

# Assurance mapping

Are your assurance activities focussed on critical risks?

2022



Do you monitor the **burden on business** from assurance activities?

Do you trust that your assurance activities are being **managed and reported in a timely manner**?

What are your long term plans for enhancing your **assurance strategy**?

Do the four lines of defence in your organisation operate together to **assure all your risks**?

Do you know if there are **gaps or duplications** in your assurance strategy over your current and emerging risks?

Do you have a **Governance, Risk and Compliance (GRC) technology** to report on your assurance across your lines of defence?

What is an assurance map and how does it impact your assurance strategy?

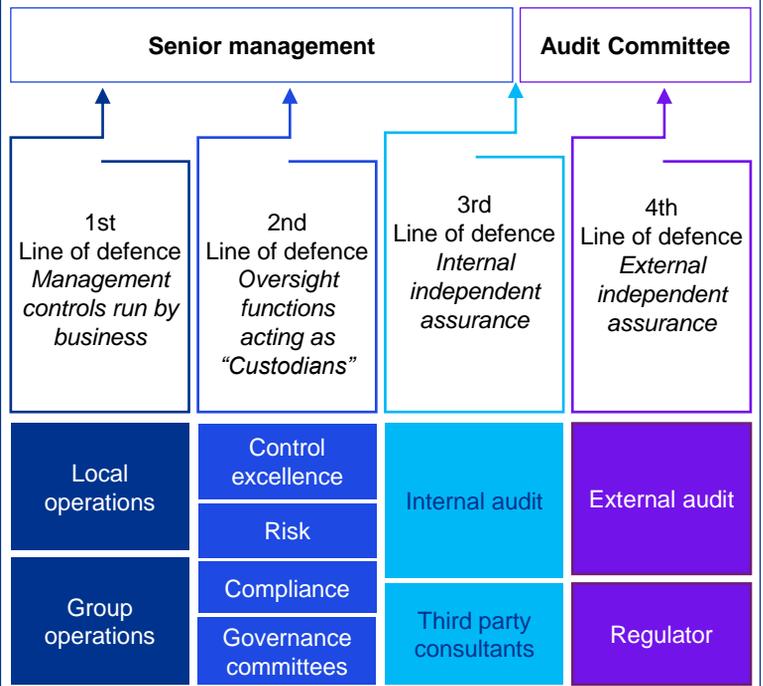
Illustrative four lines of defence (4LOD) model with non-exhaustive examples of assurance activities in each line

An assurance map is a

- **Visual and easy** to read illustration that provides an overview of the effectiveness and completeness of your assurance activities;
- **Holistic approach** to risk and assurance that allows for dynamic and effective risk management;
- Consolidated representation of the assurance provided by the **'four lines of defence'** which helps to identify the range of assurance sources available to an entity.

By identifying and outlining the assurance activities undertaken by each line of defence for your principal risks, you will be able to:

- Determine those risks which require further monitoring and management;
- Identify instances where certain risks have been excessively mitigated and managed as a result of duplicated assurance activities; and
- Make informed and focussed decisions with respect to your short, medium and long term assurance strategy over your principal risks.



## Triggers for undertaking an assurance mapping exercise

There are various drivers for an assurance map, including but not limited to, changing business environments, major transformation programmes and upcoming regulatory requirements including the demands over assurance disclosures introduced by the BEIS Whitepaper on 'Restoring trust in audit and corporate governance' and expected in upcoming legislation over audit reform.

## We have highlighted here some of the reasons why an assurance mapping exercise will be relevant and useful to you:

### Where your triggers are...

### ...and the benefits you stand to gain.

**Laws and regulations** will demand unprecedented levels of transparency and disclosure in assurance.

Building an integrated view of your assurance framework, and areas where you aim to strengthen it, is a robust first step to respond to future disclosure requirements in upcoming legislation and the **audit and assurance policy**.

Pressures exist to provide a better **view of the assurance landscape** to your Board and Audit Committee.

Integrating assurance information through leveraging technology and dashboards enables **comprehensive assurance reporting** to your stakeholders.

An optimised assurance framework gives comfort to your stakeholders that the principal risks are managed within the appetite.

**Business transformations** are the perfect opportunity to re-think how assurance is delivered.

Assurance mapping will show where assurance **duplications and gaps** exist, enabling you to optimise your assurance structure.

It also allows you to better respond to business transformation and changes in the risk landscape, as a constantly evolving assurance shows where new **assurance capabilities are required**.

Forward-looking assurance frameworks have internal audit in the driving seat, but **no longer as the sole agent of assurance**.

Assurance mapping will show you if your multiple assurance agents (internal and external) are **delivering true value** over your principal risks in a collaborative and efficient manner.

The mapping will give you an **integrated view of assurance activities** across the 4LOD, including where new capabilities are required, and enable informed decision-making.

## What does an assurance map look like in its most basic form

The map is intended to provide a snapshot view of the assurance obtained over an organisation's principal risks by various teams which form the organisation's four lines of defence. The below illustrative example of an assurance map captures both the gross risk scores prior to any assurance and controls and the net risk score post all assurance.

