Protecting stakeholders

Implementing ICFR in the UK

October 2020

EY
Building a better working world

Contents

Foreword

A holistic approach to support resilience and enhance integrity at times of crisis.

Hywel Ball
UK Chair and UK&I Regional Managing Partner

Businesses have been facing unprecedented challenges and disruption throughout the COVID-19 pandemic. The survival of many companies still hinges upon their ability to react at speed to changing influences, rapidly identify risks and mitigate their impact.

The pandemic presents nevertheless the opportunity to raise standards. In recent years, business leaders have been facing increasing pressures to run businesses in a more socially responsible way, considering effective opportunities for value creation. The current crisis is accelerating this trend, requiring boards to demonstrate that the public interest is integrated in the company's purpose, in order to deliver benefits to employees, customers, pensioners and wider society as well as to shareholders.

Now is the time to introduce constructive reforms, and embed cultural and operational changes to better equip businesses with the tools to respond to fluid and uncertain business environments; give stakeholders and regulators the opportunity to make timely interventions; and ensure companies' long-term survival.

Recent reviews into the audit market provide a crucial opportunity to respond to the breakdown in society's trust in business by strengthening the entire ecosystem for the longer term and introduce safeguards to mitigate future crises.

EY has long been an advocate for effective accountability of management and directors, including audit committees, as they are responsible for the accuracy of corporate information on which shareholders and stakeholders rely.

The introduction in the UK of a mandatory framework for ICFR – and potentially broader internal controls in future – would support both the innovation of audit to meet users' needs and expectations more effectively, and companies' response to fluid and uncertain business scenarios.

I hope this publication will be useful to policy makers and regulators while developing reform measures; to businesses in considering suitable approaches and readiness; and to investors to inform and strengthen their engagement with companies.

1 Background

In August 2019, we published a paper[1] contributing to the public debate around the introduction in the UK of an internal control accountability framework, leveraging certain aspects from the US Sarbanes-Oxley Act of 2002 (SOX or the 'Act').

Our paper followed the independent review of the Financial Reporting Council (FRC) led by Sir John Kingman[2], which concluded in December 2018 and recommended to give serious consideration to the case for a strengthened framework around internal controls within UK companies, learning relevant lessons from the US.

In December 2019, Sir Donald Brydon published his report into the future of auditing (the Report)[3], providing further impetus to the debate, elaborating on the importance and the mechanics of introducing stronger internal control measures and making specific recommendations. The Report takes an important stance on the risks in financial statements and recommends the introduction of mandatory internal control statements requirements on boards.

The ICAEW's latest essay on internal controls[4] reports on widespread stakeholders' agreement that "work is needed on the foundations for the review of internal control effectiveness that is already required in the UK. There is also agreement that the focus of this work needs to be on companies, rather than external auditors, and that greater clarity is needed about who is responsible for internal controls within companies".

Building on our August 2019 paper, and in light of the developments that followed, this paper provides additional considerations and further analysis and insights to support the development of a coherent internal controls framework for the UK market.

1 "Protecting Stakeholders – Enhancing internal control accountability in the UK", EY August 2019

2 https://www.gov.uk/government/news/independent-review-of-the-financial-reporting-council-frc-launches-report

3 https://www.gov.uk/government/publications/the-quality-and-effectiveness-of-audit-independent-review

4 https://www.icaew.com/technical/thought-leadership/audit-and-assurance-thought-leadership/internal-controls-reporting-sketching-out-the-options

2 A framework for ICFR

The UK is an important economy. It has long been regarded as a world leader in corporate governance and reporting, audit and accounting and regulatory oversight. The balance of high standards, proportionate legislative requirements and appropriate levels of flexibility have made it an attractive place to invest and do business.

Confidence of stakeholders, in the quality of business frameworks, is vital for the UK to retain its position in capital markets. But high-profile corporate failures over the past few years have raised alarms as to the effectiveness of existing frameworks. The subsequent Government reforms in corporate governance[5] and stewardship have sought to further strengthen the system and enhance accountability mechanisms as effective safeguards.

Following the 2018 corporate governance legislative measures, the Government has since embarked on wide-ranging reviews of the audit regulation, the audit profession and the future of audit, as elements of a comprehensive industrial strategy. The publication of a comprehensive package of consultations and proposed measures is expected in the coming months.

2.1. Reforming the corporate ecosystem

COVID-19 is continuing to increase systemic risks and impose huge disruption to businesses' operations. Moving forward will require a robust recovery plan, the success of which — particularly in the longer term — will heavily rely upon a holistic reform of the business ecosystem.

Comprehensive legislation, additional regulatory requirements and revised standards delivering audit reform, must be accompanied by decisive changes in corporate governance, reporting and accountability, ensuring oversight of all these by a strengthened regulator.

Crucially, a cohesive and balanced package of measures should give shareholders the right incentives and powers to exercise responsible stewardship. This package of measures will also ensure that each player in the business environment does its part and is accountable, including giving a broader range of stakeholders — employees, customers and wider society — greater insight on how companies are run.

2.2. ICFR in the UK and SOX

Strengthening the capital markets and the UK economy for the long term, will heavily rely on the successful implementation of the reforms currently being developed. Restoring stakeholders' confidence in business will require a strong focus on protecting the public interest.

EY has been consistently vocal about the need to include, in the wider audit reform objectives, particular focus on raising the bar on internal control effectiveness and accountability. Boards must be made to take responsibility for having appropriate systems and internal controls in place and be accountable for their effectiveness.

In terms of the extent of internal controls, we are of the view that it would be beneficial to introduce a requirement for companies — such as for management, on behalf of the board — to provide an attestation on all internal controls, using a recognised framework. This approach would be consistent with the UK Corporate Governance Code, and the statement boards already make on risk management and internal control systems.

However, this may prove too demanding for UK companies as they would need to have better evidence gathering mechanisms in place, more rigour and the agility of linking controls to risk mitigation. In alternative, and in addition to ICFR, consideration should be given to requiring an attestation to all internal controls at least for the principal risks or a subset of 'viability risks' even if for the medium term.

[5] https://www.legislation.gov.uk/uksi/2018/860/made

While we recognise that any reforms need to remain proportionate in the current challenging environment, we also think that it is this very environment that needs some key changes.

