May 2019 **ISACA response to the Independent Review on the quality and effectiveness of audit**

This is a response from ISACA International.

Dear Sir Donald,

ISACA is pleased to be able to respond to the Independent Review on the quality and effectiveness of audit on behalf of its 6,000+ IT audit, information and cyber security professionals in the United Kingdom and its global community of approximately 140,000 professionals.

Your review is both timely and welcome. We especially appreciate the wide-ranging and forward-looking nature of the review as, in our experience, a number of future audit, corporate governance and risk issues pertain to those brought about by the digital economy, especially around technology processes and controls. A number of our areas of interest and thinking specifically cover overlapping themes and the questions you outline—,in particular, internal controls, forward-looking audits, director attestations and statements, information subject to audit and assurance, technology's role in identifying wider material risks such as fraud detection, and increasing the scale and role of assurance in the corporate governance landscape.

As a result, we felt it most helpful to give our view on some key issues and to propose some potential solutions alongside the wider BEIS Future of Audit work, which can be taken as a whole and inform particular workstreams.

In particular, we seek in this response to outline some specific areas of focus:

- The importance of risk management processes and internal controls to corporate governance
- Five key technology and ICT considerations for future regulatory governance
- A process model for a potential future internal controls audit and attestation regime, based upon refinement of Sarbanes-Oxley from the US

We would be most pleased to be able to discuss with you further these particular points and to support your review in any way which may be helpful from a specialist perspective.

Yours sincerely,

ISACA

1.1 Overview of ISACA

ISACA plays a leading role in the UK's cyber security and workforce development efforts by providing accreditation for IT professionals in the IT Audit, IT Governance, and Cyber Security sectors. Our global thought leadership and insight on trends and best practice in these areas is recognised by IT audit practitioners, the wider audit community, Boards and policy makers as a valuable resource that enlightens best practice in corporate governance at a time of rapid change to the systems and controls that underpin organisations' operations.

In recent years, ISACA has worked with HM Government (in particular DCMS and NCSC, but also BEIS and the FRC) on cyber security skills and workforce development and wider corporate governance issues in the digital age, both as an organisation and as an active member of the Digital Policy Alliance and its Cybersecurity Skills group. In addition, ISACA has participated in DCMS working groups on the UK's Cyber Skills Strategy.

This call for views is both timely and welcome. While strategic efforts within HM Government to address the evolving audit and corporate governance and reporting landscapes are encouraging, there are several areas that ISACA believes deserve additional attention and potential action. As experts in the field for 50 years and as an organisation with a strong US footprint, we are well placed to offer specific analysis on what has been proposed for the UK and how the equivalent in these areas has been implemented in the US, not least around the Sarbanes-Oxley Act, which may be useful as BEIS takes forward its policy options in this area.

Our response below is intended to help inform the debate around these issues and is accompanied by a series of suggestions and examples. These need to be discussed in more detail with the BEIS Future of Audit team and developed further at a technical level under any new regulatory regime.

1.2 Executive summary, context and scope of response

A. Importance of risk management processes and internal controls to corporate governance

We welcome, as part of the debate around the future of audit, the explicit inclusion of risk management processes and internal controls. A key thing to remember is that the financial statements are 'tail-end Charlie'. Everything that contributes to the financials goes on before. Governance failures have shown that it is insufficient to attest to just the financial statements.

With the auditor's work reliant on technology, both as a source of data and as a tool to audit the data, ISACA promotes and supports initiatives that increase integrity over the audit process and outputs, including information communication technology (ICT) and non-ICT controls.

Moreover, with ICT both ubiquitous and pervasive throughout any organisation and its supply chain, any risk and control assessment must cover the quality of confidentiality, integrity and availability of those components and data for those authorised to access and use them. Indeed, the Protiviti Executive Perspectives on Top Risks for 2019 report[1] demonstrates that the top ten risks to an organisation are underpinned by issues pertaining to systems, controls and broader corporate governance issues.

