# Section 4: Audit, risk and internal control

The primary client of a company's auditor is the shareholder. Investors rely on a high-quality audit, where the auditors are fully independent and have exercised professional scepticism and judgement, to enable them to form a clear and accurate view of the financial health of the company.

Individual accountability here is key: if a named partner, or the chair of an audit committee, has been involved in presiding over poor audit practices elsewhere, then investors should expect that the individual is not involved on an audit committee or involved in the audit at or of another firm.

In 2021, the UK Government launched a major consultation on audit reform,[1] bringing together the recommendations of the Kingman Review,[2] the Competition and Markets Authority statutory audit market study,[3] and the Brydon Review.[4]

Recommendations from the Brydon Review, that investors may wish to consider, include:

- For the directors' risk report to be published in good time for shareholders to comment, as well as for a formal invitation to be issued to shareholders to express any requests regarding where they would be particularly keen for an auditor to focus on in the audit plan.
- A standing item to be added to AGM agendas for questions to the chair of the audit committee and to the auditor.

Though the Government had committed in the 2022 Queen's Speech[5] to bring forward an Audit Reform Bill, this legislation was not included in the 2023 King's Speech. The new Government's King's Speech[6] in July 2024 did however announce

---

[1] Department for Business, Energy and Industrial Strategy, 2021, Restoring trust in audit and corporate governance – Consultation on the government's proposals, Restoring trust in audit and corporate governance (publishing.service.gov.uk)

[2] Sir John Kingman, 2018, Independent Review of the Financial Reporting Council, Department for Business and Trade, Financial Reporting Council and Department for Business, Energy & Industrial Strategy, Independent Review of the Financial Reporting Council (publishing.service.gov.uk)

[3] Department for Business, Energy & Industrial Strategy, 2019, Market study on statutory audit services: summary of responses, Market study on statutory audit services: summary of responses to the 2019 consultation (publishing.service.gov.uk)

[4] Sir Donald Brydon, 2019. Assess, assure and inform: improving audit quality and effectiveness – final report of the independent review, Department for Business and Trade and Department for Business, Energy & Industrial Strategy, Independent Review into the Quality and Effectiveness of Audit (publishing.service.gov.uk)

[5] Prime Minister's Office, 2022, The Queen's Speech 2022, Lobby Pack (10 May 2022) (publishing.service.gov.uk)

[6] Prime Minister's Office, 2024, The King's Speech 2024, https://www.gov.uk/government/speeches/the-kings-speech-2024

a draft Audit Reform and Corporate Governance Bill. The draft bill recognises that robust and rigorous scrutiny of large companies by auditors, along with greater transparency around their finances, is essential for ensuring accurate information about the health of companies and a more secure economy. The UK plans to replace the Financial Reporting Council (FRC) with a new regulator, the Audit, Reporting and Governance Authority, which will have the powers needed to address poor financial reporting and build trust. The new regulator will have a wider remit, including extending oversight to larger private companies, removing unnecessary rules for smaller businesses, sanctioning directors for financial reporting failures, and overseeing the audit market to protect against conflicts of interest.

However, the Government has now confirmed that the Audit Reform and Corporate Governance Bill will not be brought forward in this parliamentary session. Investors should be aware that, when introduced, the Bill is expected to have significant implications for oversight, accountability, and audit market regulation. The delay reinforces the importance of investor scrutiny in the absence of legislative reform.

In May 2023, the FRC published its Minimum Standards for Audit Committees.[7] The goal of these standards is to enhance performance and ensure a consistent approach across audit committees within the FTSE 350, while the FRC aims to support the delivery of high-quality audits and reinforce public trust in the financial reporting process.

The minimum standards are referenced as part of the UK Corporate Governance Code, specifically in Provisions 25 and 26. These provisions outline the main roles and responsibilities of the audit committee and the annual report disclosures on the work of the audit committee. Given that the text included in the minimum standard was duplicative with the 2018 Code, the FRC removed the repeated wording in the 2024 Code to avoid further duplication. The changes to the FCA listing rules, including the removal of the premium listing category, do not impact these standards.