Immediate efforts and resources should concentrate on introducing a strong ICFR framework, ensuring boards and management are subject to scrutiny, accountable to an external party — whether the regulator or the external auditor or both — and required to provide evidence on a regular basis that the mechanism is designed and operating effectively.

While we agree with the aim of identifying an approach consistent with domestic frameworks, we nevertheless believe that there is merit in learning from experience in other jurisdictions.

Since its implementation in the United States, SOX has led to improvements in financial reporting (i.e., reduced number of restatements), strengthened the corporate governance requirements for listed companies (particularly with respect to audit committees), enhanced auditor independence (by prohibiting external auditors from providing certain non-audit services to audit clients) and increased investor confidence[6].

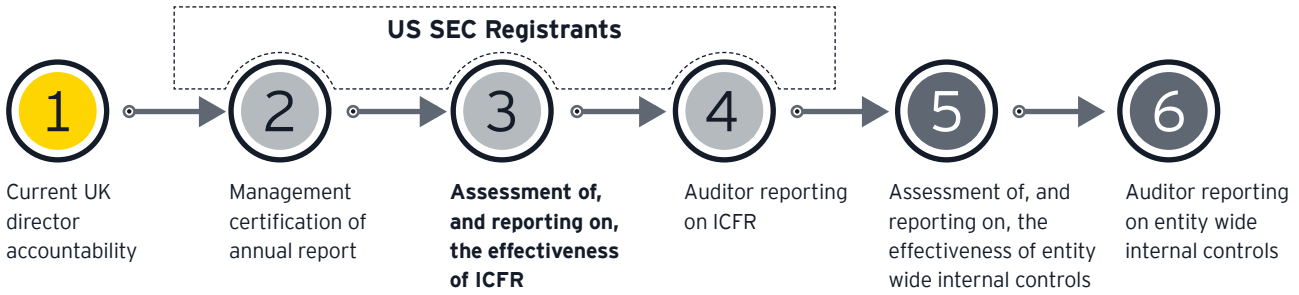
SOX provisions underline clearly that primary responsibility, for internal financial controls and the accuracy of financial reporting, rests with the management of a company. They require the CEO and CFO to gain a deeper understanding of their data and their business in order to anticipate or identify failures and take appropriate action to reduce business risk. SOX has increased the levels of trust and confidence in business, particularly where auditors provide some form of assurance.

Standards improved in the US after the introduction of the Sarbanes-Oxley Act in 2002, with restatements of financial statements now at the lowest level since 2006.

Our August 2019 paper considered an approach directionally aligned with that adopted in the US through SOX and set out six options for an enhanced internal control accountability framework in the UK (see box below).

Our recommendation from our August 2019 paper

The potential options in considering an enhanced internal control accountability framework in the UK include:



We recommend consideration be given to option 3 above: CEO and CFO certification of all disclosures in the annual report and accounts and management's assessment of, and reporting on, the effectiveness of ICFR.

We are advocating enhancements with respect to internal control accountability, in addition to the board's current responsibilities, not replacing or diminishing the board's accountability. The US experience demonstrates that the requirement for certifications will facilitate greater responsibility and focus by CEOs and CFOs to ensure that there are effective internal controls and accountability throughout their organisations.

We also believe that requiring such certifications would support the new regulator, The Audit, Reporting and Governance Authority (ARGA), in designing and operating their framework for appropriate supervision and oversight.

The recommendations in our August 2019 paper may be perceived as a significant undertaking and will require greater clarity with respect to the roles and responsibilities of directors, management, audit committees and the auditor with appropriate standards, regulatory oversight and enforcement for the parties involved.

Now, more than ever, the UK capital markets must continue to remain attractive to both investors and issuers. Enhanced corporate reporting can play an important role in protecting stakeholders. EY continues to believe that reinforcing accountability of directors is one of the pillars of enhanced corporate reporting.

[6] "The Sarbanes Oxley Act at 15: What has changed?", EY, June 2017

2.3. Effective frameworks, scrutiny and accountability

The ICAEW June 2020 essay paper — referred to above — discusses whether a new UK ICFR approach should be based on the Committee of Sponsoring Organizations of the Treadway Commission (COSO) initiative[7], specifically the 2013 framework over internal control or something else.

COSO is understood globally by regulators, companies and auditors alike. In our view, there would be clear advantages in aligning any new mechanisms to an already widely adopted framework and the informal feedback we get from companies we audit and other non-audit clients confirms it.

Developing or adopting a UK specific framework may prove counterproductive, particularly when applied across a global group, where subsidiaries are already familiar or trained in COSO.

Crucially, irrespective of whichever framework is concluded upon as being suitable for the UK market, minimum requirements should be in place.

With regards to external assurance over the management/board's attestation to the effectiveness of ICFR, direct experience and evidence-based analysis demonstrate that it provides clear benefits. In the absence of a blanket requirement for companies to seek additional assurance, it should be mandatory for the evidence supporting the design and operating effectiveness of ICFR to be retained to an auditable standard.

Allowing directors the flexibility to request additional assurance and only requiring an auditor's attestation when management identified a 'relevant control failure' as suggested by Sir Donald Brydon in his report, whether or not a failure of control has been identified, would not provide sufficient scrutiny of the work done by directors and management, but rather trigger a perverse incentive model. If not required by law, the decision on whether to request external audit should rest with the regulator and, ideally, be informed by a shareholders' vote.

Additionally, where directors attest on the effectiveness of internal controls and there is no requirement for external assurance, nor a mechanism for the auditor to provide explicit disclaimer, the risk of increasing the audit expectation gap is significantly higher.

Strong internal control requirements and effective scrutiny, supported by adequate sanctions, have proven to contribute to companies' resilience and sustainability, improved protection to shareholders and a wider range of stakeholders' interests, and driven audit quality.

Poorly governed companies may lack incentives to improve. A light-touch approach, focused on minimal burdens combined with the absence of a monitoring and enforcement regime, would not address the problem.

