Department for
Digital, Culture,
Media & Sport

Department for Digital, Culture, Media and Sport response to the

INDEPENDENT REVIEW INTO THE QUALITY AND EFFECTIVENESS OF AUDIT CALL FOR VIEWS

10 June 2019

Response by the Department for Digital, Culture, Media and Sport to the Independent Review into the Quality and Effectiveness of Audit (Call for Views)
Approved by the Minister for Digital and Creative Industries Margot James

Overview

DCMS

DCMS plays a key role in delivering the Government's current National Cyber Security Strategy.[1] Part of the DCMS Cyber Security Team's remit centres on ensuring all organisations in the UK are effectively managing their cyber risk to ensure the UK economy is safe, secure and prosperous. Central to this is that organisations understand their level of cyber risk exposure and embed proportionate cyber security practices, including throughout their governance and risk management.

Executive summary

DCMS is in favour of an extension of both the audit process and outcome to broaden its statutory scope to include and enhance the non-financial elements of business operations. In particular, we advocate enhancing the approach to assessing business continuity and core risk management functions by incorporating an assessment of cyber risk management, as a material risk faced by a majority of UK entities. A broader statutory audit remit would require an entity to provide greater assurance on non-financial aspects of business operations which are intrinsically linked to the financial viability of the entity, and therefore have a significant impact on its ongoing sustainability. Limiting the audit process to financial statements and to a binary output reduces the audit's potential assurance level, and thus its value.

DCMS is particularly concerned about the increasing pace of technological change and innovation, with an ever increasing digital component of business operations across all sectors. It is unlikely that there will be any UK business whose business operations do not, at least in part, rely on digital infrastructure or services over coming years and there is increasing pressure on CEOs to make the most of new technology for their business.[2] This is also demonstrated by recent changes to the reporting landscape, for example the fact that many businesses will soon be required to keep digital records as part of HMRC's programme 'Making Tax Digital'.[3]

The growing importance of digital transformation has placed securing business against cyber threats at the heart of the long-term viability of businesses. In this way, cyber security is already an intrinsic part of many entity's viability and long-term health, with increasing board attention.[4] Adequately managing this cyber risk has increasingly become a vital part of strategic business decision making and investment.

In particular, cyber security incidents have the potential to cause significant financial damage, to an entity's share value as a result of the incident itself, or through associated fines imposed by regulators, such as the ICO and/or sector specific regulators. Equifax totalled its spend on costs related to their breach, including the additional expenditure on IT and data security required as a

[1] HM Government, 'National Cyber Security Strategy 2016 to 2021', https://www.gov.uk/government/publications/national-cyber-security-strategy-2016-to-2021, 2016.
[2] Gartner, '2017 CEO Survey', https://www.gartner.com/smarterwithgartner/2017-ceo-survey-infographic/, 2017.
[3] HM Revenue & Customs, 'HMRC publishes more information on Making Tax Digital', https://www.gov.uk/government/news/hmrc-publishes-more-information-on-making-tax-digital, 2018.
[4] Department for Digital, Culture, Media and Sport, 'FTSE 350 cyber governance health check 2018', https://www.gov.uk/government/publications/cyber-governance-health-check-2018, 2019.

result, at $1.35 billion since reporting its data breach in 2017. UK-based research has shown that following a severe breach, share prices fall by an average of 1.8% on a permanent basis and that severe cyber breaches will become even more costly in the future.[5] The potential for these types of events has increased interest from shareholders, investors and the public in seeking assurance that cyber risk is being managed appropriately. Indeed, cyber attacks are now the biggest threat to business in the eyes of investors.[6]

As a result, cyber risk is increasingly assessed as a principal risk by boards and their audit and risk committees. However, boards and senior managers struggle to implement holistic risk governance practices that embed cyber risk management throughout their business. Increased and enhanced audit scrutiny would incentivise organisations to provide additional assurance through offering a high quality, standardised and externally verified process, both assisting and requiring organisational leaders to improve their management of cyber risk accordingly. It should be noted that, should the audit process and output be enhanced and expanded to consider and assess greater forms of risk management, this would involve greater costs. Alongside any such changes should be a consideration of scope of entities to whom statutory audit applies based on the levels of risk the entities pose to the UK economy and market.