The 2024 Corporate Governance Code[8] has now embedded across FTSE 350 companies, with early implementation revealing varied approaches to audit committee disclosures and risk oversight. Investors should assess how companies

[7] Financial Reporting Council, 2023, Audit Committees and the External Audit: Minimum Standard, https://media.frc.org.uk/documents/Audit_Committees_and_the_External_Audit_Minimum_Standard.pdf

[8] FRC, 2024, 2024 UK Corporate Governance Code, https://www.frc.org.uk/library/standards-codes-policy/corporate-governance/uk-corporate-governance-code/

are applying the revised provisions, particularly in relation to audit quality, resilience statements, and assurance policies.

Last year, shortly before the publication of our 2025 Stewardship and Voting Guidelines, Railpen published, with Governance Perspectives LTD., *Acting on Audit – an investor stewardship perspective*.[9] The purpose of the report was to highlight the importance of high-quality audits in reinforcing trust in financial reporting and strengthening corporate accountability. It examined the current state of audit quality, assessed investor engagement, and provided recommendations for improving audit practices.

The report aims to encourage system-wide changes by suggesting actions for companies, audit firms, regulators, and investors to collectively enhance audit quality. In the last year, we have seen the report help to spark renewed interest in audit committee transparency and investor access to audit-related information. Investors are encouraged to use the report's recommendations, including those on voting sanctions and AGM auditor engagement, as a benchmark for assessing audit committee performance and disclosure quality.

## The external auditor

The role of the external auditor is to provide an independent opinion of a set of financial statements to show whether these give a true and fair value of the company. There should be regular turnover in use of an external auditor to ensure that they remain impartial and are able to exercise professional scepticism.

## Risk and internal control

Risk management must be a prominent consideration at any company. In addition to an external audit, an effective, robust and well-resourced internal audit has a central role to play in supporting boards to better manage and mitigate the risks the company faces. Firms should focus on risk in the context of the business strategy, the firm's size and global footprint, as well as its assets, liabilities and the wider political and regulatory environment.

It is the internal auditor's task to provide an annual internal opinion on the state of the organisation's arrangements in relation to risk management, governance

[9] Railpen, 2024, Acting on Audit – An investor stewardship perspective, https://www.railpen.com/knowledge-hub/our-thinking/2024/acting-on-audit/

and internal control. This function may also include an advisory or consultancy function, where they support management in improving systems and controls.

## Cybersecurity and AI governance

The 2024–25 voting season has seen a marked increase in shareholder resolutions related to AI and cybersecurity governance, underscoring the urgency for investors to develop clear expectations around board oversight, responsible use frameworks and risk mitigation. Our guidelines have, and will continue to evolve, to reflect this trend.

## Cybersecurity

Cybersecurity risks are evolving rapidly and intensifying, driven by heightened geopolitical tensions that have made state-sponsored attacks, ransomware campaigns, and supply chain compromises more frequent and sophisticated. Critical sectors, such as pensions, face growing exposure as hostile actors seek to exploit vulnerabilities for disruption, espionage, and economic leverage.

These risks can arise not only from the technology itself but also from the people using it and the processes supporting it. It includes risks to information (data security) as well as assets, and both internal risks (for example, from staff) and external risks (such as hacking). Investors need to ensure that companies are managing these threats appropriately, by having governance and oversight structures in place and reporting on potential breaches and solutions.

Investors should encourage companies to explicitly disclose the governance and oversight structures in place to identify and manage these risks, as well as provide timely reporting of any breaches and the measures taken in response.

The 2024–25 period saw several high-profile cyberattacks across sectors, with material impacts on operations, customer trust, and share price. These incidents have highlighted how poor board oversight and weak internal controls can expose companies to significant financial and reputational risk. Investors should expect companies to disclose board-level responsibility for cyber risk, provide evidence of scenario planning and breach response protocols, and explain how cybersecurity is integrated into enterprise risk management.

A good source of information around how investors can positively and proactively engage was Railpen and Royal London Asset Management's *Cybersecurity Risk &*

*Resilience: Guidance for Investors*[10] report published earlier this year. It offered evidence-based insights on the financial impact and threat landscape of cyber risk, plus practical engagement guidance for investors.

The report shifts stewardship from reactive post-cyber-incident engagement to proactive resilience dialogue. It sets out expectations for assessing companies' baseline practices and progress toward best practice, structured around four pillars:

- Governance
- Supply chain & M&A
- Processes, culture & training
- Collaboration.

Cybersecurity should also be an active consideration when selecting a supplier and suitable provisions should be included in contracts. Investors should agree what metrics to use to monitor their suppliers, at a depth and frequency proportionate to their risk.