EY point of view — key requirements for effective ICFR

- The starting point should be the purpose — a strong ICFR helps to reduce the risk of fraud and corporate collapses and therefore protects shareholders and wider stakeholders.
- In terms of which entities should be caught, thresholds should be heavily influenced by investors' and other stakeholders' views. There may be merit in considering a phased implementation, as suggested in the EY 2019 paper referred to previously.
- Any new mechanism should clearly indicate relevant materiality definitions including for 'material weakness' and 'significant deficiency' and the criteria for reporting such findings publicly.
- Significant investment in robust process documentation and clear control evidence would be needed to achieve meaningful outcomes.
- The framework should clarify principles for the board's attestation, including a mechanism for directors to be required to provide documentary evidence of how they have reached their conclusions on ICFR, whether to an external regulator, external auditors or some other body.

[7] https://www.coso.org/Pages/default.aspx

2.4. Typical areas of strength and challenges for UK companies

Using the COSO framework as a starting point, we held a number of meetings with FTSE 100 and FSTE 250 companies to conduct an 'ICFR readiness assessment'. These meetings helped identify areas of strength and challenges for UK companies in ICFR. Based only on the companies we met, the observations include:

1. Leadership

Many UK companies say they have a good 'tone at the top', including appropriate board and governance structures and accountability. In improving ICFR, the challenge is for the approach to be cascaded down and embedded across the rest of the organisation. This starts with a review of the operating model across the three lines of defence including IT.

2. Strong focus on operational performance

Our interviews revealed that UK corporates generally have a strong focus on operational and business performance, which tends to be prioritised over internal controls. For such companies, the successful implementation of ICFR will rely on a change of culture, which will give internal controls equal emphasis along with more focus on assessing ICFR risks.

3. Senior leaders with ICFR knowledge and expertise

We know of several companies effectively implementing robust ICFR with no background in US SOX. Many UK companies would benefit from appointing senior finance leaders with experience of ICFR or US SOX as it would facilitate adopting a controls mindset. The numbers of executives with such experience is relatively limited within UK companies. So the challenge still lies in expanding relevant knowledge, training companies, and setting appropriate rewards, incentives and penalties in order to embed a controls culture.

4. Maintaining a strong and independent internal audit function

Our discussions confirmed that most UK corporates have an internal audit function with a broad range of responsibilities across enterprise risk. When a company enhances ICFR, the internal audit function can provide advice around who should be designing and testing any new ICFR controls. The internal audit function will need to be careful to maintain its independence of control design and operating effectiveness. This can be a challenge for companies with fewer people involved in risk management.

5. Reasonably strong IT policies and procedures including cybersecurity

Companies we met confirmed that they are mostly aware of cyber risks and have good policies to address them, along with good policies around access control and change management. The challenge is in actually turning the policies into practice. This means designing, implementing and testing the operating effectiveness of these controls.

2.5. Deficiencies and gaps include:

1. Lack of understanding of the importance of processes, risks and controls.

It was a common finding that many entities lack a widespread appreciation of the importance of robust processes, risk identification and controls. Those groups who emphasise financial and commercial performance above financial reporting controls will find they will need to address the tone from the top if they are to genuinely embed a culture of controls.

2. Inconsistent accountability and ownership of controls, issues and procedures

Accountability and ownership of controls, issues, policies and procedures is inconsistent within many companies. This is exacerbated when there are multiple hand-offs, for instance between business and a shared service centre, and no global process owners (GPO) or where responsibility sits outside of the finance team (e.g., taxation).

3. Financial and fraud risk assessment process

It was surprisingly common to hear that most UK companies have no formalised financial reporting risk assessment and no formalised fraud risk assessment. These will be an essential starting point to comply with Sir Donald Brydon's recommendations, not just on ICFR but also on fraud.

4. End-to-end process understanding and visibility

To establish effective ICFR, it is vital to ensure a good understanding of business process and underlying IT systems and reports. However, some companies lack visibility and understanding in most or all of their end-to-end processes. Setting this out clearly can be done using flow charts and risk and control matrices (RACMs). This is typically the most significant part of an ICFR improvement process, but there are now many tools available which can help companies accelerate this exercise.

5. Monitoring activities are in early stages of maturity

Effective monitoring can offer powerful 'detect and prevent' controls, but only if it is set up reliably to prevent or detect material issues. For UK groups, where monitoring is done, it is typically ad-hoc and not consistently followed month to month. UK companies should evolve controls monitoring to a consistent and reliable state and drive towards data driven 'continuous control' monitoring.

6. Non-interconnected, aging and legacy IT architecture

Some UK companies have disconnected, aging, legacy IT architecture. In any ICFR strengthening programme, the IT applications that are used to generate information that is used in the financial statements would need to have robust IT controls. For UK companies that have evolved by acquisition and have not integrated their IT systems or who have old customised IT systems, the IT SOX challenge will be significant. Even with cutting edge modern enterprise resource planning (ERP) systems there is a significant challenge if the implementation is not adequately controlled.

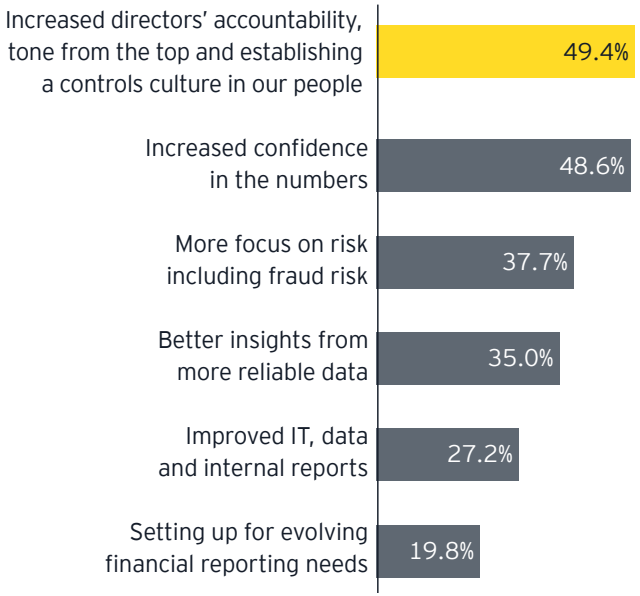
In addition to this we often see challenges in communication and accountability for data and controls between the finance and the IT departments.

2.6. Perception of strengthening ICFR among UK companies

In June 2020 we held a webcast[8] for CFOs, controllers and heads of internal audit where we discussed the introduction of a SOX-inspired framework for ICFR in the UK. We asked delegates a number of questions to explore the perception of strengthening ICFR in the UK. The findings* can be seen below.

