ACCIF – internal controls working group

Position paper – feedback draft 20 08 20

Background

The case for considering the introduction in the UK of an enhanced framework over internal financial reporting controls was first suggested by Sir John Kingman in his Independent Review of the Financial Reporting Council:

> *"BEIS should give serious consideration to the case for a strengthened framework around internal controls in the UK, learning any relevant lessons from operation of the Sarbanes-Oxley regime in the US. The pros and cons of options for change should be analysed and consulted upon, giving special consideration to the importance of proportionality in relation to the size of the company."*

In his review of the quality and effectiveness of audit, Sir Donald Brydon acknowledged that the effectiveness of internal controls is clearly of great relevance to the reliability of a company's financial (and potentially other) reporting and he put forward a recommendation for directors to report more meaningfully on their internal controls:

> *"The CEO and CFO provide an annual attestation to the board of directors as to the effectiveness of the company's internal controls over financial reporting and that this attestation be guided by new principles on internal controls reporting to be developed by the Audit Committee Chairs Independent Forum and endorsed by ARGA."*

The recommendation was carefully constructed not to disrupt the UK unitary board concept and so the CEO and CFO's attestation is proposed to be made to the board with the board then providing a report to shareholders that it has received such an attestation.

On the basis that shareholders and other stakeholders are relying on the judgment of the company's directors, Sir Donald was keen that ACCIF should develop principles that should be followed by CEOs and CFOs in making an internal controls effectiveness attestation which he suggested should be based on a UK customised version of the Internal Control – Integrated Framework (2013) issued by the Committee of Sponsoring Organisations of the Treadway Commission in the United States (COSO).

ACCIF's objectives

As Audit Committee Chairs we are supportive of this focus on raising the bar on the effectiveness of internal control systems and in particular internal controls over financial reporting.

On the basis that Sir Donald has confirmed that his recommendation is aimed at internal controls over financial reporting, we are focusing our principles on this area of controls noting that Provision 29 of the UK Corporate Governance Code currently states that:

"The monitoring and review should cover all material controls, including financial, operational and compliance controls."

We support Sir Donald's focus on internal controls over financial reporting on the grounds that these principles are to be the basis on which the attestation is provided and agree that controls over financial reporting can be appropriately "ring-fenced" to make any attestation meaningful and practical. Boards will, of course, still need to undertake their responsibilities on wider controls in accordance with the UK Corporate Governance Code. Clear accountability amongst the key executive directors with responsibility for financial reporting with supporting disclosure owned by the full board should drive more robust behaviours which should provide greater comfort on the baseline of the company's position.

In developing these principles, we have sought to meet the following criteria and to develop a framework which:

- builds on existing UK practice rather than adopting an overseas framework which is not familiar in UK;
- is capable of being applied proportionately and of being embedded in the business;
- is achievable without a huge practical burden of implementation and reporting resulting in an effective balance between cost of implementation and ongoing monitoring and the benefit which arises from that; and
- avoids being duplicative - where an organisation already applies a framework such as Sarbanes-Oxley, Spanish ICFR or Japanese SOx there should be no additional requirements.

Overview of current requirements in the UK

In undertaking this exercise, we have considered a number of different sources of requirements within the UK governance framework:

- Duty to keep adequate accounting records – Companies Act 2006
- Financial position and prospects procedures – the Listing Rules
- The UK Corporate Governance Code and supporting guidance
- The Disclosure & Transparency Rules (DTR 7.2.5R)

See **Appendix A** for an overview of the current ICFR requirements in the US, Spain and Japan.

Our proposal

The aim has been to address Sir Donald Brydon's proposal and to obtain the majority of the benefits of a Sarbanes-Oxley type attestation without all the corresponding costs. Our review has led us to conclude that the existing 'Financial Position and Prospects' (FPP) procedures requirements from the Listing Rule 8.4.2(4) could be an appropriate and effective way of doing this. This is a requirement with which premium listed entities will already have complied on listing, so should be familiar. Whilst it is likely that, for many listed companies, IPO was some time ago, the Listing Rule does include reference to maintaining procedures on an "ongoing basis".

