Spotlight on material controls

Contents

This spotlight reflects our current thinking and is informed by our experience across the market. We will make periodic updates as market practices develop.

Introduction

Boards' responsibilities for monitoring, reviewing and reporting on the effectiveness of all material controls, including financial, reporting, operating and compliance controls have been part of the UK Corporate Governance Code (the Code) for some time, but were enhanced when the Code was revised in 2024. Under the revised Code, from 2026 boards will be required to make a declaration as to the effectiveness of all their material controls as at the balance sheet date, as well as describe any material controls that did not operate effectively at that time.

This spotlight provides our view on how management and boards should be determining their material controls as part of their responsibilities under the Code

We explore how material controls are identified and share some of the approaches we are seeing in practice. We also discuss the types of material controls that are emerging as organisations prepare for their effectiveness declaration. Specifically, we cover:

- What are material controls?
- Approaches organisations are using to first identify material risks.
- Approaches organisations then use to identify the material controls that address those material risks.
- Where we are seeing 'entity-level' controls becoming more commonly identified as material controls.
- A worked example of the identification of material controls

What are material controls?

The FRC has said that material controls are those over risks that could threaten the organisation's business model, solvency, liquidity etc, controls over reporting that could be price sensitive, fraud controls, or certain IT controls. Building on this, in our view, controls are considered to be material based on the extent to which it/they prevent or mitigate the impact of a material risk event, or material reporting errors, taking into account the level of residual risk organisations are willing tolerate. There are no prescribed numbers of material controls, but the general view is that it shouldn't be a significantly large number. Some important considerations when identifying the organisation's material controls:

01

Vital to link to material risk

Our 'Approaches to identifying material risk and reporting' section, describes for operational and compliance controls in particular, how material controls should be addressing a material risk or an important element of a material risk if that risk has been disaggregated. This requires the risk to first be properly defined and be of such importance that, if the risk event happened, it could have serious consequences for the business.

02

Material controls vs 'key' controls

Not all important controls will be material for the purpose of the declaration, and it is fine to categorise some controls as key but not material. This allows for a proportionate and focused approach, but at the same time still recognises the importance of the overall suite of controls.

03

Entity-level controls (ELCs) vs 'transactional-type' controls

Sometimes an ELC has the potential to be a more powerful control than a lower level transactional control and cover more of the material risk, so may be appropriate to designate as the material control. This is dependent on it being a reliable ELC, which we cover in the section on 'Relying on entity-level controls'.

04

Maturity of the risk management and internal control framework

When considering what the material controls are, organisations should consider the maturity of their risk management and internal control framework and whether this enables a primarily 'top-down' or 'bottom-up' approach, which we explore further below in the 'Approaches to identifying material controls' section.

Some companies are performing a sense check to determine if a material control, or controls in aggregate, are *truly* material. They do this by considering whether, if the control failed and the risk event it was meant to mitigate occurred, would that risk event result in the following types of response: the need to alert a regulator; alert investment analysts; require disclosure in the annual report in its own right; or demand significant management time and effort to correct. This isn't an exhaustive list, but this type of sense check can help to differentiate between truly material controls and other important 'key' controls.

Approaches to identifying material risks and reporting

An important first step to identifying material controls is first to identify material risks and reporting before determining the controls which most effectively mitigate or prevent those risks from occurring. We believe the following are sensible approaches and are seeing them more and more in practice:

Financial reporting

Boards and management are identifying which of their areas of financial reporting are material by adopting the principles of statutory audit or other regulatory regimes such as the Sarbanes Oxley act in the US to determine a materiality threshold for financial reporting. These are typically based on measures such as profit, revenue, or balance sheet criteria (such as asset values). Their assessments often take into account any additional qualitative risk factors, such as complexity in accounting, or historical errors, which elevate the inherent risk to any account classes or group entities.