[1] https://www.protiviti.com/sites/default/files/united_states/insights/nc-state-protiviti-survey-top-risks-2019-executive-summary.pdf

In addition, with cyber threats gaining in importance within the corporate governance agenda, trustworthy assurance over an organisation's ability to protect the veracity of its data is ever more important. In practice, for any explicit attestation on the risk and control environment, ISACA encourages improved assurance over the ICT used covering the storage, manipulation, use, transport and protection of information and technical components.

B. Five key considerations for regulatory governance

We feel the broader debate about regulatory reform and corporate governance in this area should be driven by some key considerations for regulatory governance:

1. With the heavy reliance on ICT, the Regulator must recognise that it, the auditors and the auditees are now tech organisations, too. This will affect the operations of the Regulator and its expectations over the accounting, auditing and reporting of company results.
2. Therefore, a strong internal audit department must be established within the Regulator that is able to assess the risk management and control over the processes and practices used by the Regulator to deliver mandates.
3. Within the internal audit function, there must exist a highly capable ICT audit team that can focus on the impacts and outcomes of technical usage to processes, analysis, and decision-making.
4. The assurance over ICT relies on having sufficiently high technical awareness across the organisation, from the chairman to the doorman, to ensure people have a healthy balance of trust in, and scepticism of, the ICT outputs upon which they rely.
5. Any tech solution, such as AI (artificial intelligence), is secondary to first understanding and clarifying what will be audited, and only then finding the best tool to help deliver.

C. Process model for a UK-equivalent of Sarbanes-Oxley

Sarbanes-Oxley (SOX) has existed since 2002 as a response to corporate governance failure in the USA. It requires explicit attestation by company boards and others accountable to shareholders and stakeholders. Any similar framework that the UK puts in place would help improve stewardship by the firm to both the owners, on whose behalf they act, and to wider society. It would also complement initiatives for institutional investor stewardship, as set out by the Financial Reporting Council (FRC) in its "Proposed Revisions to the Stewardship Code", for example the need to 'disclose the structures and processes they have in place to ensure that information gathered through stewardship activities is factored directly into investment decision-making'.

1.3 A process model for a potential future internal controls audit and attestation regime

The need for assurance of ICT

This is an increasingly important component of any risk and control assessment because ICT is both ubiquitous and pervasive throughout the organisation and across the supply chain. It is also within the global reach of people with malicious intent. Assurance plays a key role in understanding how things are done by assessing the quality of both ICT and non-ICT controls. The objectives must include an assessment on the quality of confidentiality, integrity and availability of those components and data for those authorised to access and use them.

Controlling ICT is further exacerbated with increasing complexity and innovation. No one individual can understand, and therefore know, the true state of ICT within any organisational ICT perimeter because:

- The increasing use of mobile devices means the perimeter is mobile and fluid, especially as such devices are easily lost or stolen.
- Demand for easy-to-use, instant access and response ICT relies on valid but old protocols combined with newer ones. This bolt-on effect makes component, device and data connectivity both complex and vulnerable.
- The combination of complexity and vulnerability attracts many threats, the common ones leading to data leakage, data theft, data held to ransom and denial of services.
- Components cover firmware, software, hardware and data, all requiring the right level of protection, of which security controls are typically the most important but only if applied in the context of risk appetite, risk tolerance, and legislative requirements. These must be complemented by appropriate governance and control across individuals, individual organisations, the supply chain and the industry.
- Reliance on legal compliance, whilst important, is insufficient as legislation lags innovation. Best practice for each organisation must be better than legal compliance.
- As more analysis, decision-making and actions are carried out by ICT, the more hidden the processes become. We are giving more power to machines and less to people, making interrogation difficult when assessing what has actually happened relative to what was wanted. The paradox is that we need ICT to assess ICT to provide assurance over ICT.

