AUDITBOARD

What the 2024 UK Corporate Governance Code Means for Your Business

Four Best Practices to Implement Now

By Adam Rajah

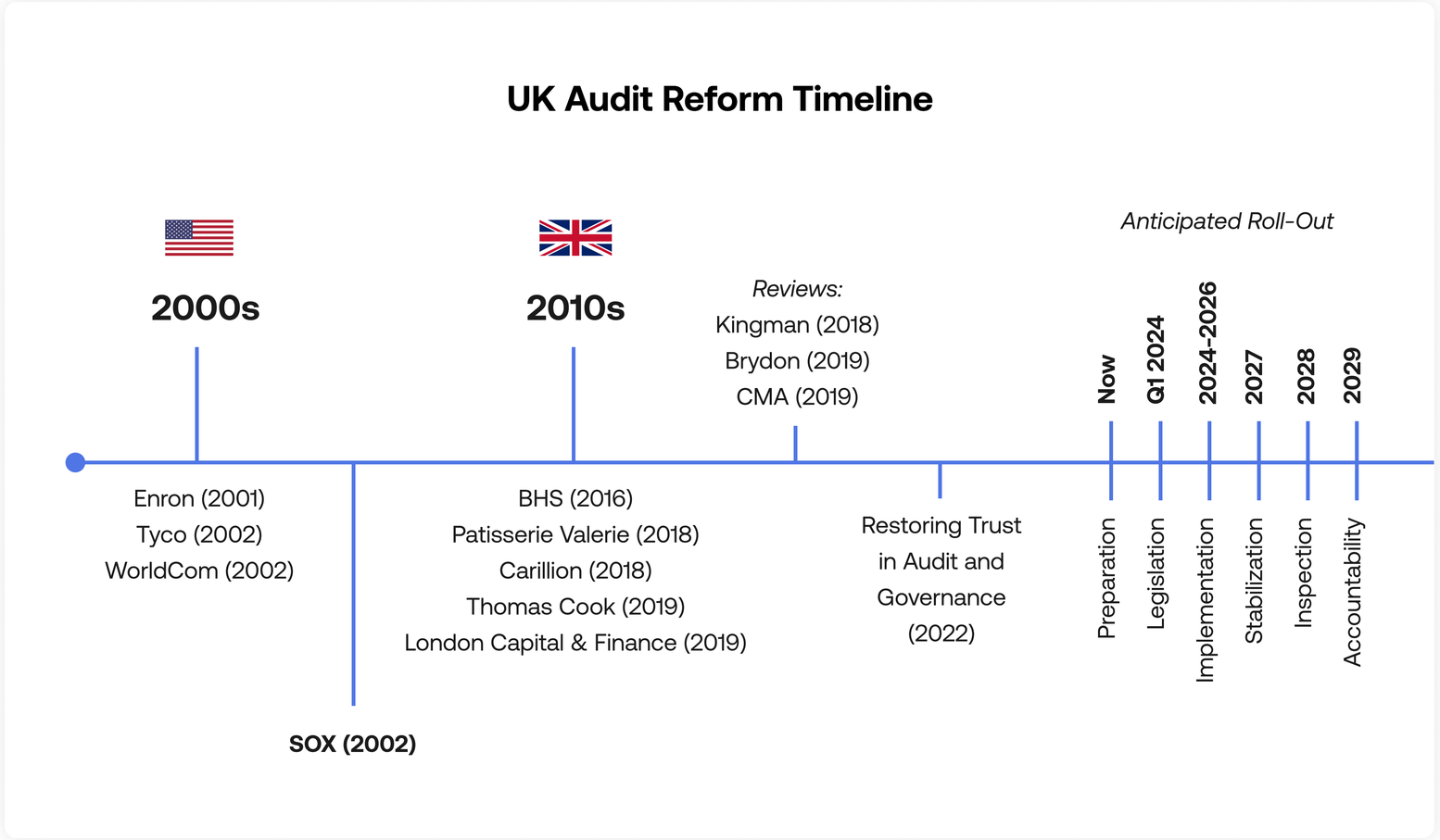
Earlier this year, the UK audit regulator (the FRC) published the 2024 UK Corporate Governance Code (the 'Code') which included its **much-anticipated updates on control reporting for companies**. This requirement will come into effect for financial years starting 1 January 2026, giving companies around two years to take steps to comply.

To remind ourselves about the impetus for this update: From 2016 to 2019, the UK experienced a series of accounting crises at companies such as BHS and Patisserie Valerie — which led to calls for increased reporting requirements in the Kingsman, Brydon, and CMA Reviews, among others. Since that time, there has been much speculation about a potential "UK SOX." Now the requirements are finally here and **companies will need to review the changes to ensure they are able to comply in the relevant timeframe**.

To help audit teams get a handle on what's in the 2024 UK Corporate Governance Code and what actions they should be prioritising, I'll discuss:

- A brief background of the **updated controls-related requirements**
- **Four key actions companies can take today to prepare for the requirements.**

Before diving in, I'd like to remind you to **take a deep breath and not to panic**. Many other organisations are in the same position, and there is enough time to plan ahead — provided you get started now and take a thoughtful approach.