In light of these considerations, the key components of DCMS' response to the Independent Review into the Quality and Effectiveness of Audit Call for Views are that:

a. **Risk management** is intrinsic to an entity's ongoing viability. Trust in business and the market must therefore be underpinned by a qualification of entities' risk management.
b. Pervasive **digital transformation** and rapid technological innovation is making the digital component of companies an increasingly critical function of business operations. This exposes companies to additional cyber threat and a majority of UK companies are seeing **cyber risk as a top principal risk**. For cyber risks to be effectively managed, they must be considered as part of the company's strategy and all relevant business operations.
c. As the central function of audit is to provide assurance in the ability of companies to operate effectively, responsibly and sustainably, we recommend:
    i. An **extension of the audit *process* to** broaden its statutory scope to extend beyond assurance of financial statements, in particular **risk management functions, including cyber risk management.**
    ii. **Amendment of viability statements to include** an assessment of the sustainability of the entity's business model in light of the nature of **cyber risks**.
    iii. **Revision of the audit *outcome*** that shifts away from its current binary nature, to enable a more graduated assessment that reflects the varying levels of maturity
    iv. That underpinning these changes, the audit process and outcome should consider **different forms of evidence and assurance** on the critical non-financial elements of business operations in order to enable greater transparency of information and nuance in the assurance provided.

In the below sections we provide responses to the questions posed in the Call for Views most pertinent to our rationale for a revision and enhancement of the statutory audit process and outcome.

[5] CGI, 'The cyber-value connection', https://www.cgi.com/sites/default/files/2018-08/cybervalueconnection_full_report_final_lr.pdf, 2017.
[6] PwC, '2018 Global investor survey: anxious optimism in a complex world'', https://www.pwc.com/gx/en/ceo-survey/2018/deep-dives/pwc-global-investor-survey-2018.pdf, 2018.

Response to individual questions

Definitions of audit & its users

1) For whose benefit should audit be conducted? How is it of value to users?

In general terms, confidence and trust in both entities and markets are derived not just from an assurance that organisations are following statutory obligations or from financial statements alone, but integrally, from a broader assurance that an organisation is managing its business responsibly. Responsible management of any entity necessarily includes thorough risk management, to ensure it is protected against and resilient to the most adverse risks it faces. Audit plays a vital role in underpinning confidence in capital markets and building trust in entities, and has the potential to play a much stronger role and more valuable role that begins to align more with expectations in both its performance and its evolution. DCMS recommends that such a role would provide a greater level of assurance of entities' sustainability and business continuity through assessing of mitigative activities toward the commonly identified principal risk of cyber security.

The value of audit will necessarily depend on each of its users' needs. A primary user of the audit outcome is shareholders and investors, who expect to see that the entity is operating in the interest of *shareholders*. The purpose of audit from this perspective should be to allow shareholders and potential investors to make more informed investment decisions using insights and assurance obtained through the audit process. Currently, the assurance aspect of audits often results in a view of the audit outcome as an indicator of business health.[7] However, informed investment decisions arguably require greater assurance than that which audit currently provides, and necessitate judgements on the entity's capability and action to mitigate key risks to business operations and revenue.

A secondary flow on from the benefits realised by shareholders, investors and lenders, is the role of the audit product in providing information transparency to the market, thereby shaping not just individual but market behaviour. The provision of this information to the market has wide ramifications with regard to macroeconomic shifts and influencing behaviour at a macro level. Audit's potential value lies not just in the specific statement it produces about an entity's financial statements, but in the underlying confidence that is being put in the entity as a result of this judgement. That is, the expectation gap cannot be discounted, as it is the perception of the entity that is derived from the audit output that is the most pertinent impact of the audit itself. Careful consideration would need to be given to the communication of any changes to audit's scope, to ensure that this opportunity is taken to redefine its potential and its limits and close the perception gap as much as possible.