As a result:

- We need experienced technical auditors to evaluate the governance, environment, processes, outputs and the outcomes of everything done by ICT.
- We need to assess the knowledge of key individuals to obtain assurance on how the latest innovations, such as blockchain, IoT, AI and machine learning are being applied, and how well bots perform, all in lieu of humans.
- There is an increasing need to assess the impacts of cryptocurrencies and Fintech are having on how organisations provide, use or account for cash transported and stored by virtual banking.
- Coping with GDPR is difficult enough, yet a 'walk in the park' when compared to a financial audit.

Pertinent aspects of the SOX framework and our analysis on its operations in the US

The key requirements are that:

a) All disclosures must be true, fair, complete and easily understandable.
b) The signatories to the financial statements attest to those statements being true, fair and complete based on the quality of internal controls and information on fraud involving employees. Organisations cannot circumvent these requirements by transferring activities outside the USA (Section 302).
c) In relation to periodic reports, there must be enhanced disclosure covering all off-balance sheet liabilities, obligations and transactions, with clarification of the accounting practices used (Section 401).

d) Organisations provide information on the scope, adequacy and effectiveness of internal controls and procedures relating to financial reporting, with auditors attesting to internal control and procedural effectiveness (Section 404).
e) On an urgent basis, organisations disclose information on material changes to their financial situation or operations, supported by trend and qualitative information (Section 409).

Positive developments from SOX:

In the wake of SOX, financial statements have become more reliable, and part of the reason for this is increased communications. Internal SOX compliance officers interact with external auditing firms to determine appropriate controls; management and the external auditing firm both have discussions with an organisation's audit committee regarding the organisation's financial reporting. These interactions and discussions are ongoing, not episodic, and ensure SOX compliance at all levels of the organisation, always.

When SOX was enacted in 2002, technology was not as advanced as it is today. One of the most significant developments in the business world has been the rise of technologies like cloud computing as well as other emerging technological risks we outline above. For organisations subject to SOX, this technological evolution brought new challenges, such as increased concerns about access controls and third-party oversight, which in turn required even greater attention to the enterprise's own internal controls and even more thorough risk assessment efforts. SOX , has evolved to keep pace with the advancement of technology, in tandem with greater demand for ICT assurance, leading to the creation of SOC audits to better audit security controls. SOC2, for example, covers assurance from service providers, including cloud service providers.

Today, there are an increasing number of organisations using technology tools—particularly in automation—within the SOX compliance process. In its recent Sarbanes-Oxley Compliance Survey,[2] research firm Protiviti noted that automation tools such as automated process approval work flow tools (31%), automated reconciliation tools (29%) and continuous controls monitoring (27%) are beginning to become more widely used, and even still-emergent technologies like robotic process automation (11%) and machine/deep learning (2%) were beginning to make their presence felt. These results may indicate potential future trends for SOX compliance.

Tangible benefits from SOX:

SOX has not been without its criticisms. Some see the additional reporting and compliance requirements of SOX as an impeder of business growth and even entrepreneurial endeavours. Others see SOX as an unwieldy construct that, when introduced into existing or planned operational efforts, no longer makes those efforts efficient or effective. That is why we recommend below a more proportionate, principles-based approach to such regulatory requirements in a UK context. However, one of the key criticisms levelled at SOX has been a fundamental one: the incurring of additional operational costs.

Balance that, however, against the following tangible benefits:

[2] *2018 Sarbanes-Oxley Compliance Survey: Benchmarking SOX Costs, Hours and Controls*; Protiviti, 2018

- The Financial Executives Research Foundation, in a 2005 survey, found a staggering 83% of large company CFOs agreed that investor confidence had increased since SOX's arrival.[3]
- Markets have been able to use information derived from SOX compliance efforts to assess companies more effectively.[4]
- Since the enactment of SOX, the pricing of IPOs increased in certainty.[5]
- Internal processes improved and, over time, internal controls testing has become more cost-effective.[6]

Intangible benefits from SOX:

Intangible benefits from SOX have likely been realized as well, particularly within the IT realm. As a result of increased emphasis on general controls within IT, how many cybersecurity incidents were prevented? How much has the attention to IT general controls benefitted overall governance of information and technology within the organisation, resulting in greater efficiencies and increased oversight? How has better attention to IT risk within the overall operation of the enterprise as a result of SOX compliance resulted in a more positive risk profile for the organisation?