Our proposal is that the CEO/CFO attestation to the board for this purpose should focus on the financial position aspects of FPP. We believe that the financial position element of this regulatory requirement is the area to focus on as this requires that the directors must already have established procedures that enable them to be informed on a regular basis as to the financial position of the applicant and its group, including assets and liabilities, profits and losses.

In addition, our proposal is that this consideration of financial position should be extended to cover the statement of cash flows (as reported under IFRS), in addition to assets, liabilities, profits and losses, to ensure that all primary financial statements are covered.

Under Listing Rule 8.4.2(4) directors of a company that is seeking a Premium Listing of its shares on the Main Market of the London Stock Exchange have to have established procedures that provide a reasonable basis for them to make proper judgements on an ongoing basis as to the financial position and prospects of the applicant and its group.

The three key elements of directors' responsibilities in relation to these financial position procedures are to:

- accept responsibility for the procedures;
- ascertain whether they have established appropriate procedures at the time of the application for listing; and
- obtain sufficient evidence that they have established the necessary procedures and document the procedures.

It is important to note that, in addition to their obligations at the date of admission, directors are also responsible for maintaining the procedures subsequently. It is this latter responsibility that leads us to our proposed choice for the UK attestation and implies that the attestation should be both about design and operating effectiveness.

The onus is on directors to determine the most suitable procedures. We suggest these should derive from consideration of the nature and circumstances of the entity, a risk assessment of the factors that are most likely to impact the entity's financial position[1] and identification of the procedures needed to address those factors. In this way the procedures adopted by an entity can be flexible and proportionate regardless of where a company sits in the FTSE and in what industry they operate.

Procedures need to be developed by the directors according to the nature of the company and the results of the risk assessment. There are a small number of recognised frameworks available including COSO's Internal Control over External Financial Reporting framework which is widely used by companies under the Sarbanes-Oxley regime.

In addition, the ICAEW issued guidance for reporting accountants on FPP which includes illustrative objectives for the procedures which may be capable of being adapted by the company.

These frameworks are not intended to be exhaustive or prescriptive examples but can provide a useful initial basis for consideration of the procedures that may need to be in place in individual cases.

Clearly, directors also have responsibility for ensuring that an organisation's culture promotes a strong control environment and that the finance function, in particular, has the requisite skills and experience to be able to deliver accurate and timely financial reporting. We also acknowledge that any framework may need to take into account any new regulatory requirements regarding directors' responsibilities in respect of fraud as currently being considered in response to the Brydon review, if this is not addressed separately.

[1] As extended to included cash flows in addition to assets, liabilities, profits and losses

COSO's Internal Control over External Financial Reporting framework is set out under the following sections:

Control Environment - the set of standards, processes and structures that provide the basis for carrying out internal control across the organisation.

Risk Assessment – risk is defined as the possibility that an event will occur and adversely affect the achievement of objectives. Risk assessment involves a dynamic and iterative process for identifying and assessing risks to the achievement of objectives.

Control Activities - the actions established through policies and procedures that help ensure that management's directives to mitigate risks to the achievement of objectives are carried out.

Information and communication – management obtains or generates and uses relevant and quality information from both internal and external sources to support the functioning of internal control. Communication is the continual, iterative process of providing, sharing and obtaining necessary information.

Monitoring activities – ongoing evaluations, separate evaluations, or some combination of the two are used to ascertain whether each of the components of internal control, including controls to effect the principles within each component, is present and functioning.

See **Appendix B** for the full set of COSO framework principles and **Appendix C** for other illustrative objectives.

Our view is that focusing a CEO/CFO attestation on the establishment of procedures and controls over financial position only (albeit adapted as described above to cover cash flows also) is a proportionate and effective way of directing resource and attention to the most important area. This view is further reinforced by analysis which we have done on the most common material weaknesses reported by those companies within the Sarbanes-Oxley regime (see **Appendix D**). This supports the view that it is controls around information on financial position which should be the focus including those significant elements of control which are embedded in an entity's IT environment.