Non-financial reporting

Boards and management are applying judgement to determining non-financial reporting that may be material as it involves both qualitative and quantitative data. They are considering factors such as: (a) What information reported by organisations do investors and other key stakeholders rely on when making decisions and the potential impact or implications of misstating this, (b) The potential impact to the business that could occur if the information is incorrect or misleading, (c) If there are existing, or anticipated new, relevant reporting standards, (d) Whether the information contains significant estimates or judgements, and (e) Whether there is existing guidance to inform materiality such as the double materiality guidance in the European sustainability reporting standards.

Compliance and operational risks

Organisations are leveraging their existing risk identification and assessment processes to identify which risks may be material. They have leveraged their risk appetite statements, and their impact and likelihood guidance across different categories (e.g. financial, reputational, health and safety) to identify a threshold above which they consider a risk to be 'material.' In practice, many organisations have defined their principal risks as material given their significance, with others defining key leadership risks as material also. Depending on the precision with which their risks have been articulated, organisations are needing to disaggregate principal or material risks to a sufficient degree of detail to identify their most material elements and to allow specific controls to be identified and meaningfully attributed to the disaggregated risk elements.

Approaches to identifying material controls

Following the identification of areas of material risk and reporting, organisations then need to consider the maturity of their risk and internal controls frameworks in order to determine whether they can take a 'top down' approach which relies more heavily on framework or entity-level controls, or whether they should adopt a 'bottom- up' approach that relies more heavily on more granular transactional-type controls.

01

Top-down

Organisations may take a primarily top-down approach to identifying material controls, rationalising existing frameworks into single material control 'areas' and/or adopting some entity-level controls such as policies, standards or committees over principal risk areas which already incorporate the output of underpinning controls.

This tends to be common where organisations have existing mature control frameworks that are assured and can be 'rolled up' into a lower number of material control 'areas' to support internal reporting to the board, and the annual declaration. Such organisations often exist in highly-regulated sectors which require specific control frameworks or have existing SOx-reporting requirements.

02

Bottom-up

Organisations which have more ad hoc or less developed frameworks face a need to first develop an effective risk management and internal controls framework, and so tend to adopt a primarily 'bottom up' approach, working through the full business processes underpinning each material reporting or risk area and identifying the relevant areas of control in a comprehensive manner that addresses risk to the extent they require.

The overall framework is characterised by a more comprehensive approach and a higher number of controls which may be badged as 'material' – either individually, or in aggregate.

Combined approach

Depending on their individual circumstances, many organisations are adopting a combination of both approaches, with still more using the the imperative to comply with the revised Code to help drive cultural, technological or operational change within their business. These organisations may have controls frameworks in place already, but they are focussed on how they can evolve or optimise their existing arrangements through the use of technology or better standardisation, for example, to drive greater value and efficiency through the investment they have made in their risk and controls arrangements.

Relying on entity-level controls as material controls

We are increasingly seeing organisations identify some entity-level controls (ELCs) as material controls, especially those with more mature control frameworks as described previously. With this in mind, it is important to understand how an ELC can be relied on as a material control.

ELCs can include, for example, board reviews, management committees, frameworks or systems. These are controls that often sit above process-level and transactional-type controls: they can operate as a standalone control or be an aggregation of other underpinning controls. If ELCs are to operate effectively as controls, organisations should be clear which risks they are addressing, what their objectives are, and what activities constitute the control.

In particular, organisations relying on ELCs as material controls still need to identify and consider the effectiveness of any underpinning controls before it can form a conclusion on the effectiveness of the ELC itself. Below, we explore what this would mean on a practical level.