Impactful legislative and regulatory policies, like SOX, have changed the face of corporate accountability and reshaped the audit, governance and security aspects of the IT function. Accountability and trust cannot be additional considerations as the UK continues to transition from a digital to a cognitive economy; they must remain where SOX has placed them—as foundational considerations for the organisations SOX impacts.

That is why we suggest that a tailored UK SOX is the optimal way forward to ensure a proportionate approach that delivers core policy objectives and takes industry with it as a positive corporate governance development. We must also ensure that any future regulation is in line with the UK tradition of principles based legislation that has strong internal buy-in across Boards rather than any rules-based, top-down system which would run both contrary to the UK's approach but also could risk becoming obsolete as new technologies come on stream and new corporate structures begin to develop globally under different legal and accounting structures. We must enact a principles-based structure with consent from regulators and the regulated. This is why the proposals outlined below must be developed further in consultation with a future regulatory regime.

A possible UK approach for attesting on internal controls?

As mentioned in the introduction, the key thing to remember is that the financial statements are 'tail-end-Charlie', with everything that goes on before contributing to the financials. With governance failures proving it insufficient to attest just to the financial statements, the shortcomings can be addressed by covering three things when providing attestations and assurance.

ICT

The first is ICT, as it is now the key mechanism for the changes to, transport of, and storage of data and information. Cyber-threats are also ubiquitous and pervasive, so much so that any interference with data and systems is undetectable in many cases. It is often only when the consequences are

[3] Hanna, J.; *The Costs and Benefits of Sarbanes-Oxley*; Forbes (online); March 10, 2014
[4] *ibid*
[5] *ibid*
[6] *ibid*

made public by the perpetrators does an organisation know its data and systems have been compromised. In the meantime, both auditors and auditees may, unknowingly, be providing reports and assurances based on false information. If ICT is not assessed as part of the audit, then all aspects leading to the financials cannot be seen as accurate or valid.

Organisational governance
The second is organisational governance to assess if the behaviours, relationships and culture from the chairman to the doorman reflect legal requirements and organisational policy. If there is deviation from either, then both the financial attestations and assurances are compromised.

Operational controls
The third is operational controls as they are the agreed way the organisation will carry out its commitments to provide outputs and associated outcomes. If the controls are identified as inappropriate, or are not being complied with, there will be increased risk to, and under-performance by, the organisation. This is a social as well as shareholder loss.

Thus, organisations must ensure their risk management and control functions are working effectively and that due regard is given to the findings and recommendations of Internal Audit and any other independent, third party review. Only then can the scope of the financial audit be established.

Potential process model for a UK-equivalent of Sarbanes-Oxley

The scope, referred to above, must, of course, reflect the more explicit statements around risk management and internal controls if a SOX-equivalent is introduced. There is the question of whether these statements should be subject to audit. Assuming they are, here are two approaches for illustrative purposes.

The first is that auditors perform audits on these statements, essentially applying the equivalent (yet to be defined standards) of financial accounting standards, using the explicit statements made by the directors as the benchmark for their independent assurance. The second is that auditors execute enhanced reviews to support 'going concern' statements, in which case their results should complement directors' explicit statements.

Both approaches rely on sound judgement that requires a combination of knowledge and expertise over corporate governance and accounting. That covers a huge variety and volume of financial and non-financial data. ICT will be heavily involved. AI, which is good at comparing and analysing structured and unstructured data, can help check for complementary, contradictory and missing statements. The use of AI is not a panacea, just a tool. The optimum solution, AI or other options, relies on first understanding and clarifying what will be audited, then finding the best tool to help deliver, with supporting controls to ensure trust in its outputs.