Appendix E sets out proposed wording for board approval which could be considered in developing the CEO/CFO attestation suggested by Sir Donald Brydon.

Rebuttable presumptions we have incorporated:

- The CEO/CFO attestation should cover both design and operational effectiveness.

- For these purposes, "financial position" covered in the CEO/CFO attestation covers the assets and liabilities, profits and losses and cash flows as set out in the primary financial statements. The attestation does not extend specifically to reporting in the notes to the financial statements.

- We do not reference the director's existing responsibilities under the Companies Act 2006 on adequacy of accounting records in the attestation as this is already covered explicitly in the directors' responsibilities statement.

- Where a company already provides an attestation on internal controls over financial reporting under a recognised regime such as Sarbanes-Oxley, no incremental requirements apply.

- The decision on whether the attestation is subject to further assurance should be made by the audit committee. To the extent that parts of their audit are controls based rather than substantive, it may be possible for the auditors to leverage their controls testing to provide some external assurance over the CEO/CFO attestation, should they be commissioned to do so.

Questions on which we would welcome your views:

1. To which groups of companies should this be applied (options: FTSE100, FTSE350, all premium listed and AIM or all PIEs (but in all cases attestation should only need to be made by UK TopCos)? Please provide the rationale for your recommendation.

2. Do you agree that this approach is capable of being applied in a proportionate manner or would some listed companies find it too inflexible or too much of a burden? If you believe that it would be too inflexible or too much of a burden, please advise why and what you would propose to address this risk.

3. What are your views on the wording of the proposed attestation to be provided by the CEO/CFO to the board as set out in Appendix E?

4. How should we develop a UK guidance framework for the procedures, potentially drawing on elements of existing recognised frameworks, such that it can be considered for approval by the FRC as guidance for CEO/CFO as attesters plus the audit committee who would have oversight of it? (We are aware that the FRC would be unable to approve the existing ICAEW framework as they oversee the ICAEW, which would create a conflict of interest)

5. Is there appetite to consider a phase two of this project to extend to wider controls beyond those over financial reporting? This could, for example, include (i) budgeting and forecasting, and by extension, consideration of financial prospects, going concern and longer term resilience; (ii) fraud prevention and detection; (iii) wider operational and compliance controls.

Matters for specific consideration by the FRC and BEIS:

- Could auditors be permitted to provide assurance over the attestation, if requested, by including this service in the list of permitted services under the new Ethical Standard, recognising that it would nevertheless count as a non-audit service? It needs to be recognised that if it were to be permitted, this could make compliance with the cap challenging for some entities and this may lead to more requests to the FRC for approval of a cap waiver.

- In light of the current circumstances, what is the most appropriate timing for further consultation on this?

APPENDIX A

Overview of the current ICFR requirements in the US, Spain and Japan

High-level overview of the US requirements – s404 of the Sarbanes-Oxley Act

Each issuer is required to include an internal control report that contains management's assertions regarding the effectiveness of the company's internal control structure and procedures over financial reporting. The report must articulate the following:

- management's responsibilities to establish and maintain adequate internal control over the financial reporting for the company;
- the framework used by management to provide criteria for evaluators to assess the effectiveness of the company's internal control over financial reporting; and
- management's assessment as to the effectiveness of the company's internal control over financial reporting based on management's evaluation of it at year end, including disclosure of any material weakness in the company's internal controls over financial reporting identified by management.

For larger companies, Section 404 also requires the company's independent auditor to attest to the effectiveness of the company's internal control over financial reporting in accordance with standards established by PCAOB.

High-level overview of the Spanish requirements

In Spain public companies are required to describe the mechanisms that comprise the risk control and management systems in relation to internal control over financial reporting in the company in their Annual Corporate Governance Report. The report must describe:

- The main features company’s control environment
- An assessment of risks in relation to financial information
- Control activities
- Information and reporting
- Supervision of system operation

If the ICFR information supplied to the market has been reviewed by the external auditor, the corresponding report should be attached. If this is not the case, the report should explain why.