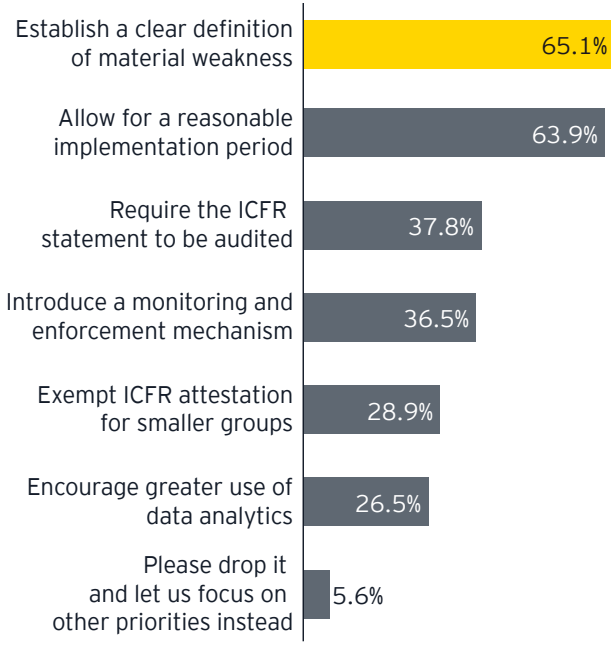
For your company what would you hope to be the main benefits of strengthening your ICFR?

(# responses = 257)



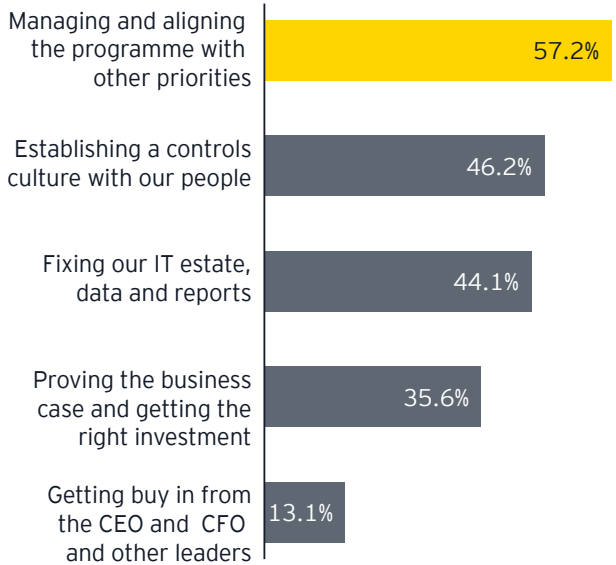
Which aspects should be addressed by Government and regulators to help UK entities implement an effective ICFR regime?

(# responses = 249)



What will be the main challenges of strengthening your financial controls?

(# responses = 236)



* Note: Participants were able to select up to two options per question and the results are shown here. The first three questions are about benefits, regulation and challenges of implementing ICFR. The fourth question concerns the use of technology and was added to give a sense of where companies may be able to implement ICFR more efficiently than was the case when US SOX was introduced.

[8] https://event.on24.com/eventRegistration/EventLobbyServlet?target=reg20.jsp&referrer=&eventid=2395968&sessionid=1&key=B09423B4EF5093D463D045C794633FD1&regTag=&sourcepage=register

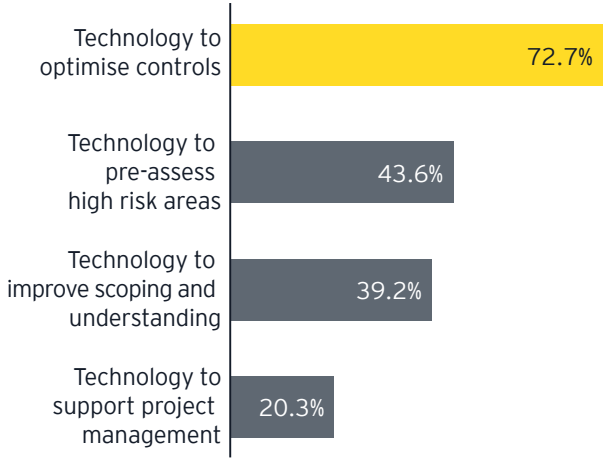
Responses showed that the main benefits of strengthening ICFR, were increased directors' accountability and increased confidence in the numbers, followed by a focus on risk including fraud risk, better quality data and improved IT. Increased directors' accountability and confidence in numbers were significantly aligned with a necessary change in the companies' internal culture, which demonstrate an understanding that, in order to be effective, reforms require the 'buy-in' of the entire organisation.

While clarity on materiality definitions and sufficient time to implement the reforms were identified as top priorities, about a third of respondents were in favour of the ICFR statement being audited and a further third (with a small amount of overlap) voted in favour of a monitoring and enforcement mechanism for ICFR. Less than 30% wanted smaller groups to be exempt from ICFR attestation and only about 5% voted for ICFR changes to be dropped entirely.

In summary, from the sample surveyed, there is broad support for an effective, monitored and enforced, and possibly audited, ICFR mechanism to be introduced in the UK.

Where do you think investment now in your organisation would bring most value later? Select two.

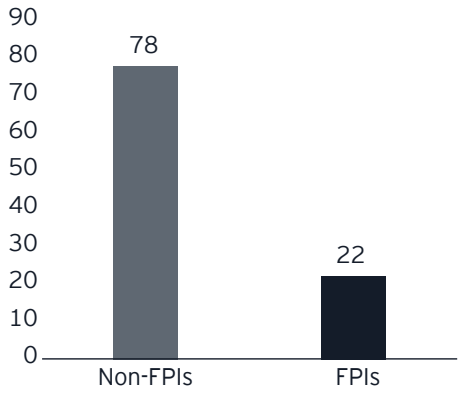
(# responses = 227)



The majority of respondents noted that automating controls in their IT systems would be a good investment now, compared to investing in project management technology. Indeed, using more automation to help eliminate some manual processes should enable companies to reinvest savings into other areas of improving ICFR.