What Are the Requirements of the 2024 UK Corporate Governance Code?

Before we dive into the requirements audit should be aware of, it will be useful to take a brief backtrack to consider what is in the code as compared with earlier proposals. The updated Code comes after lengthy discussion between the audit regulator and the industry over the last six years. After the Kingman, Brydon and CMA papers, **the UK government released the 'Restoring trust in audit and corporate governance' paper in 2022 that outlined three possible options for control reporting requirements for the industry**. Specifically, in order from smallest proposed transformation to largest proposed transformation:

1. Company directors should be required to carry out a review of the effectiveness of their company's internal controls each year and make a statement, as part of the annual report, as to whether they consider them to have operated effectively. The statement should disclose the benchmark system used and explain how the directors have assured themselves that it is appropriate to make the statement;

2. The audit report should describe the work the auditor is already required to do to understand the company's internal control systems to the extent needed to perform the audit, and to state how that work has influenced the audit, but without a formal auditor opinion on the internal controls' effectiveness being required; and

3. The auditor should be required to provide a formal opinion on the directors' annual attestation about the effectiveness of the company's internal controls, potentially limited to key internal controls over financial reporting, or a sub-set of that.

There had been much discussion between the industry and regulator since these options were outlined. In the end, the **updates in the 2024 Code have landed closer to the smaller transformation**.

It is worth noting that the 2024 Code has, apart from the updates on controls reporting, multiple other updated provisions including on governance, culture, and remuneration.

One critical change that all internal auditors should be aware of involves Provision 29 and the company's annual report, which should include:

- A description of how the board has monitored and reviewed the effectiveness of the [internal control] framework.
- A declaration of effectiveness of the material controls as at the balance sheet date.
- A description of any material controls which have not operated effectively as at the balance sheet date, including any action taken, or proposed, to improve the controls, and any action to address previously reported issues.

Some were anticipating this to be a UK SOX — it's not quite as rigorous as SOX, but it does require companies to take a number of steps to comply with the new requirements. Key differences between US SOX and the Code include:

- The Code, as a whole, has always been a **principles-based Code**. This is in contrast to the more prescriptive PCOAB-led controls regime in the U.S.
- **Companies must have financial, operational, reporting, and compliance controls** — an important difference from SOX which focuses exclusively on controls over financial reporting.
- In its annual report, the board will need to make a statement on the condition of the material controls, but **no third-party attestation is required**.

Companies have roughly two years to get their houses in order, as the controls effectiveness requirements give companies until financial years starting 1 Jan 2026 to comply. The following section identifies what companies can start doing now to prepare.

What Should My Business Do to Comply With the 2024 UK Corporate Governance Code?

What do organisations need to be doing now to ensure they are ready when they publish their 2026 annual reports? In my view, there are four core areas you and your CFOs, risk managers, and other leaders should consider prioritising to prepare for compliance with the 2024 UK Corporate Governance Code:

1. **Assessing organisational resources needed** to achieve the transformation
2. **Scoping "material" controls**
3. **Defining appropriate testing methodology**
4. **Leveraging enabling technology** to enhance risk and control management processes

1. Assess resources needed to achieve transformation

Depending on your company's level of controls maturity, **achieving compliance with the new requirements may require a significant transformation**. For some companies, the new requirements will mean:

- Designing new controls; that is writing control descriptions for the first time and assigning relevant control owners
- Performing annual entity/process risk assessments; which means reviewing which controls need to be tested each year.
- Deciding on a testing methodology
- Collating more specific annual reporting

Therefore, a company will need to:

- **Assess whether additional resources should be hired.** Determine if, given the size of your organisation, additional resources are needed to achieve compliance in the next two years. For example, a large organisation might need to implement, test, and report on at least 20 controls across 5 or more entities — that would be over 100 new controls. This transformation may be large enough to merit creating a dedicated controls team that is separate from the internal audit team. Companies setting up controls for the first time may also want to consider consulting with professional services firms to assist them with control implementation.
- **Determine controls testing responsibility.**
  Some companies may have more than 500 controls spanning multiple entities for their annual attestation. Even with a dedicated controls team, it may be extremely difficult to independently test all controls in a single financial year — especially if the company has just designed them. Therefore, it may be prudent to start with self-assessment testing or "first line testing", where a review and conclusion are given directly by the control owners. Though it is important to ensure the controls team still tests out the highest risk controls, using self-assessment testing for lower-risk controls may be sensible in the early stages of an organisation's controls compliance when the size of the controls team is still small. Refer to The Institute of Internal Auditors' Three Lines model for guidance on different potential lines of testing, including the first-line self-assessments described above.
- **Get senior stakeholder buy-in:**
  When implementing controls, it will be necessary to assign responsibility for owning controls to individuals. Control owners will typically be current employees of the business, and performing the control will be a new action added to an employee's existing workload. Therefore, getting senior stakeholder buy-in and support in communicating the importance of internal controls throughout the business will be critical to ensure controls are operated effectively in the year.