## Artificial intelligence (AI)

As we have outlined in previous iterations of our Guidelines, artificial intelligence (AI) is likely to be one of the biggest technological leaps in history. It is poised to unlock new business models, transform industries, reshape jobs, and boost economic productivity.

AI has the potential to change the investment landscape:

- Investors will place more value on the quality of a company's AI assets and capabilities.
- Investors themselves will rely far more on AI-based research techniques to support their investment approach.
- Investors will compete head-to-head with the technology sector for AI talent.
- AI has the potential to create entirely new fields of work that, at this stage, it is impossible to foresee.

Although AI has the potential to generate significant opportunities, it can also generate risks for businesses, including the amplification of discrimination,

[10] Railpen and Royal London Asset Management, 2025, Cybersecurity Risk & Resilience – guidance for investors, https://www.railpen.com/media/4itdafvg/railpen-cybersecurity-report-2025.pdf

proliferation of misinformation and privacy violations – particularly in relation to generative technologies – and additional cyber and data vulnerabilities.

Resolutions related to AI governance are increasing rapidly, reflecting investor concerns about deployment risks, bias, misinformation, and regulatory lag. Stewardship expectations vary depending on use case. For example, algorithmic trading requires different oversight than customer-facing AI tools. Investors should assess whether companies have board-level accountability for AI, disclose responsible use frameworks, and align with emerging standards on transparency and fairness.

Investors will need to consider the economic viability of AI which is uncertain due to the high costs involved in developing and maintaining AI systems, including expenses for research and development, specialised hardware, ongoing updates, and regulatory compliance. These significant financial costs create uncertainty about long-term profitability, as businesses may struggle to achieve sufficient returns on their investment.

Investors should also be aware that AI is evolving quickly, and comprehensive global governance frameworks are struggling to keep pace. This regulatory lag creates uncertainty around responsible standards, accountability, and oversight, potentially leading to inconsistent policies across regions. Without effective regulation, there is a risk of AI being deployed in ways that undermine privacy, exacerbate biases, or perpetuate inequalities.

In addition, AI is likely to be highly disruptive in the employment space, being poised to replace workers' jobs worldwide in the future. Indeed, some large technology companies are already starting to feel the heat from ESG-focused shareholders concerned about job losses due to AI, as well as the potential introduction of discrimination in employment decisions.

Investors should ensure that companies are accountable for their social impacts by aligning with evolving industry good practice in the AI space. It may be that AI and AI-enabled technologies will be subject to new standards and requirements in the future in order to promote safety, security and equity. Investors will need to ensure that companies are adhering to these standards and requirements.

Pensions UK has already worked with PWC to produce a Made Simple Guide[11] and will continue to engage heavily on the topic of AI to:

[11] Pensions UK, 2025, Artificial intelligence for UK pension schemes Made Simple, https://www.pensionsuk.org.uk/Policy-and-Research/Document-library/Artificial-intelligence-for-UK-pension-schemes-Made-Simple

- Support trustees
- Explore how AI impacts the responsibilities of trustees and the pensions industry more widely
- Consider in more detail the role of AI in investments.

## Evidence base

The key source of information provided by the auditor is the audit report. Investors should pay attention to the following information:

- Evidence of professional scepticism by the auditor
- The critical accounting policies and principles used
- The level of materiality adopted
- Assumptions and judgements
- The findings of any review undertaken by the FRC's Audit Quality Review Team (and actions taken by the board in response to the findings).

Investors, including pension schemes, also pursue a variety of voting sanctions on audit, including where:

- There are concerns about the company's financial policies and processes (vote against the audit committee chair)
- Previously identified material weaknesses have not been addressed, or disclosures are inadequate (vote against the audit committee chair)
- The audit firm's tenure is considered excessive (vote against the auditor and sometimes audit committee chair)
- There are considered to be excessive non-audit fees or other concerns about independence (vote against the auditor and sometimes the audit committee chair).[12]

Few investors are experts on audit assumptions and methodologies and there is an ongoing policy debate regarding to what extent investors can expect to be. The key determinant of a high-quality audit is professional scepticism and a willingness to challenge management.

Investors should be prepared to dig deeper and ask questions, including disclosure on areas where the auditor challenged management and the outcome, or even

[12] Railpen, 2024, Acting on Audit – An investor stewardship perspective, https://www.railpen.com/knowledge-hub/our-thinking/2024/acting-on-audit/

simply making a request that the auditor be present at the AGM to answer any questions and present their report.