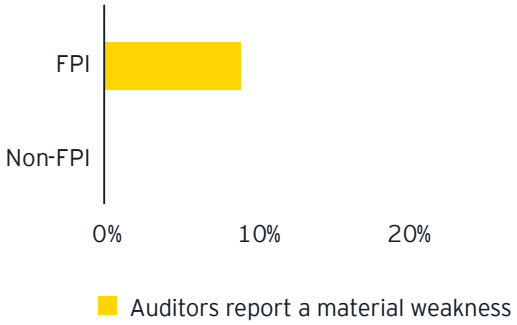
3 An overview of ICFR for the FTSE 100[9]

Out of the FTSE 100 companies, 22 are already foreign private issuers (FPIs) i.e., they already file ICFR audit opinions in the US markets.



For this reason, and to avoid a two tier approach in the UK, we would encourage avoiding duplication of requirements. Instead, we think that a reasonable degree of equivalence or relief, with the exception of any new potential requirements in the areas highlighted in Sir Donald Brydon's Report (such as fraud, key performance indicators and alternative performance measures and the resilience statement), should be allowed.

The Report, as indicated in previous sections, does not recommend a mandatory ICFR audit opinion, unless an internal control failure has occurred.



In the audit opinions in their most recently filed annual reports (August 2020) two out of the 22 FPIs (circa 9%) in the FTSE 100 reported a material weakness in ICFR. None of the 78 non-FPIs reported a material weakness in ICFR, although there is no basis for such reporting under ISAs. The UK Corporate Governance Code requires directors to report on their review of the effectiveness of the system of risk management and internal control. As part of this they need to explain actions which have been or are being taken 'to remedy any significant failings or weaknesses'. In practice the statements that UK companies make to satisfy this requirement are generally high level and lack the specificity that would be needed when, for example, an FPI reports a material weakness under US SOX. Although none of the 78 non-FPIs reported a material weakness, in a small number of audit opinions, the auditors stated that they were unable to rely on controls for the purposes of their audit and so performed additional substantive procedures instead.

In addition to auditors commenting on controls in their audit opinions, companies are also highlighting ICFR weaknesses elsewhere in their annual report, often in the audit committee report.

FPIs report a higher percentage of control issues than non-FPIs, as might be expected given their requirement to comply with US SOX. Furthermore, FPI auditors and their management teams are generally more aligned on ICFR issues than non-FPIs.

If the UK mandates an ICFR attestation requirement, we would expect UK companies to report more material weaknesses in internal controls than they report today. If, in addition, the UK mandates external auditor attestation on ICFR we would also expect (i) a further step up in the number of material weaknesses reported and (ii) there to be more alignment between auditors and management about what the ICFR issues actually are.

[9] Source: EY analysis August 2020

3.1. Audit opinions on the effectiveness on ICFR

Our 2018 FPI SOX survey noted that those companies that changed auditor reported relatively more material weaknesses and significant deficiencies than those who did not change auditor. This finding may imply that a fresh pair of eyes is more likely to identify ICFR issues.

The finding also supports the view that external audit of ICFR is likely to facilitate identification of material weaknesses in ICFR, therefore highlighting one of the advantages of involving auditors from the outset.

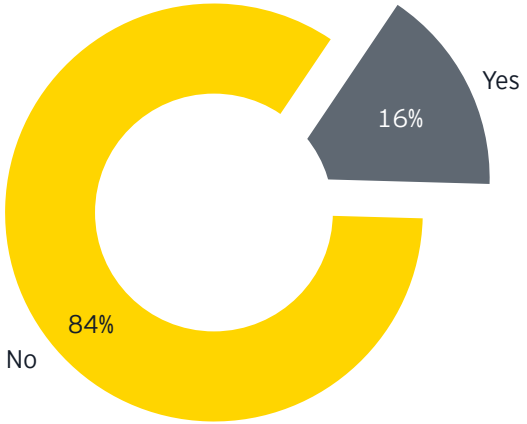
EY point of view

Evidence from the US generally supports the view that CEO and CFO accountability for, and attestation of, the effectiveness of ICFR contributes to increased quality of the financial reporting and reduction in the number of material misstatements. For US reporters, the involvement of the auditor further supports this aim by providing an independent opinion on the effectiveness of ICFR.

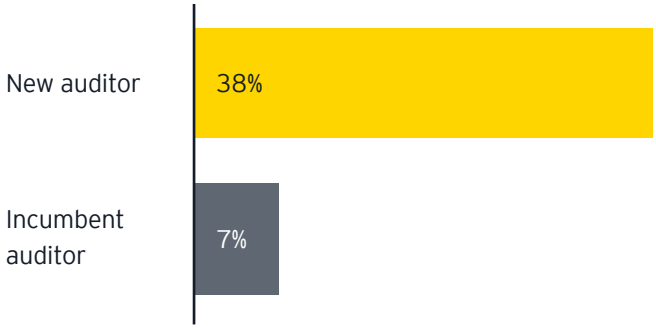
Involving your auditor

Did you change your auditor recently and what was the impact?

Auditor change within the last two fiscal years



Did you experience an increase in control deficiencies? (Yes answers)



- When auditors test ICFR controls for the first time, they tend to find issues which may be beyond what management has identified.
- Involving the auditor to test and report on the effectiveness of ICFR will increase the audit fee for the company. However, if the auditor's work helps management focus its efforts on areas where they may have had a blind-spot, it will reduce the risk of errors, increase trust and confidence in the financial reporting and lower remediation costs later.

Source: EY Foreign Private Issuer SOX Survey 2018

4 Lessons learnt from US Sarbanes-Oxley

4.1. Restatements and material weaknesses after US SOX was introduced

Restatements are a very strong indicator that there was a material weakness (MW) in ICFR. So, in assessing whether US SOX has been effective in its objective, it is worth revisiting the US history of (i) restatements and (ii) material weaknesses in ICFR.