High-level overview of the Japanese requirements

Since April 2008, Japanese listed companies have been required to produce “internal control reports” along with their annual financial statements, to demonstrate the soundness of their financial practices.

A company representative is required to evaluate the effectiveness of the internal controls and submit a written statement attesting to the accuracy of the financial statement.

Both the financial statement and internal control reports have to be approved by the external auditors.

If either the representative or the auditor judges the firm's internal controls inadequate and likely to result in major errors in the financial statement, the company will be required to report that its internal controls are flawed.

APPENDIX B

The principles set out in each component of COSO's Internal Control over External

Financial Reporting framework Control Environment

- The organisation demonstrates a commitment to integrity and ethical values.
- The board of directors demonstrates independence from management and exercises oversight for the development and performance of internal control.
- Management establishes, with board oversight, structures, reporting lines and appropriate authorities and responsibilities in the pursuit of objectives.
- The organisation demonstrates a commitment to attract, develop and retain competent individuals in alignment with the objectives.
- The organisation holds individuals accountable for their internal control responsibilities.

Risk Assessment

- The organisation specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives.
- The organisation identifies risks to the achievement of its objectives across the entity and analyses risks as a basis for determining how the risks should be managed.
- The organisation considers the potential for fraud in assessing risks to the achievement of objectives.
- The organisation identifies and assesses changes that could significantly impact the system of internal control.

Control activities

- The organisation selects and develops control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels.
- The organisation selects and develops general control activities over technology to support the achievement of objectives.
- The organisation deploys control activities through policies that establish what is expected and in procedures that put policies into action.

Information and Communication

- The organisation obtains or generates and uses relevant, quality information to support the functioning of internal control.

- The organisation internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.

- The organisation communicates with external parties regarding matters affecting the functioning of internal control.

Monitoring activities

- The organisation selects, develops and performs ongoing and/or separate evaluations to ascertain whether the components of internal control are present and functioning.

- The organisation evaluates and communicates internal control deficiencies in a timely manner to those parties responsible for taking corrective action, including senior management and the board of directors as appropriate.

APPENDIX C

Guidance on Financial Position and Prospects Procedures

A. Risk assessment of FPP

The company has established procedures that operate, or are capable of operating, to:

- identify the information needed to monitor the business and manage risk so as to make proper judgements on FPP (FPP Information);
- identify, assess and document the risk factors likely to impact on:
  - financial position, prospects and any changes thereto; and
  - preparation and communication to the directors of related information;
- identify, assess in relation to FPP Information and consider risks including those relating to:
  - the high-level reporting environment (see section B);
  - forecasting and budgeting (see section C);
  - the management reporting framework (see section D);
  - significant transaction complexity, potential financial exposure or risk (see section E);
  - strategic projects and initiatives (see section F);
  - financial accounting and reporting (see section G); and
  - the IT environment (see section H).

B. High-level reporting environment

The company has established procedures that operate, or are capable of operating, to:

- identify and document the high-level reporting controls, governance and financial accounting procedures and IT controls over FPP Information;
- recruit board members with relevant and complementary skills, including financial skills, enabling:
  - the board to exercise oversight over reporting of, and assessment and use of, FPP Information; and
  - non-executive directors to provide robust challenge to management on FPP Information;
- assess the culture and management's operating style and ensure that these encourage effective control over reporting of FPP Information;
- organise the finance function with staffing levels, qualifications and capability commensurate to the accounting and reporting complexity and tax profile of the business;
- communicate board decisions on FPP Information to those responsible for implementing them;
- maintain risk processes and financial controls that have implications for FPP Information;
- determine authority levels for approval of activities which carry risk or significant accounting complexity;
- appraise, select and approve strategic projects and document decisions which may impact on FPP Information;
- provide clear financial reporting lines and accountability, with segregation of duties;
- maintain accounting records that are up to date and from which timely, reliable management information can be produced;