Relying on entity-level controls as material controls (continued)

An important first step to identifying material controls is first to identify material risks and reporting before determining the controls which most effectively mitigate or prevent those risks from occurring. We believe the following are sensible approaches and are seeing them more and more in practice:

01 Specificity	02 Precision	03 Reliability of underpinning data or controls	04 Assurable	05 Authority and capability of committees or reviewers
Organisations specify the processes or activities undertaken that constitute the ELC. Activities may be specified broadly or in aggregate. Alternatively, they may be precise and separate, indicating the ELC is a process-level control.	The ELC should operate with sufficient precision to ensure that business objectives and the relevant risk(s) are robustly addressed. For example, 'The committee reviews cyber security KPIs,' does not articulate how this is achieved, how often, whether there is a threshold above or below which KPI performance is considered problematic, what action they should take to respond to exceptions, and how their review is evidenced. The activities are vague and if the committee operated as such, the control could be considered not to be designed effectively.	Organisations relying on ELCs need to identify and consider the effectiveness of any underpinning data or controls before it can conclude on the effectiveness of the ELC. This may include gaining confidence that both those controls and any data relied on is complete and accurate, that underpinning controls address all material areas of risk sufficiently and are operating effectively, or that any deficiencies in those controls are taken into consideration before the business concludes on the overall effectiveness of the ELC.	Control activities should be assurable. Evidence to demonstrate that the ELC has been operated should be clearly defined and retained to allow the control to be tested or audited. In our cyber committee example, the retention of clear minutes and action logs for the committee indicating that it has fulfilled all aspects of the control would demonstrate this.	Where a committee or review process is the ELC, descriptions or terms of reference should outline objectives, roles and responsibilities, the specific activities the committee/review will undertake, and areas that it is authorised to act or make decisions in. Committee membership, in particular, should be sufficiently experienced and capable to make decisions or perform the control activities required of them.

Worked example of identifying material controls

Worked example: Identify the material risk

This example illustrates the two different approaches to identifying material controls described above. The example is focused on compliance controls in a regulated business, but the approaches can be used more generally. The risks and controls are illustrative only and have been modified for the purposes of providing contextual information for this worked example. In the example we describe the thought process of how a principal risk has been disaggregated, first to level 2 and then, ultimately to level 3, which is the element of risk that is considered most material. We then identify the controls associated with this risk element and describe the two approaches to identifying which are the material controls, depending on the maturity of an organisation's risk management and internal control framework.

Identify principal risk

Level 1 – Principal risk 'Failure to comply with relevant laws and regulations'

The business has identified the failure to comply with relevant laws and regulations as a principal risk. Its rationale is that it operates in a highly regulated sector. Given the size and complexity of its business, and the number of compliance requirements in place, it has determined there is a strong inherent likelihood that it may unintentionally breach those requirements. It has assessed the potential inherent impact as material, given the possibility of some form of a serious sanction or significant penalty.

As the principal risk covers a very broad area, the organisation is now seeking to identify the components of that principal risk it believes are most material so as to define and apply material controls. It will do this through disaggregating the risk into successively more granular layers ('level 2' and 'level 3') of its risk taxonomy to home in on the most material components.

Risk disaggregation

Level 2 – 'Non-compliance with new consumer duty requirements'

Non-compliance with the new FCA consumer duty requirements has been identified as a material component of the principal risk. The business considers it possible that a breach may occur given this is a new requirement which the business must adapt to, and the business deals with a very large number of customers. It considers the impact of the risk crystallising to be high as the FCA have the power to implement a range of fines or sanctions in the case of breaches, which can be significant, financially and operationally.

Level 3 – 'Failure to identify vulnerable customers and support them'

The business has further assessed a failure to identify vulnerable customers and support them as the most significant component of the Level 2 risk. Its rationale is that vulnerabilities may not be immediately obvious to staff contacted by phone or internet so there is a heightened likelihood that staff will not identify vulnerable customers or offer measures to support them. The potential inherent impact of the risk crystallising is as per the Level 2 risk.

Having identified the material risk it wants to focus on, the business must now identify the controls over that element, which we demonstrate next.

Worked example: Identify the controls relating to the material risk

The organisation has identified the following controls over the level 3 risk 'Failure to identify vulnerable customers and support them':

C.01

Staff prompt sheets are provided and regularly reviewed to ensure staff handling communications are reminded to ask questions to help identify and record vulnerable customers, and offer reasonable adjustments for them.