2. Scope “Material” Controls

Rather than jumping in to implement fully fledged controls on all possible processes, start by investing time in proper planning to ensure that your efforts are directed at implementing right-sized controls for the right entities. The updated Code does not require controls in every financial or operational process — only reporting on the effectiveness of “material controls.” Crucially, the Code leaves it to companies to determine what those are. In implementing the transformation needed to comply with the new requirements, companies will likely face resource constraints (as described above) as well as competing priorities with other company projects.

It is possible to cast too wide a net and end up scoping in more controls than are necessary for compliance or implementing controls that are excessively burdensome. Therefore, it is critical to take a rigorous approach to ensure companies choose the appropriate entities and appropriate processes to implement controls over. Organisations should consider:

- **Materiality concept:** Financial and non-financial considerations should be given to choosing appropriate materiality thresholds in the risk assessment process in choosing processes and entities to test. Determining an appropriate concept of materiality is crucial to ensure that controls are only implemented at relevant entities.
- **Right-sized controls:** companies should ensure the controls within processes themselves should be right-sized, that is, appropriate to the company’s size and industry. For example, a company could implement Control X, ‘Review all changes to purchase order limit changes for all suppliers’. A better control for the company’s risk profile may be to design Control Y, ‘Review all changes to purchase order limits which have increased by more than 20% for any supplier’. With Control Y, the company is choosing a certain risk profile to ensure it can focus its effort on the highest risk in the business.
- **Maturity and importance of non-financial controls:** The Code makes references to operational and compliance controls as well. If these are not yet properly formalised, it is timely to plan to scope in relevant controls in these areas.

As with any project, proper planning is crucial to success. Investing the time now will ensure efforts in the next two years are focussed on the entities and processes that present the most risk to the business.

3. Choose an appropriate testing methodology

After having selected material controls for your company, the next step is to decide which testing approach you will take. Unlike SOX 404, a third-party conclusion on control effectiveness is not required by the updated Code. Only the board attesting to controls is relevant. Therefore it is crucial companies decide their testing approach for controls so the organisation can properly manage testing through the year and to balance that with the board being able to make a conclusion on controls effectiveness at the year end.

Organisations should consider:

- **Reviewing common industry practices** for testing approaches and audit methodologies.
- Determining an **audit testing approach proportionate to and appropriate for the significance of the risk and control**. Audit testing can take the form of inquiry, observation, inspection, reperformance, or using company-assisted audit techniques (CAAT). Depending on the risk profile of a control, this means a fully fledged reperformance form of testing (that U.S. SOX can take with a lot of controls) is not always necessary.

Having detailed SOX-style workpapers for every financial control may be unwarranted. Instead, a documented form of inquiry for some set of controls may be more useful. Examining the right testing approach before commencing testing will allow companies to tailor their approach and potentially save hundreds of hours.

4. Enhance Risk and Control Management Via Enabling Technology

The UK Corporate Governance Code stresses the board's responsibilities in ensuring there is an appropriate risk management system, which is key to any internal control framework. In many companies where multiple units span different geographies, it can be challenging to establish a single list of risks and controls and keep it updated. In addition, it can be difficult to keep organised with controls testing across multiple entities and processes.

Organisations may consider:

- **Using a central technology solution** to maintain a single repository of risks, controls, issues, and associated action plans for remediation for the company.
- Perform controls testing and sending document requests by using **enabling technology** to support testing across multiple entities and processes.
- Ensuring there is a **robust process to review and update** the company's list of risks on a periodic basis. Technology can automate much of the review process.

Companies should leverage enabling technology to support integrated risk and control management practices for (a) identifying, reviewing, and responding to current and foreseeable risk exposures, and (b) controls testing. Technology can lead to greater efficiency, better data by eliminating discrepancies, and real-time insights for different stakeholders.

Seize the Day! Getting Ready for the UK Corporate Governance Code

Companies should already be thinking about how they will comply with the annual attestation on material controls so they can comply for the financial years starting on 1 January 2026. Much action is required, and the earlier the planning takes place, the better. Organisations that don't plan ahead risk doing unnecessary work.

It can be helpful to remember that the updated Code isn't just a matter of performing actions to comply; it's a real opportunity to improve your system of internal control. Risk and control management in many companies can be disorganised, operates in silos, and supported by manual work in Excel spreadsheets. A standardised, centrally led, and technology-enabled model of enterprise risk management and controls testing will not only satisfy the requirements of the Code, but also improve both strategic and operational decision-making.

About the Author

Adam Rajah is an Implementation Manager at AuditBoard who helps clients configure the platform on initial set-up. Previously a Manager at EY UK, Adam has significant experience in controls implementations and SOX testing.

About AuditBoard

AuditBoard is the leading cloud-based platform transforming audit, risk, and compliance management. More than 40% of the Fortune 500 leverage AuditBoard to move their businesses forward with greater clarity and agility. AuditBoard is top-rated by customers on G2, Capterra, and Gartner Peer Insights, and was recently ranked for the fifth year in a row as one of the fastest-growing technology companies in North America by Deloitte. To learn more, visit: AuditBoard.com.