A further user of the audit process and outcome are the audited entities themselves. Audit should also be an essential mechanism for companies to receive external verification over both internal processes and controls. Being overseen and publicly reported on provides a benefit in stimulating better practices within the company itself. This has the potential to improve risk management, including of cyber risks, and should audit capture elements of non-financial risk management more broadly. Moreover, risk management is an essential part of an entity's financial management as it enables an entity to ensure it has sufficient contingency in place should significant risks be realised, such as in the event of a cyber attack or data breach.

[7] ICAEW, 'Audit and beyond', https://www.icaew.com/technical/audit-and-assurance/faculty/audit-and-beyond/audit-and-beyond-2012/june-2012/from-perception-to-perfection, 2012.

2) Should the audit be designed to enhance the degree of confidence of intended users in the entity or just in the financial statements?

If the public, shareholders and investors, and the companies themselves are taken to be beneficiaries of the audit process and outcome, we recommend that to be of most value to these user groups, audit should be expanded and amended to reflect the already existing perception of it as a confidence building mechanism in the *entity*, not just in the financial statements in and of themselves. Users currently view the assurance derived specifically from the auditing of financial statements as representative or a reflection of the entity itself, its performance and its sustainability.

Overcoming the expectation gap is a complex and long-term task, and failing to address the gap has the potential for audit to become a less important assurance mechanism as a result of lower expectations by intended users. Previous work to better communicate and increase messaging to address the perception gap has shown to have failed over the course of decades.[8] Therefore, moving the audit function closer to where current expectations and perceptions lie provides opportunity to increase the value of the audit by extending its scope to cover other current and future business risks.

We recommend that a broader statutory audit remit requires an entity to provide greater assurance on non-financial aspects of business operations that are intrinsically linked to the financial viability of the entity and can therefore have a significant impact on the ongoing sustainability of the entity. The business landscape has radically changed and is ever more closely intertwined with various other social and economic external risks, such as corporate social responsibility requirements, climate change, modern slavery and others.

The shift toward a more digital economy has brought with it a certain set of risks, one of which centres on cyber risks, which is pertinent to a nearly all organisations today with all sectors targeted by increasingly sophisticated cyber attacks. The increased importance and prevalence of cyber risk is demonstrated in the World Economic Forum's *2019 Global Risk Report,* which highlights cyber as one of the top five global risks. Cyber risks are increasingly a central focus of corporate reporting, being reported as a principal risk in the annual reports of large companies (89% in 2018)[9] and IT disruption and data compromise being listed as top operational risks across most organisations.[10] Over recent years, cyber risk has been squarely situated as a central cross-sectoral operational risk across the UK economy, particularly for large organisations. However, many organisations do not yet have the maturity or have not taken sufficient action to effectively deal with cyber risk. This can have significant implications for business resilience and continuity, and for the strength and resilience of the UK economy as a whole.

DCMS recommends the audit process provides assurance more broadly over the entity in order to ensure investment decisions are based on a more holistic understanding of the entity. Such a view of the entity would necessarily and primarily need to include an understanding or judgement of the entity's risk management toward principal risks. Accordingly, cyber risk management should be brought within the audit process remit to provide increased confidence in the business' ability to be viable through the digital transformation that now underpins the UK economy. Given the increased cost burden to the entity that these changes would mean, a review of entities in scope of such a modified audit would be required. The scope, with regard to entities, of a statutory audit with

[8] Association of Chartered Certified Accountants, 'Closing the expectation gap in audit', https://www.accaglobal.com/content/dam/ACCA_Global/professional-insights/Expectation-gap/pi-closing-expectation-gap-audit.pdf, 2019.
[9] Deloitte, 'Governance in focus: cyber risk reporting in the UK', https://www2.deloitte.com/content/dam/Deloitte/uk/Documents/audit/deloitte-uk-gif-cyber-risk-reporting-uk-march-2018.pdf, 2018.
[10] Risk.net, 'Top 10 operational risks for 2018', https://www.risk.net/risk-management/5424761/top-10-operational-risks-for-2018, 2018.

enhanced cyber risk management assessments should be proportionate to those entities that pose a greater risk to the UK economy by virtue of their size and capacity to adversely affect the market.