(i) Restatements

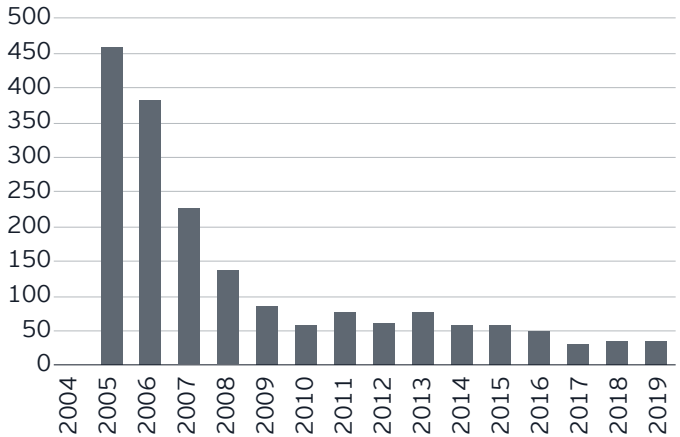
('Big R' restatements)[10]

A restatement happens when companies discover a material error, after the fact, in already issued financial statements and need to correct that error and disclose that correction. It tells the shareholders that the previously reported financial results were not reliable. A restatement represents the most severe issue with financial reporting and the situation can get more serious if the error was a result of a fraud.

A restatement may cause stakeholders to lose confidence in the management team and therefore may have a disproportionately negative impact on market value.

The number of restatements reported by US public companies has been steadily decreasing since the introduction of SOX.

Restatements in the financial statements of accelerated filers publicly listed in US[11]



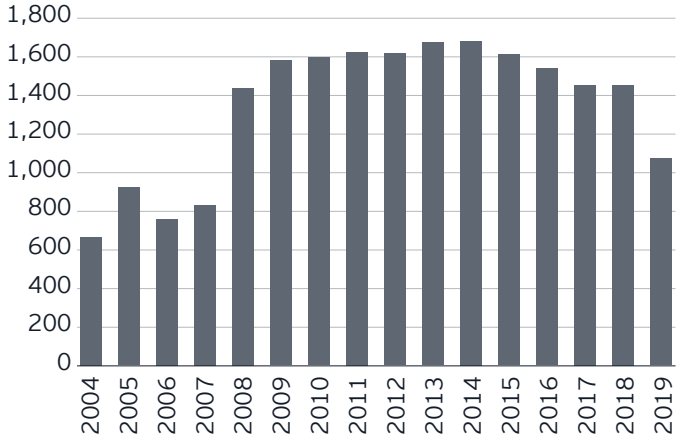
This picture offers some evidence that mandating CFOs and CEOs to attest to the effectiveness of ICFR may have helped to reduce the volume of restatements for US reporters by around 90%.

(ii) Material weaknesses

According to Auditing Standard 5 in the US, a material weakness in a control environment is a deficiency, or a combination of deficiencies, in internal control over financial reporting, such that there is a reasonable possibility that a material misstatement of the company's annual or interim financial statements will not be prevented or detected on a timely basis.[12]

A material weakness must be reported in management's assessment and the auditor's attestation on ICFR in the annual report and informs shareholders that the management team failed to effectively design or operate controls over ICFR.

Reported numbers of material weaknesses[12]



The number of reported material weaknesses for domestic US and foreign filers increased from 2004 to 2009 and it has remained at a high level since then. At the same time the number of restatements of financial statements filed with the SEC has been steadily decreasing since 2004, with a significant drop in the years following SOX implementation.

The auditor's regulator in the US, the Public Company Accounting Oversight Board (PCAOB)[13], plays a critical role. Through inspections of audit firms, the PCAOB in effect is setting out what is expected for ICFR audits. This has brought more consistency and standardisation in the application of ICFR findings in US corporates.

The lesson learnt from the US is that, with the CEO and the CFO being held responsible, there's a drive for improvement in ICFR, and there are subsequently fewer restatements resulting in more trust and confidence in financial reporting.

[10] Restatements, known as 'small R restatements' are also required as a result of transition to a new accounting standard but these are not considered to be as a result of errors.

[11] Source: EY Analysis of SEC data

[12] https://pcaobus.org/Standards/Archived/PreReorgStandards/Pages/Auditing_Standard_5_Appendix_A.aspx

[13] https://pcaobus.org/Pages/default.aspx[2] "The Sarbanes Oxley Act at 15: What has changed?", EY, June 2017

Before and after SOX, if a control was going to be relied on, for the purposes of the audit, it would have had to be verified as effective or substantive procedures would be performed. That did not change. However, it is an observation that, at the same time as the numbers of restatements have been decreasing, the numbers of reported material weaknesses increased from 2004–2009 and have then stayed fairly high. When a material weaknesses in ICFR is identified during an audit, the auditor will generally perform more substantive procedures to compensate for being unable to rely on certain controls and reduce the audit risk to a reasonable level. This approach should reduce the risk of an error in the financial statement audit and therefore reduce the risk of a restatement.

4.2. Cost and scope of ICFR

When establishing ICFR, companies face two types of costs: (i) the cost of external assurance over ICFR if external assurance is required and (ii) the entity's own internal costs to establish and maintain ICFR. The ICAEW paper[14] points out that, in the US, the latter cost is typically much more significant than the former.

The Brydon Report recommends that ICFR should be mandatory for all listed companies that benefit from public investments, and that external auditor assurance should only be required where there has been a failure in financial reporting controls within the last three years. As noted, 22 of the FTSE 100 companies are already listed in the US markets. The US ICFR audit threshold does not capture entities with less than $75 million of free float. In the UK, this would currently equate to smaller companies in the FTSE 250. We note however, that US companies are generally larger, so a like for like cut off in the UK should be lower than this level and so include more companies in scope. The US ICFR audit rules also exclude emerging growth companies[15] in their first five years post initial public offering (IPO).

A 2014 University of Kentucky and Louisiana Tech University study[16] of the period from 2007 to 2013 found that companies subject to ICFR audits experienced higher valuation premiums and higher credit ratings (which results in overall lower costs of debt). A Butler University and North Florida study[17] of the impact of SOX on the cost of equity capital of Standard & Poors (S&P) firms (for the period from January 1996 to December 2006) found that the cost of equity capital decreased post-SOX for the smaller firms.

14 https://www.icaew.com/insights/viewpoints-on-the-news/2020/june-2020/icaew-publishes-internal-controls-reporting-paper

15 An Emerging Growth Company in the US has annual revenues of under $1,07 billion and other conditions have been met as further explained in https://www.sec.gov/smallbusiness/goingpublic/EGC

16 An Analysis of the Costs and Benefits of Auditor Attestation of Internal Control Over Financial Reporting (October 2014).

