departing from the Code's provisions: if it still ensures effective governance practices, the departure from the Code should be allowed, as it could bring substantial benefits in terms of flexibility and proportionality.

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

ISACA agrees that all Code companies should prepare such an Audit and Assurance Policy, as this can reasonably reduce information asymmetry and provide incentives to investors.

For the sake of clarity and completeness, ISACA is also calling to replace the word 'audit' with 'auditing' in the Code context. This is because 'auditing' refers to different audit types together (e.g., financial statement audit and internal audit), while 'audit' only refers to one type. Consequently, the 'audit committee' should be replaced with the 'auditing and assurance committee', since auditing is evolving into an assurance.

ISACA welcomes recognition that all Code-compliant firms – including those outside of the PIE bracket - could benefit from the introduction of APPs and agrees that encouraging this approach will result in greater consistency and more comparable reporting, across the economy. To further encourage compliance and ensure this consistency is realised, and in recognition of the growing risks posed to corporate resilience by firms' increasing adoption of emerging technologies and the potential future systemic importance of many of these new systems, as a next step, ISACA encourages the Government to consider drafting a timeline for the gradual expansion of the definition of PIEs to broaden the scope of mandatory compliance with APPs and Resilience Statement requirements.

Lastly, ISACA highlights the positive effects that the use of blockchain technology could bring to accounting and auditing. Several studies[1] demonstrate that such a technology can provide reasonable assurance of sustainability information by enabling verifiability, traceability, and transparency of data. Using blockchain can not only mitigate information asymmetry, but also ensure a system of automatic assurance and auditing that is quicker, safer, and more accurate.

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?

ISACA would welcome the expansion of the remit of audit committees to include narrative reporting, including sustainability matters. Moreover, to improve the assurance of sustainability information and other narratives, ISACA believes that the role and responsibilities of the audit committee (provision 26 of the Code) should be expanded even further by also seeking assurance for the accuracy of narrative information. The sole monitoring activity of the integrity of narrative reporting, in fact, is not sufficient by itself to ensure a positive outcome, as narratives may be open to information overflow.

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?

The proposed 'comply or explain' approach for internal controls aims to reflect the flexibility, proportionality, and consideration of the particular circumstances of individual companies. While the principles-based approach has many advantages over rules-based regulations, it is applicable if the country

[1] Pizzi et al. (2022) - https://www.emerald.com/insight/content/doi/10.1108/SAMPJ-07-2021-0288/full/html; Dai and Vasarhelyi (2017) - https://publications.aaahq.org/jis/article-abstract/31/3/5/1105/Toward-Blockchain-Based-Accounting-and-Assurance?redirectedFrom=fulltext

has social norms and restrictions, shared values, and interests besides having a common law and outsider-dominated ownership structure. However, if social norms begin to change, a principle-based approach may not be sufficient to prevent opportunism and inner behavior. Therefore, a hybrid approach including rules along with principles may be needed for effective corporate governance. Given the increase in adoption of emerging technologies, foremost machine learning, and the delegation of duties to these technologies, it will be important to set a reasonable timeframe for reviewing the relative success of the current approach. We suggest an annual review would make natural sense, given the rapid development of machine learning solutions.

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?

ISACA believes declarations are more valuable if they reflect continuous monitoring up to the date of the annual report. A declaration based on a single point in time is a one-dimensional statement. A declaration based on, for example, KPIs measured at regular points throughout the year which reflect performance during the year, would be much more informative. Mandating this approach is more likely to encourage closer scrutiny of and diligence to risks and their management throughout the year.

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?

ISACA believes this change would be beneficial on the grounds that it would promote greater transparency and encourage firms to provide more information. This aligns with ISACA's Digital Trust approach to governance of digital risks, and our understanding that it is increasingly necessary to take a holistic approach to risk by establishing security-oriented cultures throughout organisations.

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?