The scope and purpose of audit

12) Should directors make a more explicit statement in respect of risk management and internal controls? If so, should such a statement be subject to audit?

Since the financial crisis and more recent audit failures, such as the collapse of Carillion, there has been action taken for increased scrutiny of company directors, such as the introduction of the Senior Managers Regime and increased powers to the new Audit, Governance and Reporting Authority. These changes mean directors are going to be increasingly held to account for preparing and approving true and fair accounts and compliant corporate reports. Risk management is fundamental to the success of an organisation, given its integrity to business continuity and, as such, information has increasingly been sought from entities on elements of their risk management through the introduction of viability statements.

In a digital age, the opportunities that organisations can leverage are increasingly the result of advances in technology. The digitization of the economy means that all facets of the business environment, from the design of new products and services, to distribution networks and customer data, are now more vulnerable to cyber threats. Digital transformation has thus become a key focus of business strategies, which brings with it additional cyber risk, and senior leadership and directors have begun to acknowledge the centrality of cyber risk management. Since 2013, we have seen a rise from 25% of FTSE 350 boards perceiving cyber risks as a high or very high, to now 72% in 2018.[11] Companies furthermore acknowledge this risk in their reporting, with 89% of FTSE 100 companies identifying cyber risk as a principal risk in 2018.[12]

Company directors and organisational leaders play a key role in managing cyber risks to ensure an entity and its investments remains protected and resilient throughout its business operations. The board is responsible for directing the organisation and ensuring its prosperity within it's regulatory jurisdiction. A key mechanism to provide assurance of this is through audit.[13] Despite business operations often linking audit and risk, the current audit process does not place enough emphasis on risk assurance in accordance with its central role in creating confidence and trust in the entity.

Risk management is furthermore intrinsically linked to an entity's financial stewardship, and whether audit remains an assurance mechanism over financial information or whether its remit is expanded, DCMS recommends that it nevertheless capture a certain level of risk mitigation activity and governance to give increased confidence in the audit outcome. Audit users must be provided with assurance that the risks to the business are being managed and mitigated appropriately. As noted above, an enhanced or expanded scope for statutory audit would also require the consideration of who should be subject statutorily to such an audit. Given the increased cost burden to the entity, due consideration should be given to ensuring that entities that pose a greater risk to the UK economy by virtue of their size and capacity to adversely affect the market are those subjected to this process.

[11] DCMS, 'FTSE 350 Cyber Governance Health Check 2018', https://www.gov.uk/government/publications/Cyber-governance-health-check-2018, 2019.

[12] Deloitte,'Governance in focus: cyber risk reporting in the UK', https://www2.deloitte.com/content/dam/Deloitte/uk/Documents/audit/deloitte-uk-gif-cyber-risk-reporting-uk-march-2018.pdf, 2018.,

[13] Internal DCMS report available on request, report prepared by CybSafe Ltd., 'Rapid evidence assessment on board engagement in cyber risk management', 2019.

17) Should directors make a statement about the sustainability of the entity's business model beyond that already provided in the viability statement?