- enable the financial position on a statutory basis to be established and reconciled with the management accounts;
- collate FPP Information and report it to the board on a timely basis;
- enable whistleblowing and escalation of problems and concerns to senior management and to monitor how these are addressed;
- evaluate whether internal control over reporting of FPP Information is present and functioning;
- identify internal control deficiencies and communicate them in a timely manner to parties responsible for taking corrective action, and to management and the board as appropriate;
- respond in a timely way to points affecting FPP Information arising from external audit and, where applicable, internal audit and to monitor progress;
- enable internal audit, where applicable, to focus on factors that could affect FPP Information;
- identify, document and test recovery procedures and cover arrangements essential to producing FPP Information; and
- facilitate regular review and reassessment of the company's FPP procedures.

C. Forecasting and budgeting

The company has established procedures that operate, or are capable of operating, to:

- reflect key business risks in strategy and plans;
- determine and document budgeting and forecasting processes to meet the needs of the business, to reflect strategy and plans and to identify changes to its prospects;
- identify and monitor risks to achieving forecasts, in terms both of over- and under-performance;
- adopt a model for budgeting and forecasting that satisfies the needs of the business, including its plans for growth; involve staff in the preparation of budgets and forecasts with sufficient knowledge of the business and market and provide for input from those who will be charged with achieving them;
- distribute budgets and forecasts for review and approval by senior management and the board on a timely basis;
- compare management accounts against budgets and forecasts and analyse and explain positive and negative variances that are reviewed by senior management and the board on a timely basis; and
- adapt plans as necessary based on monitoring of progress against budget and forecast and organise resources and capabilities to implement changes.

D. Management reporting framework

The company has established procedures that operate, or are capable of operating, to:

- consider the nature of management information and KPIs required to monitor the business and inform the board about FPP;
- generate and report to senior management and the board timely and reliable information including material financial information and KPIs; and
- provide the board with timely information between periodic reporting dates about events with a material financial impact.

E. Significant transaction complexity, potential financial exposure or risk

The company has established procedures that operate, or are capable of operating, to:

- inform the board of the accounting, measurement and tax implications of transactions involving significant complexity;
- measure, record and report complex financial instruments and transactions involving such financial instruments on a timely basis;
- report to the board the extent of commitments and contingencies and potential financial liabilities and related taxation consequences, arising, for example, from pensions, lease commitments, leasehold dilapidations, litigation, onerous contracts, foreign currency, warranties and indemnities given, deferred consideration payable, environmental matters and future site rehabilitation costs;
- report to the board any exceptions to authority levels for such commitments and contingencies;
- scope and approve outsourced arrangements and monitor their performance;
- consider and act upon advice obtained from external experts in relation to FPP Information; and
- monitor compliance with covenants and legal and regulatory requirements and report exceptions to the board.

F. Strategic projects and initiatives

The company has established procedures that operate, or are capable of operating, to:

- carry out project planning, management and delivery through experienced staff or third-party experts with senior management oversight and upward reporting;
- determine and monitor budgets, KPIs, milestones or other benchmarks and provide regular and timely reports to the board;
- measure, account for and assess tax implications of strategic projects through experienced staff with senior management oversight;
- record transaction information relating to strategic projects in the right period;
- provide up to date reporting of strategic projects;
- measure and assess economic lives of assets, and support and document decisions for asset replacement; and
- scope and approve contractors and monitor their performance.

G. Financial accounting and reporting

The company has established procedures that operate, or are capable of operating, to:

- evaluate, determine, approve and document appropriate accounting policies that comply with applicable Generally Accepted Accounting Principles (GAAP);
- apply chosen accounting policies consistently;
- consider the impact of new financial reporting standards on a timely basis and determine, document and promptly communicate changes to accounting policies;
- identify, consider and disclose uncertainties and risks from applying chosen policies, including assumptions underpinning fair values and other key accounting assumptions as defined in relevant financial reporting standards; and
- document and assign responsibilities for external reporting obligations, monitor compliance with these and investigate and remedy delays.