On ESG metrics, it is desirable that the sustainability metrics provided by companies be assured and that the rationale for the choice of assurance provider (including whether external or internal) is made clear.

## What does good company behaviour look like?

Audit

- The audited accounts represent a 'true and fair' view of the state of affairs of the business. This should include its assets, liabilities, financial position and profit or loss – all of which should be prudently assessed to avoid overstating capital.
- The audit committee obtains a high-quality audit in the interests of shareholders, allowing for proper accountability between the audit company and the investors. This committee has arguably the most complex brief of any of the board committees, as objective and prudent accounts sit at the heart of an effective accountability regime.
- The audit committee demonstrates sufficient independence from company management. The committee should be staffed solely by independent directors (both from the executive but also taking into account independence from the external auditor) and enjoy sufficient relevant experience to carry out its responsibilities to a high standard.
    - The company should apply the FRC's Minimum Standards for Audit Committees[13] on a voluntary basis, including clear disclosures on auditor selection, independence safeguards, and audit quality indicators. Investors should expect meaningful commentary in the audit committee report, not repetition of the auditor's findings.
- The audit committee report provides 'colour' and detail. This should not simply mirror the auditor's report. It should include the right quality and amount of information to give investors an insight into the audit process, including:
    - Explicit details of the criteria used for auditor selection and evaluation, including any contractual obligations to appoint audit firms.

[13] FRC, 2023, FRC publishes minimum standard for audit committees, https://www.frc.org.uk/news-and-events/news/2023/05/frc-publishes-minimum-standard-for-audit-committees/

        - Details of the audit tender process, including when the audit was last tendered and how the company ensures independence is safeguarded.
    - How the audit committee satisfied itself that it got the highest quality audit possible.
        - Any changes to the process and plan of the audit (and reasons for these changes), including any changes to the audit partner and the process carried out by the audit committee to agree this appointment.
    - The audit tendering process is in line with regulations[14] and has been rigorous. Any tendering process should enable the audit committee to compare the quality and effectiveness of the services provided by the incumbent audit with other audit firms – including those outside the Big Four. The intention to tender the audit contract should be disclosed in advance within the report and accounts and the process should focus on audit quality – not costs – including the auditors' independence and processes to ensure professional scepticism.
- The audit committee fully discloses any members' connections with the current or potential auditor. Committee members should also have recent and relevant financial experience related to audit, accountancy or investor practitioner expertise.
- Additional disclosures clearly cover any reasons for any auditor resignations and fully detail all non-audit fees and policy on non-audit work. Where the auditors supply non-audit services to the company, the audit committee should keep the nature and extent of such services under regular and closer review, to ensure objectivity is not compromised. Disclosure of non-audit fees should include:
    - Clear breakdown between the types of services received
    - Tax compliance services are differentiated from tax advisory services
    - Non-statutory acquisition-related services are separated from statutory services.
- Appropriate use is made of third parties for non-audit services (including outside the Big Four). Where the company also uses its auditors for non-audit work, the rationale must be clearly explained. No more than 50% of the audit fee should be spent on non-audit services.
- The AGM includes a presentation from the auditor. This happens increasingly rarely, but Pensions UK would be keen for this to take place more frequently. Such appearances would give investors the opportunity to directly ask questions and hopefully raise the profile of audit issues.

[14]The Stationary Office, The Statutory Auditors and Third Country Auditors Regulations 2016, 2016, The Statutory Auditors and Third Country Auditors Regulations 2016 (legislation.gov.uk)

- The company is looking to apply on a voluntary basis the FRC's Audit Committees and External Audit: Minimum Standard.
- The audit committee requests that the auditor includes graduated findings in their reports, providing a nuanced view of key management estimates and judgments.
- The audit committee could ensure that engagement-level audit quality indicators (AQIs) are published or shared with investors upon request.
- The company should prepare a resilience statement and an audit and assurance policy, sharing these documents with shareholders.
- The audit committee should agree to meet with shareholders upon reasonable request to discuss audit-related issues and the company should encourage its auditors to hold at least one investor roundtable each year.
    - The company should support the publication of the names of companies and additional information when reporting on audit quality inspections.[15]