A viability statement contains the directors' assessment of the company's prospects over an appropriate specified period, taking account of its current position and principal risks.[14] While viability statements have been a useful development in corporate reporting, companies often produce boilerplate statements which have limited meaningful information.[15] Many companies now regard viability statements as just another legal and compliance hurdle to overcome. Whilst the FRC has encouraged their use and has stimulated conversation across industry, it has not done enough to encourage long-lasting best practice and innovation in this area. Going forward, more needs to be done to drive better disclosure from boards on how they assess their viability, including what risk management approaches support their continued viability, and over what time period. Investors want to see meaningful long-term statements. A PwC report highlights that where possible, viability statements should contain a genuinely long-term focus on a company's business model and strategy.[16] As this Call for Views references, Sir John Kingman's Independent Review of the Financial Reporting Council has recommended that these statements should be abolished if they cannot be amended into a substantially more effective requirement.[17]

DCMS agrees that viability statements should be reformed to include more useful information on the sustainability of the entity's business model alongside an assessment of the company's current position and principal risks. Risk is inherent in an organisation's decisions regarding the pursuit of opportunities and growth. In a digital age, the opportunities that organisations can leverage will continue to increasingly be the result of advances in technology.[18] Digital transformation has thus become a key focus of business strategies, which brings with it additional cyber risk. Moreover, the speed, complexity and systemic nature of this technological change has the potential to threaten an entity's whole business model and operations. It is therefore essential that viability statements include an assessment of emerging risks to the businesses model due to factors that could significantly impact business operations such as technological developments and cyber threats.

Additionally, a key concern for managing cyber risk is that many organisations still only consider cyber security to be an IT-specific or security-specific issue, rather than a responsibility embedded across the entity as a whole. Effective cyber risk mitigation underpins an entity's entire business model and operations, from security measures through to business strategy and decisions which integrally centre on senior leadership and the board such as mergers and acquisitions, and entering new markets.

When cyber risk is identified as a principal risk and considered in viability statements, it should be reviewed alongside the entity's business model to ensure that cyber risk is being considered as part of the company's strategy and all relevant business operations. The previous ineffectiveness of the implementation of viability statements also suggests that both further stipulations of what level of detail they include, and a stronger form of audit or assurance over these statements would be necessary.

---

[14] Financial Reporting Council, 'Guidance on Risk Management, Internal Control and Related Financial and Business Reporting', https://www.frc.org.uk/getattachment/d672c107-b1fb-4051-84b0-f5b83a1b93f6/Guidance-on-Risk-Management-Internal-Control-and-Related-Reporting.pdf, 2014.

[15] PwC, 'Tackling the viability statement: Practical suggestions, positive thinking – An update', https://www.pwc.co.uk/audit-assurance/assets/pdf/tackling-the-viability-statement-an-update-web.pdf, 2016.

[16] PwC, 'Tackling the viability statement: practical suggestions, positive thinking – an update', https://www.pwc.co.uk/audit-assurance/assets/pdf/tackling-the-viability-statement-an-update-web.pdf, 2016.

[17] Sir John Kingman, 'Independent review of the Financial Reporting Council', Recommendation 52, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/767387/frc-independent-review-final-report.pdf , 2018.

[18] PwC, '2018 Global investor survey: anxious optimism in a complex world'', https://www.pwc.com/gx/en/ceo-survey/2018/deep-dives/pwc-global-investor-survey-2018.pdf, 2018.

18) Should such a statement be subject to assurance?

DCMS recommends that viability statements which consider the sustainability of the entity's business model should be subject to assurance. Audit or other assurance could be required to validate the process undertaken by the entity to produce and assess viability statement. Many companies already report on how they have assessed viability through exercises such as stress and sensitivity analysis, or disclosure of how scenario analysis has been applied to principal risks. An FRC Lab Project Report highlighted that investors find this information very useful for understanding the company's resilience to risk.[19] It would be possible for audit to review and test that these exercises had been conducted and considered by the entity's audit committees when developing viability statements. Sir John Kingman's Independent Review of the Financial Reporting Council also proposed that companies could be required to provide additional details of the testing used to underpin viability statement and that this testing should be subject to audit, or some other form of assurance.