H. IT environment

The company has established procedures that operate, or are capable of operating, to:

- align IT business and strategies and obtain board approval for planned use of IT for FPP Information;

- document the general features of key systems impacting inputs to and production of FPP Information;
- formally approve changes to the systems impacting inputs to and production of FPP Information;
- monitor reliability and maintenance standards of key systems impacting inputs to and production of FPP Information;
- support systems so that they are capable of producing accurate, useful and timely FPP Information;
- document, approve and communicate disaster recovery plans and procedures;
- periodically test disaster recovery plans, describe results and address matters arising;
- restrict physical access to IT networks, equipment, storage media and program documentation to authorised individuals;
- restrict logical access to IT systems, programs, master data, transaction data and parameters and to processing in web-based or web-enabled financial systems;
- document security arrangements and procedures for processing internet trading arrangements and online transactions to authorise and protect processing;
- identify, assess and manage risks of outsourcing to data integrity and governance; and
- determine requirements for outsourced systems and select and authorise suppliers.

Alignment of COSO and FPP (excluding section C which is around prospects)

COSO	ICAEW Guidance - FPP
Control Environment - the set of standards, processes and structures that provide the basis for carrying out internal control across the organisation.	**Section B** - High-level reporting environment
Risk Assessment – risk is defined as the possibility that an event will occur and adversely affect the achievement of objectives. Risk assessment involves a dynamic and iterative process for identifying and assessing risks to the achievement of objectives.	**Section A** - Risk assessment of FPP
Control Activities - the actions established through policies and procedures that help ensure that management's directives to mitigate risks to the achievement of objectives are carried out.	**Section D** - Management reporting framework **Section E** - Significant transaction complexity, potential financial exposure or risk **Section F** - Strategic projects and initiatives **Section H** - IT environment
Information and communication – management obtains or generates and uses relevant and quality information from both internal and external sources to support the functioning of internal control. Communication is the continual, iterative process of providing, sharing and obtaining necessary information.	**Section G** - Financial accounting and reporting
Monitoring activities – ongoing evaluations, separate evaluations, or some combination of the two are used to ascertain whether each of the components of internal control, including controls to effect the principles within each component, is present and functioning.	No equivalent in the guidance although the reporting does suggest that directors have to continue to maintain the procedures.

APPENDIX D

Some of the most common material weaknesses reported by those companies within the Sarbanes-Oxley regime

Ranking #	Material Weakness key theme
1	Accounting documentation, policy and/or procedures
2	Material and/or numerous auditor /YE adjustments
3	Accounting personnel resources, competency/training
4	Information technology, software, security & access issues
5	Segregations of duties/ design of controls (personnel)
6	Inadequate disclosure controls (timely, accuracy, completeness)
7	Non-routine transaction control issues
8	Restatement or non-reliance of company filings
9	Untimely or inadequate account reconciliations
10	Journal entry control issues
11	Restatement of previous 404 disclosures
12	Senior management competency, tone, reliability issues
13	Insufficient or non-existent internal audit function
14	Treasury Control Issues

Further information on each of these is available on the SEC's website.

APPENDIX E

Proposed attestation for the CEO and CFO to provide to the board

Board responsibilities

As directors of ABC plc we are all responsible for designing procedures and controls over financial reporting, and ensuring their operational effectiveness, that provide a reasonable basis for making proper judgements on an ongoing basis as to the financial position of ABC plc. For these purposes "financial position" includes assets and liabilities, profits and losses and cash flows.

CEO/CFO responsibilities

In discharging our responsibilities on behalf of the board we, the CEO and CFO, have conducted a risk assessment of the nature and circumstances of the business and:

- information needed to monitor the business and manage risk so as to make proper judgements on ABC plc's financial position; and
- factors likely to impact on ABC plc's financial position and the preparation and communication of related information.

Confirmation to the board

We confirm that we have established procedures and controls over financial reporting which provide a reasonable basis for us to make proper judgements as to the financial position of ABC plc[2] as at [date] having taken into account the [name of a recognised framework] .

[CEO or CFO]
[Date]

Signed on behalf of the CEO and CFO

---

[2] Amended appropriately to cover additional considerations for cash flows