Risk and internal control

- The annual report covers the key elements of the business. It should explain how the company generates value from its key tangible and intangible assets. It should set out the how the board establishes and maintains an effective risk management and internal control framework – including ESG and reputational risks.
- The annual report covers emerging risks, demonstrating a dynamic approach to risk assessment. This could include risks from climate and cybersecurity, or tax management (and the potential impact on reputation and brand value). The company should be communicating what changes have occurred in relation to their risks over the previous year, how it has chosen to respond and the impact so far – including likely impact on the overall business strategy and model.
- Directors state whether they expect the company to meet its liabilities as they fall due over the period of their assessment. This should include drawing attention to any qualifications or assumptions as necessary. This should be as part of an articulation as to whether they have a reasonable expectation that the company will remain a viable and sustainable enterprise for the foreseeable future.
- Directors articulate their reasons for choosing a specific timeframe. This should follow the FRC's guidance that the length of the period should take account of the board's stewardship responsibilities, previous statements

[15] Railpen, Acting on Audit – An investor stewardship perspective, 2024, https://www.railpen.com/knowledge-hub/our-thinking/2024/acting-on-audit/

they have made, especially in raising capital, the nature of the business and its stage of development.

Cybersecurity and AI

- The company has identified its cybersecurity vulnerabilities - including any that arise from the use and integration of AI - and has robust policies and procedures in place in case of a cyber-attack.
- The company has a cybersecurity training policy in place for employees and has adopted best practices to enhance network and device security. The company should extend cybersecurity training and best practices for employees to include AI as appropriate.
- The company has implemented robust data anonymisation techniques when using AI, which allows businesses to protect data privacy.
- The company takes a zero-trust approach when selecting AI tools and third-party services, by vetting them against corporate privacy and security policies, to ensure the business is not being exposed to risk and vulnerabilities.
- The company could have, or be considering, cyber insurance as well as options for legal, technical and PR support. Several high profile cyber-attacks in 2024-25, including ransomware incidents and data breaches, have materially disrupted business operations, damaged reputations, and triggered regulatory investigations. These events have highlighted how oversight failures, including lack of board-level accountability and inadequate risk planning, can expose companies to significant financial and strategic risk. Increasingly, investors should expect companies to embed cybersecurity into their broader governance and resilience strategies. This includes:
    - Assigning board-level responsibility for cyber risk
    - Conducting regular stress tests and scenario planning
    - Disclosing how cyber risks are monitored, mitigated, and integrated into enterprise risk frameworks
    - Reporting on lessons learned from past incidents and how these have informed improvements in controls and oversight
    - Appointing a Chief Information Security Officer, or equivalent, with supporting resources
    - Evaluating cybersecurity and AI skills in board effectiveness reviews
    - Conducting effective due diligence and monitoring of supply chain cybersecurity
    - Including cyber considerations in inorganic growth strategies, including the due diligence and integration phases
    - Maintaining relevant cyber certifications or holding an independent audit report (e.g. aligned with NIST and ISO 27001 standards).

- Specifically related to AI, stewardship expectations should be tailored to the specific use of AI within a company. For instance:
    - Customer engagement tools raise concerns around bias, misinformation, and data privacy
    - Algorithmic trading systems require scrutiny of model transparency, risk controls, and regulatory compliance
    - Operational AI, such as predictive maintenance or supply chain optimisation, may pose risks around resilience and accountability.
- Investors should assess whether boards understand these distinctions and have governance structures appropriate to each use case. This includes board-level responsibility, responsible use frameworks, and alignment with emerging standards on transparency, fairness, and safety.

Voting decisions should reflect the materiality of the risk, the company's exposure, and the adequacy of its response. We are clear that where companies fail to demonstrate adequate governance of AI or cybersecurity risks, or where there is evidence of egregious conduct (particularly in high-impact sectors), investors should consider voting against the annual report and accounts, the audit committee chair, or relevant directors. For completeness, we have outlined below what could be perceived as egregious behaviour that may warrant voting action:

- Lack of transparency & governance: Failure to disclose how AI systems make decisions, what data they are trained on, or known incidents of harm, bias, or breaches. Deploying models without adequate governance, responsible safeguards, or risk controls.
- Algorithmic bias & discrimination: Ignoring known risks of bias in training data and failing to implement processes to detect and mitigate discriminatory outcomes, especially in sensitive areas like hiring, healthcare, or credit scoring.
- Cybersecurity & data privacy failures: Scraping personal data without consent, deploying insecure models, neglecting encryption or incident response planning, and failing to disclose breaches or vulnerabilities.
- Intellectual property infringement: Using copyrighted or confidential material without permission, allowing outputs that replicate protected works, and lacking processes to audit and remove infringing content.
- Environmental negligence & misrepresentation: Making no effort to reduce AI's energy and water footprint or offset emissions and engaging in 'AI washing' by exaggerating AI capabilities to mislead investors.