Given the intrinsic nature of viability statements (and their treatment of principal risks) to an entity's continuity, their additional assurance through the audit process would be particularly useful if other related proposals of Sir John Kingman are also implemented. The Independent Review of the Financial Reporting Council recommended the establishment of a new regulator with additional corporate reporting oversight and enhanced audit regulation and quality control. If adopted, these recommendations could require viability statements to be subject to secondary independent assurance through the regulator, including:

- Increased scrutiny of viability statements in annual reports;
- The proposed new regulator having powers to require a company to procure additional assurance on the viability statement such as where there are concerns about the credibility of a company's viability; and
- A duty of alert for auditors to report viability or other concerns relating to audit to the regulator.

20) Is there a case for a more forward-looking audit? What would be the main benefits and risks?

DCMS believes that the audit process should be extended to include further non-financial elements of business operations, particularly an increased focus on risk, including cyber risk, and the longer term health of an entity. Companies need to demonstrate that they are able to adequately respond to the present cyber threat and future trends in order to protect not only themselves and their shareholders, but also the broader economy given the systemic nature of many supply chain threats that we have seen spread such as NotPetya and Wanna Cry. As the long-term health of companies is increasingly reliant on technological developments, it is imperative they have the ability to adapt to these advancements and the related threats. A broadened audit remit should require information and assurance of how their ability to respond to associated cyber risks of digital transformation will impact the long-term health of the business, including the business model, principal risks, and future viability.

These more subjective business areas will naturally require different types of evidence to be provided by companies undergoing an audit. Ideally, the assessment of the long-term health of a business would develop to be a varied assessment, drawing on established assurance processes which support the recommended broader scope such as indicators of good governance and risk management. However, in the short to medium term, this may likely require a binary assessment of long-term business health while the sector matures to provide the appropriate supporting assurance mechanisms.

[19] Financial Reporting Council, 'Risk and viability reporting', https://www.frc.org.uk/getattachment/76e21dee-2be2-415f-b326-932e8a3fc1e6/Risk-and-Viability-Reporting.pdf, 2017.

21) Would audit or assurance over financial and non-financial information outside the annual financial statements (for example KPIs or non-financial metrics, payment practices or half-yearly reports) enhance its reliability and therefore be of benefit to users?
22) If so, what information might usefully be subject to audit or another form of assurance and why?

As noted throughout this submission, DCMS believes that the audit process should be extended to include additional non-financial elements of business operations. Given the intrinsic and fundamental nature of risk management to the success of an organisation, and given its integrity to business continuity, we recommend the inclusion of indicators of the management of principal risks be included in and subject to audit or assurance processes. We furthermore recommend that under such a change, an entity's mitigation and resilience be covered to provide additional assurance on the entity's cyber risk management.

Should non-financial information be included in an audit or assurance process, due consideration must be given to how this information would be both assessed and reported on. As per the below response to question 25, it is common for organisations to apply a financial and binary approach to risk management, however, security and cyber risks specifically would necessarily require more nuanced, judgement based decision making.[20] In contrast to financial investments, the appropriateness of internal controls in light of a given risk exposure requires a more in-depth assessment by auditors. Auditors would also be required to provide a meaningful opinion which incorporates an indication of why and to what extent the auditor has assessed the company to have taken informed and proportionate steps to mitigate their risks. This currently occurs in more in-depth process audits, however, process audits can be more subjective, time consuming and require a broader skill set than that currently held by the general audit profession.

Risk management, including the identification, assessment and treatment of risk, is often subjective and judgement-based. Whilst business approaches to risk management mature, there may be a need for binary approaches, in particular in emerging areas of risk. However, as explained above, the longer term ambition should be to provide further insights into the entity's continuity and viability that lie across broader activities than just the production of financial statements, and should include an assessment of the management of principal risks.

