IAAC Submission to the Independent Review into the Quality and Effectiveness of Audit.

7th June 2019

To: brydonreview@beis.gov.uk

About IAAC.

The Information Assurance Advisory Council (IAAC) is an independent not for profit body that brings together a community of cyber security professionals in order to address information assurance and related challenges and opportunities faced by the 'Information Society'. This includes corporate leaders, government officials, members of the defence, security and law enforcement communities, academics, scientists and technical experts. IAAC was founded in 1999. Since then, through its strategic research and influence, it has been at the leading edge of many of the developments in Information Assurance and Cyber Security thinking in the UK, maintaining a non-partisan position on matters affecting the way society uses and protects information and services. Contact details for IAAC are at the end of this document.

Introduction

IAAC welcomes the opportunity to contribute to the Review. Our submission is built upon a study developed through 2018-19 on the valuation of the information asset, findings from which are shortly to be published.

We started with a working hypothesis that security professionals responsible for the security of an organisation's information assets were undervaluing the asset by focusing mainly on the cost of its loss. This was in the context of an economy in which businesses were increasingly generating value through data and digital services. Moreover, markets were valuing companies on the basis of their intangible assets rather than simply those appearing on the balance sheet.

IAAC recognised that this represents a problem for security professionals and business leaders alike, when trying to understand the 'true' value to the business and what was to be exploited and protected. It is also a challenge for investment decisions and shareholders when trying to quantify and qualify the value to the business. There was also the question of whether businesses were paying enough due care and attention to maintaining the asset.

On this challenge one must overlay sectoral regulation regarding information governance, and new regulations such as the General Data Protection Regulations (GDPR) and the Network and Information Systems Directive (NISD) for operators of essential services. These must be seen in the context of increased public interest - in both meanings of the word 'interest'- and citizens' rights regarding the stewardship of data and information by organisations and companies.

Whilst IAAC noted some progress, there has yet to be sufficient movement from organisations and businesses in addressing this appropriately. There is therefore a need for a series of interventions to bring about the change required.

Alongside calls for the information asset to be valued on the balance sheet, IAAC research demonstrated why this was unlikely to happen. Instead we began to focus on methods which would sit readily in the realm of internal management accounting, whereby a scorecard or narrative report might be developed to show the relationship between the information or data asset, its processing and its value to the business. IAAC and its contributors did, however, recognise that there was an imperative to have some form of information asset or cyber audit in external auditing, even statutory audit. It is for this reason that IAAC is responding to this timely review, informed by the work conducted over the past twelve months.

Why the information asset and not other intangibles?

Before addressing the Review chapter specific questions, it is worth clarifying what we mean by an information asset. IAAC understands the term 'information assets' broadly to mean both a body of organised knowledge, including the data in it, as well as the processes of an organisation applied to data, such as its analytics or its ability to control or manage its digital processes or electronic infrastructure. We argue that it is worthy of specific attention in auditing as an asset, compared to other intangibles, for three main reasons.

The first is the way data is driving value for many businesses and how the innovative use of information and information systems is at the heart of the modern economy and society. Second is the public good, as citizens have a stake in how their data is used and maintained by organisations, arguably in many cases with the same interest as though it were their money; or because they are the beneficiary of critical digitally-enabled services. The third develops on this last point: nationally, our reliance on digital services represents an existential vulnerability worthy of transparent accountability and therefore quality auditing.

There is an opportunity for the UK to lead in this important area of governance.

Chapter One

In relation to chapter one, IAAC argues that the audit audience is broader than the company and shareholders, because of the public good imperative. For the reasons described above, the audit should provide assurance to users of the entity, and not just its shareholders.

Chapter Two

Paragraph 25 mentions 'capital maintenance'. In line with emerging principles in Integrated Reporting, data and information can be seen as one of the intangible capitals, referred to as 'intellectual capital'. IAAC would wish to use 'information asset' as a specific term in which we see an 'expectation gap' in reporting. We would argue that capital maintenance of the information asset requires that risk-based processes and controls are suitable for the confidentiality, integrity and availability of data, information and information systems. Whilst in the area of personal data GDPR and UK data protection law has laid out guidance and responsibilities, it is almost always in the

context of a breach that the reasonableness of a company's risk assessment, risk management and controls, will be tested. There is therefore a strong argument for statutory reporting on a regular basis, related to assurance about reasonable management and controls.

Chapter Three

Question 8 asks 'Can the level of assurance that an audit provides legitimately vary in different circumstances, for example depending on the business sector in question, and the nature of the entity's business risks?' IAAC recognises that the nature of the business, the services it provides, the data it holds and processes, national and citizens interests, all impact upon business risk. We would expect that audit would take account of this, through a process of assessing an appropriate mix of standards, reasonableness and internal processes. Businesses across sectors, of differing sizes, should play a key role in developing, or adapting existing, criteria in this area. This should include communication of internal management accounting and information governance processes.

Chapter Four

Q13: Should auditors' responsibilities regarding assessing the effectiveness of an entity's system of internal control be extended or clarified?

It is our judgement that an assessment of internal controls is likely to be a key part of addressing Question 8 in Chapter 3, discussed above.

Q14: Auditors are currently required to report to audit committees their views on the effectiveness of relevant internal controls for listed and other relevant entities. Should auditors be required to report publicly these views?

It is IAAC's view that in the area of reporting about information governance, some aspects should be public in order to provide general assurance, and some aspects should only be reported to the audit committee. This is because some specific elements of unfavourable reporting about the organisation may mark it out as a target for malicious exploitation or attack. A multi-stakeholder approach should be adopted to examine the trade-offs involved in this.

Questions 15-19

The questions regarding going concerns and viability is an interesting one which requires more research, as companies in markets driven by data intangibles may represent unquantifiable risk for investors and other stakeholders. One recommendation we would make is that, as a minimum, a company should provide, in a narrative account, a 'value chain map' to communicate the logical link between the intangible asset and the business benefit derived from it. This could show an annotated link between the asset, the internal business process it supports, the derived service to the customer and the financial outcomes as a result. This could form part of benchmarking and trend data over time, with KPIs and periodic reporting. This construct is based on previous work undertaken to show the value of HR to a business. [1] IAAC has applied it to data and information in our study, which is due for publication in the coming weeks.

[1] See Brian Becker, Mark Huselid, Dave Ulrich. The HR Scorecard: Linking people, strategy and performance. Harvard Business Review Press, 2001

Chapter 5

Reporting such as that discussed above may also help address Q 27 regarding reducing boiler plate disclosures. Whilst this remains a real risk, the requirement to show investors how the company generates value, may also require the ability to show differentiation in the market. How a company uses and maintains its intangible information asset capital to create value, and avoid loss or reputational damage, is a differentiator that drives market value, and one in which risks can be communicated. It is therefore also one that can prevent full disclosure to the public, which is another reason for some reporting to be treated as per Q14 above.

Chapter 6

As discussed above, developments in **regulation and law** in the area of information and system governance can be strengthened by external audit.

Chapter 9

Regarding auditor liability, there is no doubt that specialist skills and knowledge will be required on auditing teams regarding the information asset. This may be developed in line with current professional practice advocated by professional and other certification bodies.

Chapter 10

Regarding culture, the organisation's stewardship of information is one of good governance and care for shareholders and clients. This results in care for information and data as an asset. Reporting on risk and internal control processes, given the value of the assets, is likely to be a proxy for communicating good information governance culture.

The IAAC report will be available in the next few weeks on our website, www.iaac.org.uk should further information be required following this consultation.

Nigel A. Jones
CEO IAAC
Info@iaac.org.uk