ISACA is a firm believer in the value of integrated risk management frameworks and suggests the inclusion of case studies displaying suggested best practice methodologies and frameworks would have benefits to ensuring consistency across the economy. Moreover, ISACA encourages the Government to consider creating portfolios of best practice that can be hosted on the Government's website as a reference point for firms. This model could replicate existing Government models, such as the Centre for Data Ethics and Innovation's recently established portfolio of case studies displaying a variety of best practice techniques for building AI assurance within organisations. Such portfolios are effective in promoting engagement with affected firms, as well as underlining best practice.

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?

ISACA broadly agrees with the definitions included and would support the addition of a definition on 'material weakness' to aid firms in their assessment of whether they have the appropriate systems of control in place to mitigate against any risks and improve their resilience.

ISACA believes effective risk management process should be documented, have sponsorship from senior management, have oversight from regular committee meetings to review level of risk, have clear risk ownership, and be coordinated across all business functions.

Internal controls should be documented, cross-referenced to the business processes they protect, and have clear ownership. Controls should also be periodically audited.

As ISACA promotes ownership of skills and capabilities, we stress the significance of clear risk ownership. This resonates with our mission to empower professionals to take charge of risks, which it turn fosters a culture of accountability.

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

In the absence of technology rated principles within the Code, ISACA believes Government should include direction to IT, Data, and Cyber specific guidance within the Code. Such guidance will be necessary to help company directors identify risk appetite and tolerance across material aspects of operations, such as cybersecurity, and are good indicators about how robust their controls need to be. This guidance will be most effective if it includes direction toward certifications that organisations can use to assess and improve their resilience, such as CyberEssentials or ISO27001. Effective risk management is multidimensional and requires an understanding of the potential causes of risks to understand the impacts one or multiple control failures will have, and whether containment and severity is isolated or systemic for the organisation. This means continuous assessment holistically across the organisation, region by region, department by department, function by function, basis, with attention to governance of supply chains, too.

Q19: Do you agree that current Provision 30, which requires companies to state whether they are adopting a going concern basis of accounting, should be retained to keep this reporting together with reporting on prospects in the next Provision, and to achieve consistency across the Code for all companies (not just PIEs)?

As stressed earlier in our response, while ISACA is supportive of the Government's proposals to introduce mandatory resilience statements, as a next step, we encourage the Government to consider drafting a timeline for the gradual expansion of the definition of PIEs to broaden the scope of mandatory compliance with APPs and Resilience Statement requirements. As more companies

Furthermore, assuming alignment, we are unsure what the FRC's reporting expectations of non-PIE Code Companies will be. With a longer-term view to broadening levels of compliance and ensuring consistency, ISACA believes that firms not covered by the definition would benefit from clarity of guidance concerning the extent to which they are expected to comply with APPs and Resilience Statement requirements.

Q20: Do you agree that all Code companies should continue to report on their future prospects?

ISACA believes reporting on future prospects is important, not only as it enhances transparency and future accountability, but because it fosters investor confidence in UK companies and aids effective decision making and sustainable growth.

Q26: Are there any areas of the Code which you consider require amendment or additional guidance, in support of the Government's White Paper on artificial intelligence?

ISACA is broadly supportive of the Government's principles-based approach to regulating AI. Combined, the principles will be the right instrument to guide regulators and firms and leave sufficient room for future maneuverability, which in turn promotes investment in this important technology. ISACA would also encourage that the language used within the corporate governance code and guidance reflects the variable evolution of the many possible applications of this technology. Firms will need to reach and adapt to certain levels of cyber security capability maturity to ensure safe adoption, and that these levels in turn should be properly assessed. In line with this, ISACA suggests that official guidance encourages firms to think about their resilience relative to the risks posed by adoption of AI systems in terms of maturity, and that there should be direction towards suitable maturity assessment and measuring frameworks. As previously stated, this could take the form of a Government library or portfolio of best practice, which promotes case studies from affected firms and demonstrates suitable adoption and maturity monitoring techniques and frameworks.