## How investors should consider voting

Investors should note that in most cases, but not always, there are separate resolutions which cover the appointment of external auditors and the setting, or authorisation of the board to set, auditors' fees. This is important because investors may have concerns about the balance between audit and non-audit fees, which need to be considered separately to the appointment of the auditor alone.

There are a range of resolutions that investors might use as a vehicle to express concerns regarding audit process or outcomes. These include: the vote to appoint or reappoint the auditor; the vote to give directors power to agree the auditor's fee; the vote to approve the report and accounts; or the election of the chair (or other members) of the audit committee. More information on different examples of investors' audit voting approaches can be found in Railpen's latest report (page 22).[16]

Investors should consider voting against the annual report and accounts and perhaps also the auditor and/or audit committee chair if there are ongoing concerns in relation to:

- The audited accounts fail to provide a true and fair view of profit or loss, assets or liabilities (for example, they overstate profit or assets or understate likely liabilities such as pension or climate-related liabilities). Please note: if the auditor is seen to have helped reveal this issue, then their re-election, all other things being equal, should be strongly supported.
- The ongoing use of alternative performance measures to report on business performance where their use is not transparent and fully justified or appears to flatter management delivery through unclear use of generally accepted accounting principles or regularly changing calculations.
- There is poor disclosure of the strategy and risk exposures or a lack of disclosed review of the company's risk management and internal control systems.
- There is either no viability statement which looks multiple years ahead, or one which does not evidently consider a full range of risk factors.
- The climate change assumptions that underlie calculations of relevant and publicly stated asset valuations or business profits are not sufficiently transparent or appear to be inconsistent with science and expert opinions on climate change.
- The company has not demonstrated that cybersecurity risks are sufficiently well governed or managed.

[16] Railpen, 2024, Acting on Audit – An investor stewardship perspective (page 22), https://www.railpen.com/knowledge-hub/our-thinking/2024/acting-on-audit/

- The company has experienced a material cyber breach and failed to disclose lessons learned or governance improvements.

Investors should consider voting against the re-election of the chair of the audit committee and reappointment of the auditor if:

- The tenure of an external auditor extends beyond ten years and there has not been a recent tender process and where no plans to put the audit service out to tender are disclosed.
- The auditor has been in place for more than 15 years.
- The non-audit fees exceed 50% of the audit fees in consecutive years without an adequate explanation being provided.
- There are major concerns regarding the audit process and quality of accounts – particularly a failure to provide a true and fair view (or good visibility over the payment of dividends) and these are not resolved satisfactorily by the board.
- Cybersecurity risks (or any breach responses) are not being sufficiently well managed.

Investors should consider voting against authorisation of auditor's remuneration (or the reappointment of the auditor if these resolutions are bundled) if:

- The auditor's report fails to address a key issue or is otherwise unsatisfactory.
- Audit fees have been either increased or reduced by a significant proportion (e.g. more than 20%) in a given year without a clear justification.
- Resolutions are bundled (e.g. auditor reappointment and fee authorisation), and there are concerns about either component, investors should consider voting against the bundled resolution and request future separation for transparency.

Investors should consider voting against the re-election of the chair if:

- There are extreme concerns or persistently poor disclosure in regard to the sufficient auditing of the company.

Investors should consider voting against the re-election of a director (including re-election of the chair) if:

- AI is deployed in high-risk areas and the company fails to disclose governance structures, responsible safeguards, or board-level accountability.
- There is evidence of egregious conduct attributable to a particular director around the development and deployment of AI.
- Companies are failing to act on AI proportionate to risk exposure, business model and potential impacts, focusing on the key pillars of board accountability, risk management and transparency.

# Disclaimer



This material provided is meant as general information on matters of interest and is not intended as accounting, financial, legal or any other professional advice. You should speak to your professional advisers for advice.

The publisher cannot accept responsibility for any errors in this publication or accept responsibility for any losses suffered by anyone who acts or fails to act as a result of any information given in this publication.