C.02

Risk indicators to identify vulnerable customers are reported and reviewed by management. The outcomes of internal assurance checks are compiled and reported to senior management on a monthly basis, with any trends and root causes commented on. Management review the risk indicators and explanations and take action where appropriate.

C.03

Telephone exchanges are regularly checked to validate that vulnerable customers have been identified. An internal compliance team tests interactions on a sample basis to identify where a vulnerable customer may be present. Where this is the case, the tester assesses if they have been correctly identified and responded to appropriately by staff.

C.04

Staff receive annual training to identify vulnerable customers and understand how to respond. Training completion is monitored by the Development Team.

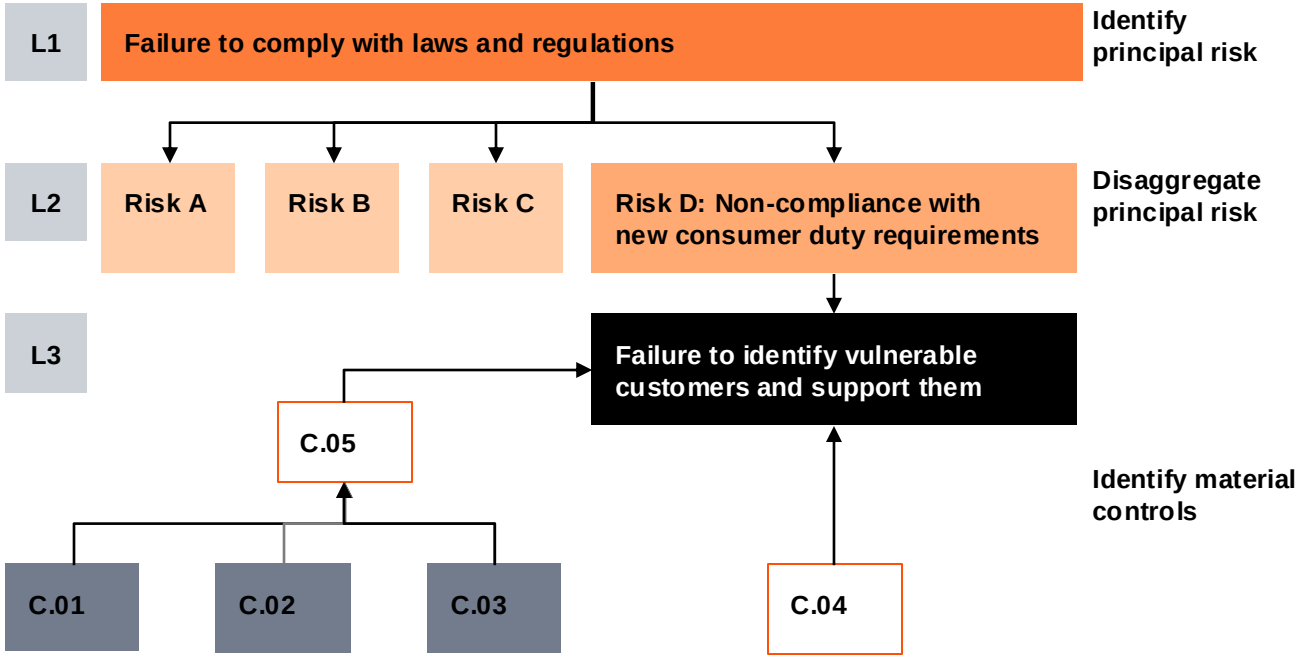
C.05

Compliance Risk Committee (ELC). The Compliance Risk Committee is responsible for overseeing the identification, assessment, and management of compliance risks across the business, reviewing the effectiveness of related controls, including around vulnerable customers, and ensuring staff are properly trained. The Committee meets on a monthly basis to review key conduct risk indicators, emerging risks, customer outcomes, and regulatory developments. It ensures that appropriate actions are taken to mitigate conduct risks and reports regularly to the board and relevant governance committees. Meeting minutes and actions are documented and subject to independent review to ensure accountability and continuous improvement. Controls C.01-C.03 feed into this ELC.