In order to aid the work of auditors in arriving at a more nuanced audit opinion, a standardised framework that provides guidance around how companies should be assessed against their ability to proportionately and appropriately manage their risk(s), would enable a harmonised approach across industry. DCMS strongly recommends that standardised frameworks be adopted for areas of key concern across the economy, such as cyber risk management. Given the likely increased associated costs of such a type of audit, the scope of entities statutorily subjected to the audit process should be considered alongside any greatly enhanced or expanded scope for audit. Those in scope should be those considered to pose a greater risk to the UK economy by virtue of their size and capacity to adversely affect the market.

Audit product and quality

25) What additional benefit might a switch from a binary audit opinion to a more graduated disclosure of auditor conclusions provide?

[20] Institute of Risk Management, 'Cyber risk: resources for practitioners', https://www.theirm.org/media/3814330/IRM-Cyber-Risk-Resources-for-Practitioners.pdf, 2014.

DCMS recommends that a more graduated disclosure of auditor conclusions, for example in the form of graduated verbal statements (e.g. “audited with some reservations”, “audited with observations”, etc.) would be beneficial for providing more value to the intended users of the audit. A more nuanced audit opinion would provide additional information to the users by exposing areas of concern or highlighting needs for improvement. Importantly, the current binary nature of the audit opinion potentially limits the opportunities to expand and change the scope of the audit, as many non-financial areas of business operation do not lend themselves to binary assessments.

DCMS advocates for a consideration of risk management as part of the audit process. As a result of the importance placed on financial experience in the audit and risk committee, it is common for organisations to apply a financial and binary approach to risk management, whilst security and cyber risks specifically would perhaps benefit from more nuanced, judgement based decision making.[21] In contrast to financial investments, the appropriateness of internal controls in light of a given risk exposure requires a more in-depth assessment by auditors and a meaningful opinion would need to incorporate an indication of why and to what extent the auditor has assessed the company to have taken informed and proportionate steps to mitigate their risks. This currently occurs in more in-depth process audits but process audits can be more subjective, time consuming and require a broader skill set than that currently held by the general audit profession.

Risk management, including the identification, assessment and treatment of risk, is often subjective and judgement-based. Whilst business approaches to risk management mature, there may be a need for binary approaches, in particular in emerging areas of risk. However, as explained above, the longer term ambition should be to expand the binary audit opinion to provide further insights into the maturity of the organisation in operating their business, including how they manage their risk.

In order to aid the work of auditors in arriving at a more nuanced audit opinion, a standardised framework that provides guidance around how companies should be assessed against their ability to proportionately and appropriately manage their risk(s), would enable a harmonised approach across industry.

26) Could further narrative be disclosed alongside the opinion to provide more informative insights?

A change to the current binary nature of audit opinions could take different forms and there are benefits and risks associated with each option. Adding a further narrative to the opinion would provide auditors with the opportunity to highlight any concerns that may have been raised during the audit process and to include further information for the intended users of the audit in the narrative. A narrative may further open up the audit opinion to questions and different interpretations. For example, if any concerns are raised in the narrative, this may give rise to users questioning the validity of the positive audit outcome.

However, introducing narratives alongside the binary audit opinions may introduce problems and comes with associated risks. Without mandating clearly defined content and scope of information provided in the narrative, it can be an ineffective tool and enable a less than transparent disclosure of information, as has been commented on recently with regard to viability statements.

As such DCMS does not recommend this approach be taken, but rather, that a non-binary approach to the audit process and reporting of its outcome be adopted in the form of a more graduated audit opinion as explained above. This would necessarily include further information and qualitative

[21] Institute of Risk Management, ‘Cyber risk: resources for practitioners’, https://www.theirm.org/media/3814330/IRM-Cyber-Risk-Resources-for-Practitioners.pdf, 2014.

judgements regarding specific observations or concerns. DCMS is in favour of considering a switch from the binary nature of the current audit process in order to cover assurance of an entity's risk management, however, the benefits and risks associated with potential approaches to this need to be carefully evaluated and mitigating measures should be put in place if such change was to be mandated.