17 The Impact of the Sarbanes-Oxley Act (SOX) on the Cost of Equity Capital of S&P Firms.

5 Accelerating ICFR implementation

Imagine a future world where UK directors are attesting to the effectiveness of their ICFR and there is general agreement that the introduction of UK SOX is positive and valuable for the companies they oversee.

In such a world, management teams would have established an appropriate governance structure for ICFR and will have developed a deep understanding of their data and the risks impacting their businesses and the controls to mitigate these risks. They may see, perhaps on an automated dashboard, when controls fail and take appropriate action to reduce business risk. Management teams will be using reliable data and analytics to give additional assurance and insights into business and commercial operations.

The good news is that UK entities in 2020 can expect to implement ICFR more efficiently than their US counterparts in 2004. The main drivers for this include:

- **ICFR practices and understanding:** ICFR practices, auditing standards, accounting standards and regulatory practices have been evolving over the years driven by the work of audit firms, regulators and risk management professionals so that generally, there is a far better understanding and appreciation of ICFR now than in 2004 which leads to more effective and focused ICFR programmes. Arguably this is the most important driver.
- **Technology:** 15 years of technological progress and the development of relevant software will help entities accelerate and reduce the risk of their ICFR implementations. Useful software includes analytical tools, process mining, spreadsheet analysers, SOX controls dashboards and modern IT systems that have built-in automated controls.

5.1 ICFR FAQs

This section will address typical queries we receive from UK businesses. It sets out how companies can strengthen their ICFR and take advantage of some of the technologies, tools and practices available to make their programme effective and successful.

How should companies typically get started with an ICFR strengthening programme?

While there are many challenges in implementing any ICFR improvement programme, we highlight some of the actions companies take in order to make a start on their ICFR improvement journey.

Chief among our recommendations are:

- Establish appropriate governance, resourcing and accountability in finance and IT to promote and bring a culture of controls to life. This may include the use of training, and establishing a suitable three lines of defence model.
- Run a detailed scoping and ICFR risk assessment and a fraud risk assessment and prioritise the most significant risks.
- For the most important processes in scope, develop an end-to-end understanding of the business process and supporting IT applications. Identify and fix any control gaps in both business and IT processes.
- For complex IT environments with a history of acquisitions that have not been integrated, assess options available to rationalise IT applications and use automated IT controls. IT change programmes can be multi-year exercises so companies should ensure a strong degree of linkage between the IT and the finance department during the IT and the ICFR improvement programmes. Investing in this area may help save SOX implementation costs later. We recommend that any IT change programme should include people with finance knowledge skills so they can design appropriate ICFR controls into any new systems.
- Establish an effective monitoring regime across the lines of defence.

The three lines of defence model divides responsibilities for internal control as follows:

- The first line of defence – functions that own and manage risk
- The second line of defence – functions that oversee or specialise in risk management and compliance
- The third line of defence – functions that provide independent assurance

Controls readiness assessment: We recommend companies start off with an internal controls readiness assessment. A readiness assessment tool which covers the COSO framework and is benchmarked against many other companies, should allow management teams to have a good indication of where a company's current control environment stands versus peers and identify areas of weakness.

What does a typical ICFR improvement programme look like?

Companies generally undertake their scoping and top-down risk assessment to identify financial reporting risks and fraud risks in all significant classes of transactions. This risk assessment is done with an end-to-end walkthrough of the main processes from initiation to final completion and recording. This ensures that risks are identified before designing and finalising the relevant controls to mitigate them.

It is during this risk assessment and walkthrough phase that companies should consider any IT implications and assess how to use technology to drive efficiency – through automation of, and monitoring of, controls.

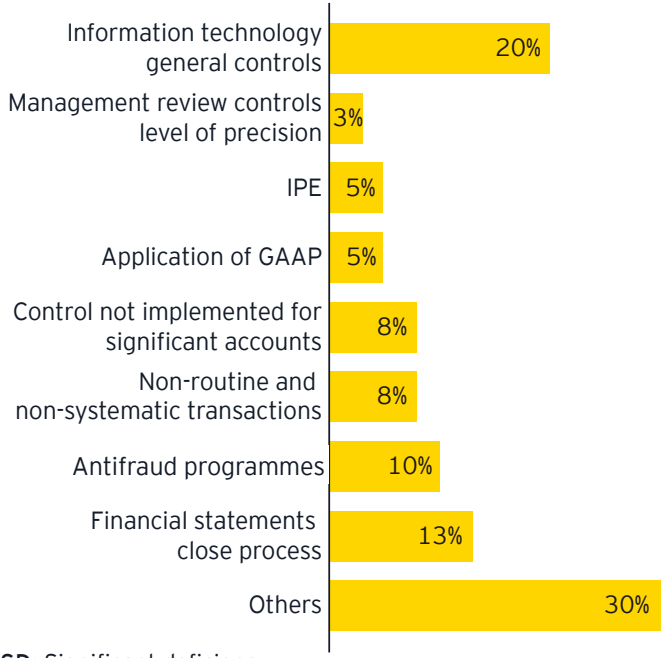
Gaps in the framework will be identified at this time, and so controls to cover these gaps must be designed, or improvements to existing controls must be made in order to meet the relevant objectives and cover the relevant risk.

Once the company has documented a robust end to end process for each significant class of transactions, the improved controls framework must be implemented, and then regularly tested.

What is the definition of a control failure and how would directors identify these?

A control has failed when it was either not designed properly, or its operation is ineffective such that it does not mitigate the risk it was intended to cover. Control failures would be identified during the walkthrough or testing phases of work.

If you did identify a MW or SD in your last ICFR assessment, what did it relate to?



SD: Significant deficiency
IPE: Information produced by the entity
CAAP: Generally accepted accounting principles
AI: Artificial intelligence

Source: EY Foreign Private Issuer SOX Survey 2019

Would IT controls be in scope for UK ICFR?

Although there are many more aspects to ICFR than IT only, we focus in the sections below on IT for two reasons. Firstly, IT is an area where US SOX reporters experience the highest number of material weaknesses and secondly because, based on our interviews with FTSE 100 and FTSE 250 companies, we have seen that there will be significant IT challenges for UK companies when it comes to improving their ICFR. All IT systems used in the processing of financial transactions and financial reporting for in-scope business processes will be in scope. Key IT controls operating in these applications, including IT general controls (ITGCs), will therefore be in scope. ITGCs include logical access controls, IT change management controls and IT operations controls.