Once these controls have been identified, the organisation then determines which are material based on the extent to which it/they prevent or mitigate the impact of the material risk event, taking into account the level of residual risk the board is willing tolerate and based on whether a primarily top-down or bottom-up approach is most suitable. This whole process from risk disaggregation to material controls identification is illustrated in the diagrams below.

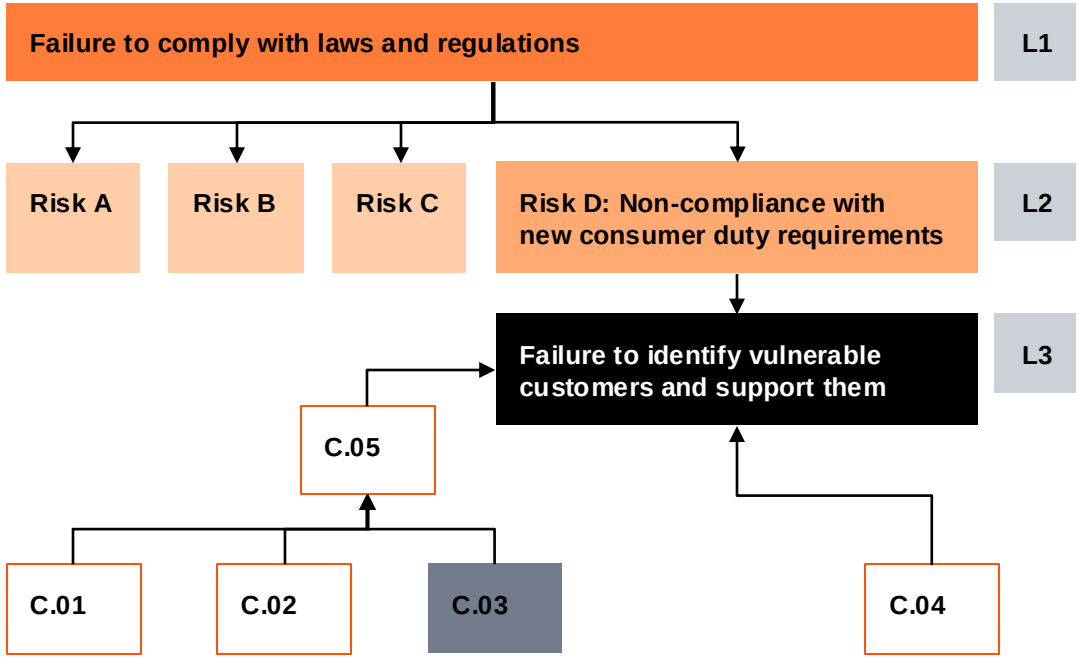
Worked example: Identify the material controls

Approach 1: Top-down



In this instance, the business has a mature existing controls framework. It is therefore confident that a primarily 'top-down' approach is suitable and identifies the ELC **C.05 (Compliance Risk Committee)**, into which outcomes from C.01-C.03 controls are reported, as an effective material control. In addition, it identifies **C.04 (Staff receive annual training),** as a separate material control over the material risk.

Approach 2: Bottom-up



In this instance, the business has a less well developed control framework and so does not think it can rely on an ELC - **C.05 (Compliance Risk Committee)** - as its only material control against this material risk. So it also identifies two other material controls that underpin the ELC i.e. **C.01 (Staff prompt sheets are provided and regularly reviewed), C.02 (Risk indicators to identify vulnerable customers are reported and reviewed by management),** In addition, it identifies **C.04 (Staff receive annual training),** as a separate material control against the material risk.

Thank you

© 2025 PwC UK. All rights reserved. PwC refers to the UK group of member firms and may sometimes refer to the PwC network. Each member firm is a separate legal entity.
Please see www.pwc.com/structure for further details.
RITM0291750

pwc.com