Principal Risks	Current Gross Risk score (pre controls)	First Line of Defence Business operations "Management Controls"			Second Line of Defence Oversight functions, e.g. Finance, Legal, HR, H&S, Risk and Compliance				Third Line of Defence Internal Audit and other independent assurance providers		Fourth Line of Defence Regulators and External Audit		Current Net Risk score (post controls)
		Group Function	Division	Sites	Compliance	Control Excellence	Risk	Governance Committees	Internal Audit	Third Party/ Consultant	Regulator	Ext. Audit	
1. Regulatory change	15	M	M	M	N/A	M	M	M	M	M	N/A	M	12
2. Loss of facilities	8	H	H	H	N/A	H	L	H	N	M	N/A	H	3
3. Ability to attract and retain talent	15	H	H	M	N/A	H	M	H	N	M	N	N/A	8
4. IT Resilience	8	H	M	N	M	M	O	M	N	N	H	N/A	4
5. Supply Chain incl. rising costs	9	H	H	N	N/A	H	L	M	N	N	N/A	M	6
6. ESG	12	M	M	M	M	M	M	M	N	N	N/A	N/A	8
7. Cyber	12	L	L	L	N	O	H	M	N	M	N/A	N	10
8. Transformation delivery	8	H	M	N	H	H	M	M	N	N	H	N/A	6

1

**High assurance**  
Control(s) cover all aspects of the risk and are effective.

2

**Medium assurance**  
Control(s) cover significant aspects of the risk and/or are partially effective.

3

**Low assurance**  
Control(s) provide minimum coverage of the risk and/or are not effective.

4

**Other assurance**  
Control(s) do not directly cover the risk but can be secondary source of assurance.

5

**Not applicable or No assurance**  
N/A - Source of assurance is not applicable for this risk.  
None – no assurance identified by management.

## Where we've done this previously

The management, Boards and Audit Committees at our clients have found it useful to conduct assurance mapping to gain awareness of the way in which they are receiving assurance in relation to key areas of operations and over significant risks.

### Client Ask

A new client wanted a **holistic view of its internal control and risk framework** and, in particular, the Audit Committee wanted oversight of how its principal risks were being managed.



*"In all my years of being a Chair of Audit Committee, this is the most useful document ... presented to me to allow [my team and I] to understand the holistic view of the internal control environment and allow us to undertake our responsibility in holding the executive to account on the control and risk environment".*



### Our Approach

In response, we applied our **assurance mapping methodology**. The process we adopted was to hold a mini risk workshop with each risk owner. By leveraging the existing risk registers, we facilitated the conversation to understand the controls in place to manage each risk and categorise them across the 4 lines of defence.

### The Detail

We categorised each control between **detective and preventative** to provide oversight over whether the control environment was appropriately balanced in terms of the nature of controls. As part of this process, we also captured **future mitigating controls** the risk owners had already identified, and using our established risk and control matrices, were able to offer **challenge around additional controls** that should be in place for each risk.

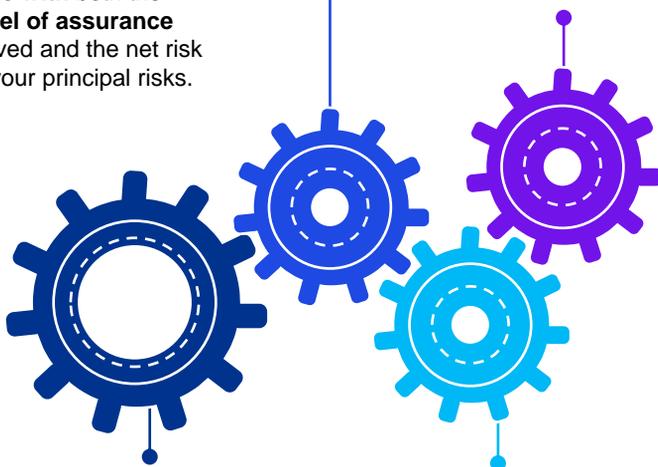
### Outcome

The resultant assurance map is used as a **live document** to manage the principal risks, monitor the current control framework and identify thematic areas that may need management or internal audit attention.

## Suggested next steps

Consider whether you and your Audit Committee are **comfortable with** both the **current level of assurance** being received and the net risk scores for your principal risks.

Finally, check whether you have enough information on the assurance obtained in the organisation to guide your **decision on areas of internal audit focus**.



Consider undertaking a **'blank page' strategic risk review exercise** to start with to ensure you have captured the right principal risks at an organisational level.

Assess whether the level of assurance obtained is **appropriate for your risk appetite**.

For further information, please reach out to:

#### Rachel Linhares

Director, Governance, Risk and Compliance Services  
rachel.linhares@kpmg.co.uk

#### Anupama Panikar

Senior Manager, Governance, Risk and Compliance Services  
anupama.panikar@kpmg.co.uk

#### Niall McClelland

Senior Manager, Governance, Risk and Compliance Services  
niall.mcclelland@kpmg.co.uk



[kpmg.com/socialmedia](https://kpmg.com/socialmedia)

Some or all of the services described herein may not be permissible for KPMG audited entities and their affiliates or related entities

The information contained herein is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavour to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act on such information without appropriate professional advice after a thorough examination of the particular situation.

© 2022 KPMG LLP, a UK limited liability partnership and a member firm of the KPMG global organisation of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

The KPMG name and logo are trademarks used under license by the independent member firms of the KPMG global organisation.

**Document Classification: KPMG Public**