These director attestations are ultimately providing declarations that:

- Their organisations are honest, competent and trustworthy.
- Third parties have confidence in their organisations' integrity and capability.
- Operations are carried out under worthy leadership and within an appropriate culture, meeting all relevant regulatory, professional and organizational standards.

- Board, management and staff feel positive about being part of the organisation, aligning their behaviour and relationships to stated corporate values.

That means auditors need to check for:

1. A comprehensive, understandable, integrated ICT and business, enterprise risk management framework, for example:
    a. Stating defined risk appetite and tolerances across all aspects of the business supported by the relevant risk assessments.
    b. Demonstrating how ICT is incorporated within business lines and how effective the interaction between ICT and business staff is.

2. Explicit testimony over the key risks and quality of controls, for example.
    a. Having clear responsibilities across the three lines of defence, i.e., business management, risk managers and internal audit.
    b. Attestation that policies are relevant and being complied with.
    c. Evidence of staff having the relevant knowledge and experience to deliver, use, maintain, secure, assure and repair ICT.
    d. Evidence of effective ICT controls that interact usefully and continuously with business strategy, processes and practices.

3. Application of recommendations from the three lines of defence or justification for why recommendations were rejected, for example:
    a. Evidence of sound anti-fraud, business continuity, crisis management and disaster recovery plans.
    b. Remedial processes to inform, correct and compensate stakeholders, including customers, the regulator and police.
    c. Full disclosures over rejected recommendations and why non-application fits within risk tolerances.

4. Compliance with legal, regulatory, policies and procedures, for example:
    a. Demonstrable, relevant interaction between the board, the audit committee, the external auditor, the internal audit and the executive that enhances, not compromises, the opinions and judgements made. This can be described as working 'hand-in-hand' to deliver stakeholder value, whilst avoiding being 'hand-in-glove', which compromises independence and obscures the actual state of things.
    b. Suitably frequent reviews of policies, procedures and practices, including risk and control assessments.
    c. Demonstrable proof that the financials are supported by operations, outputs and outcomes, including all shortfalls as well as achievements.

5. Attestation that the process and ICT used to provide all of 1-5 is valid, true and complete.

1.5 Conclusion and next steps

The future is challenging. Something that will need to be catered for is the growing trend in businesses becoming tech-service-centric. ICT's uses create a conundrum: when is ICT the business rather than just the infrastructure, demonstrated by the rise of technology platforms delivering other sector products such as retail, transport and accommodation? Fintech is doing the same in banking. The point here, is that any financial audit faces the dual complexity of auditing intangibles that are difficult

to value, on platforms comprised of many parties' intellectual property. The FRC is currently reviewing how intangibles can best be valued (see https://www.frc.org.uk/news/february-2019/consultation-into-improvements-to-the-reporting-of). Any SOX-equivalent requirements will have to take the FRC's conclusions into account.

Taking all of the above into account, ISACA welcomes the Review's scope and some of the initial BEIS and FRC thinking around audit reform, but would recommend that more attention be paid to the role ICT plays in providing the very information on which annual reports and accounts are produced and audited. A SOX-like approach, to explicitly include attestations by both auditor and auditee on the risk and control environment is encouraging but, to be fully effective, must include ICT. At the very minimum, any approach must include a focus on assurance around ICT controls, organisational governance and operational policies and controls, and our proposed model looks to incorporate this in a practical new regulatory structure.

We are pushing at an open door. At a 10th April event on 'Audit Reform in the UK', hosted by City & Financial Global, the idea of a UK-equivalent SOX was warmly supported by non-executive directors, audit committee chairs and auditing firms alike.

We would be very pleased to discuss this further with the review secretariat in person, especially around how a UK Sarbanes-Oxley regime might be structured and operated.