What are the most common IT control failures?

ITGCs and IT application controls (ITACs) underpin the accuracy and completeness of data in key IT systems which are used in reports and preparing financial reporting information. If ITGCs cannot be relied on, then the reports that finance professionals use may not be relied on either. Since IT systems underpin much of financial reporting, a control failure in IT can often result in a material weakness in internal control. Even after 15 years of SOX, IT remains one of the most significant reasons for companies reporting material weaknesses.

Challenges that arise when companies set out to establish strong controls over IT include:

- Obtaining a complete list of applications and reports in scope.
- Identifying data used in reports and the appropriate data owners.
- Establishing appropriate access controls, change controls and IT operations controls.

For access control, companies need to include controls around password complexity, administrative access, user generic accounts, logging and monitoring of IT administrative activities, provisioning/de-provisioning of user access and the execution of periodic user access reviews.

For change management, companies need to include controls around approval of all changes to IT applications, testing of such changes and segregation of environments to ensure the same individual cannot develop and implement a change without authorisation.

For general IT operations, companies must establish controls around backup and recovery of data and the appropriate management and monitoring of IT batch jobs.

Many IT controls are detective controls with a strong manual component such as periodic user access reviews or removal of access to leavers. This results in inefficiency but also a greater likelihood of manual error and such controls commonly fail. It is important that companies start implementing automated system controls, which prevent the risk from occurring in first place, or enable the automated handling of such risk.

How do companies monitor compliance of their internal controls framework?

Monitoring should be performed by evaluating the controls in place — either by management, or by third parties. Any issues identified in the evaluation process should be logged and timely corrective action be taken. It is critical that the correct level of accountability is in place for this monitoring process to be effective.

Risk and control matrices have previously been advocated as a measure to assess financial risks and manage the responses to these risks. Are these matrices still relevant?

Risk and control matrices still play an important part in the overall risk assessment process. However, they are just one step in an internal control's improvement programme. It is also good practice to use a summary flow chart on one page to give an overview of how a process works and the controls and IT applications supporting it.

How can technology be used to support an internal controls framework?

As mentioned above, in a recent client webcast we explored the significant role technology can play in accelerating and de-risking ICFR improvement programmes. Four areas where technology can help are set out below:

1. Technology can be used to optimise controls through embedding controls within applications, or helping set out how transactions flow through a process and therefore assist in identifying duplicate controls that are reducing efficiency. Such technology has the potential to create savings which can be reinvested in further strengthening ICFR.
2. For companies doing ICFR for the first time, data analytics can identify higher risk areas by showing insights into the data, spotting outliers in a population where there may be a heightened risk requiring an additional control (for example a monitoring control) to mitigate the risk.
3. Data analytics can assist with the initial scoping and understanding of existing processes and controls.
4. Project management tools are available to support the ICFR programme, particularly for controls attestation or testing, i.e., showing on a live dashboard which controls have been operated and which have not yet been performed and highlight any challenges. Many US companies are still using spreadsheets to do this in 2020. When setting up their ICFR programme for the first time, UK companies could now use inexpensive technology that would show a real-time controls dashboard which would be updated live as people perform their controls as part of the month end close process. This will significantly increase productivity and effectiveness compared to using a spreadsheet.

Appendix

Checklist for getting started on an ICFR project

Readiness assessments

1. Undertake an ICFR COSO readiness assessment to benchmark against other entities and prioritise where to focus your efforts. Typically these will be in many of the areas set out below.
2. Conduct an IT general controls readiness assessment to get an idea of the IT landscape and the number of systems that will be in scope, and how an ICFR programme may fit in with the IT strategy.
    a. For access controls include: password complexity, privileged access, generic accounts, logging and monitoring, and joiners and leavers.
    b. For change management include: approval of all changes to IT applications, testing of IT changes, and segregation of environments.
    c. For IT operations controls include: backup and recovery of data, and IT batch jobs management.

Governance

3. Establish the appropriate governance, accountability, tone at the top and controls culture using training and incentivising the desired behaviours. Compare the 'as-is' operating model for risk management to the 'to-be' operating model and identify any gaps in resources and skills

Risk assessment and fraud risk assessment and scoping

4. Run a comprehensive ICFR risk assessment and fraud risk assessment in the business.
5. Use technology to achieve an efficient scoping and risk assessment. Where possible, use data analytics to identify outliers and risks.

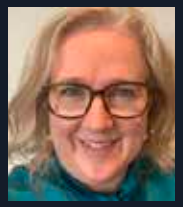
Quick wins

6. Identify opportunities for automating controls and access savings.
7. Establish clear and consistent accounting policies.
8. Although not a quick win, if you are already planning an IT rationalisation or upgrade, this action will significantly help any ICFR improvement later: Establish a common data model, chart of accounts and ERP IT system.
9. Involve finance professionals in the design of any ongoing or planned IT transformation.
10. Do a pilot: prepare end to end process documentation for a pilot process e.g., record to report or purchase to pay.

Documentation

11. Use flow charts to aid understanding of the end to end process.
12. Establish what assurance you will need from service organisations.
13. Establish the appropriate project management, reporting and monitoring tools.

Contacts



Kath Barrow

Managing Partner
UK&I Assurance

Tel: + 44 20 7951 0979
Email: kbarrow@uk.ey.com

Christabel Cowling

Partner, UK&I
UK Head of Regulatory & Public Policy

Tel: + 44 113 298 2364
Email: ccowling@uk.ey.com

Dan Feather

Partner
Assurance

Tel: + 44 7747 764 838
Email: dfeather@uk.ey.com

Ilaria Lavalle-Miller

Associate Director
Regulatory & Public Policy

Tel: + 44 7393 758 878
Email: ilaria.lavalle.miller@uk.ey.com

Notes:

Notes:

EY | Building a better working world

EY exists to build a better working world, helping to create long-term value for clients, people and society and build trust in the capital markets.

Enabled by data and technology, diverse EY teams in over 150 countries provide trust through assurance and help clients grow, transform and operate.

Working across assurance, consulting, law, strategy, tax and transactions, EY teams ask better questions to find new answers for the complex issues facing our world today.

EYG No. XX0000
EY-000126770.indd (UK) 11/20.
Artwork by Creative Services Group London.

ED None

ey.com