

The Audit and Assurance Policy and Assurance Mapping: Tools to rethink assurance

Understanding and transforming the
approach to assurance

May 2022



Background to the Audit and Assurance Policy (AAP)

On 31 May 2022, the Government (BEIS) published its Response Statement (the Statement) following its consultation on reforms aimed at 'Restoring trust in audit and corporate governance'. BEIS intends to introduce a statutory requirement for the publication of an Audit and Assurance Policy (AAP). For most, the AAP will be published in the same section as the Audit Committee Report in the Annual Report. The AAP should explain the company's approach to assuring the quality of the information it reports to shareholders beyond that contained in the financial statements (statutory and voluntary disclosures).

In this presentation we outline the proposal for an AAP, which will apply to listed and private UK companies with 750 or more global employees and an annual turnover of at least £750m. We then describe the process of Assurance Mapping and how it can be an important part of developing the AAP as well as the broader benefits it can bring to risk management and optimising your assurance framework.



An opportunity for companies to set out more clearly to users the extent to which the annual report and other disclosures have been scrutinised, whether by the existing company auditor or someone else.



The BEIS Proposal for an AAP

BEIS Proposal

BEIS is proposing there be a legislative requirement for listed and private companies with 750 or more employees and an annual turnover of at least £750m, to develop an Audit and Assurance Policy requiring:

- Explanation of the company's approach to assuring the quality of information it reports to shareholders beyond that contained in the financial statements. This includes whether independent assurance is 'limited' or 'reasonable' or whether alternative forms of engagement/review is performed.
- Publication every three years with an annual update report (usually from the audit committee) on how the assurance is progressing.
- Minimum requirement to set out whether, and if so how, a company intends to seek independent (external) assurance over any part of the Resilience Statement and over reporting on its internal control framework.

1

- A description of the company's internal auditing and assurance processes, including how management conclusions and judgements in the annual report and accounts can be challenged and verified internally, and how the company is ensuring the integrity of their internal assurance process, and considering whether any improvements are needed.

2

- A description of the policy the company has in relation to the tendering of external audit services (including whether the company is prepared to allow the external company auditor to provide permitted non-audit services).

3

- Companies will have to demonstrate how they have taken account of shareholder views, although it won't be put to a shareholder advisory vote.
- Companies will also be required to state whether, and if so how, they have taken account of employee views.

4



***The Resilience Statement** – BEIS intends to introduce a statutory requirement for a Resilience Statement that will combine the existing going concern statement and viability statement.

What are we seeing?



Such is the interest from stakeholders (investors, regulators, audit committees, etc.) that many companies have started developing their AAP and a few have already published it.

Whilst a mandatory requirement to have a published AAP may be a couple of year end cycles away, many companies are already undertaking exercises, including reviewing their corporate governance disclosures and infrastructure and identifying the gap between their current assurance landscape and the landscape they and their stakeholders expect. Questions being asked include:

- What key areas to report on, what to include in the AAP and what level of assurance is likely to be expected?
- What AAP items are assured already and to what level?
 - consider wider assurance framework (four lines) – opportunity to review and revise.
 - assurance mapping as a practical tool to assess assurance coverage and depth. More details on assurance mapping can be found in the next section of this paper.
- How can the AAP be used to add value in addition to achieving compliance?

Internal Audit and other assurance and compliance functions are often actively involved in development of the AAP and associated interactions with the Board and AC.

For a more indepth look at the Audit and Assurance Policy please refer to our PwC paper 'Restoring Trust through an Audit and Assurance Policy':

<https://www.pwc.co.uk/services/audit/insights/restoring-trust-audit-corporate-governance/restoring-trust-through-audit-assurance-policy.html>

First steps in establishing an AAP

First steps to consider in establishing an AAP



Establish a shared understanding of the purpose of the AAP and how it will work

A cross functional working group/committee should understand, up front, the reasons for its development, the process for development and how it will be used. It is also important that it is started/updated in a timely manner and not left to the latter stages of the corporate reporting cycle when it is too late to properly think through the potential complexities.



Understanding stakeholder expectations

Investors and other stakeholders are placing increasing importance on company reporting beyond financial statements. Different stakeholders will have different needs and expectations when it comes to different company information. It will be important when developing the AAP to establish a way to consider the views of a wide range of stakeholders, and demonstrate sufficient engagement - understanding both the key areas shareholders consider important and balancing that with the views of management. Both are required to ensure the AAP is a successful and useful policy.



Establishing governance and ownership responsibilities

Establish, up front, the governance process around the AAP, who 'owns' its development and updating and ensuring the right resources are dedicated to its development and implementation. Consider:

- A number of functions within the business are likely to be involved, for example: risk management, finance, internal audit, Tax, Legal and Company Secretarial, sustainability and compliance functions (depending on the size and structure of the company).
- Initial responsibilities for updating the AAP are likely to sit with management and/or internal audit/compliance/legal and company secretarial functions.
- Ultimate approval would be by the Board, possibly through the audit committee. Consider the timing and frequency of when the AAP is updated and reviewed and approved. There will be a requirement for an annual update report from the audit committee on how assurance activity is progressing. It is worth also considering the enhanced role of the Audit Committee - many companies are undertaking a review of the structure, capabilities and governance support provided to the Audit Committee to ensure it is able to deliver on its enhanced role, including the new mandatory standards, for FTSE 350 audit committees, to be implemented by the Audit, Reporting and Governance Authority and the increased role the Committee will have engaging directly with shareholders.
- Ensure the Board/audit committee has adequate time to input into the process up front, making sure they are part of the decision process around the information to be included and the assurance needed. The Board/audit committee should also be updated regularly in relation to how assurance is working in practice, to support development of the annual update report and to ensure sufficient consultation and counsel is sought.

Assurance Mapping

Assurance Mapping to support an AAP

Background

Many organisations are familiar with assurance maps and have been using them for many years. We have taken the existing principles and methodology for developing assurance maps and adapted them for use in building an assurance map to support the new AAP requirement.

Assurance mapping enables the identification of any gaps or overlaps in assurance coverage by mapping assurance providers and their activities to reported information.

As part of the AAP, assurance mapping helps boards and audit committees to assess the reliability of their reported information and improves trust in the corporate reporting system.

This section also provides more details on the process of assurance mapping for use in broader risk management.



What does an Assurance Mapping exercise typically involve?



With all of the above in mind, the typical structure of an Assurance Mapping process is as follows (we will explore a number of these areas in the following slides):

1 Mobilise

- Define your starting point. For the mapping process to be most meaningful, it needs to be focused on the most important reported information (in the case of the AAP) or risks (when used for broader risk management purposes).
- Determine the required (future) assurance level so recommendations for optimising the assurance framework are commensurate with aspirations. It is paramount that your decision process on the level of internal or independent assurance required is supplemented by a robust and rigorous justification.
- Identify assurance providers (internal and external).



2 Build and validate understanding

- Engage with nominated stakeholders to understand assurance mechanisms – processes, people and functions – that assess how effectively the reported information is assured or the key risks mitigated, as well as the scope and frequency of assurance activities undertaken.
- Mapping of assurance activity to reported information or risks. Assurance activities are considered to be tests of controls (such as continuous monitoring, spot checking and independent testing) or review of other procedures and activities performed to give stakeholders confidence that those activities are functioning effectively.
- Determine the level of assurance provided by assurance activities using set criteria.



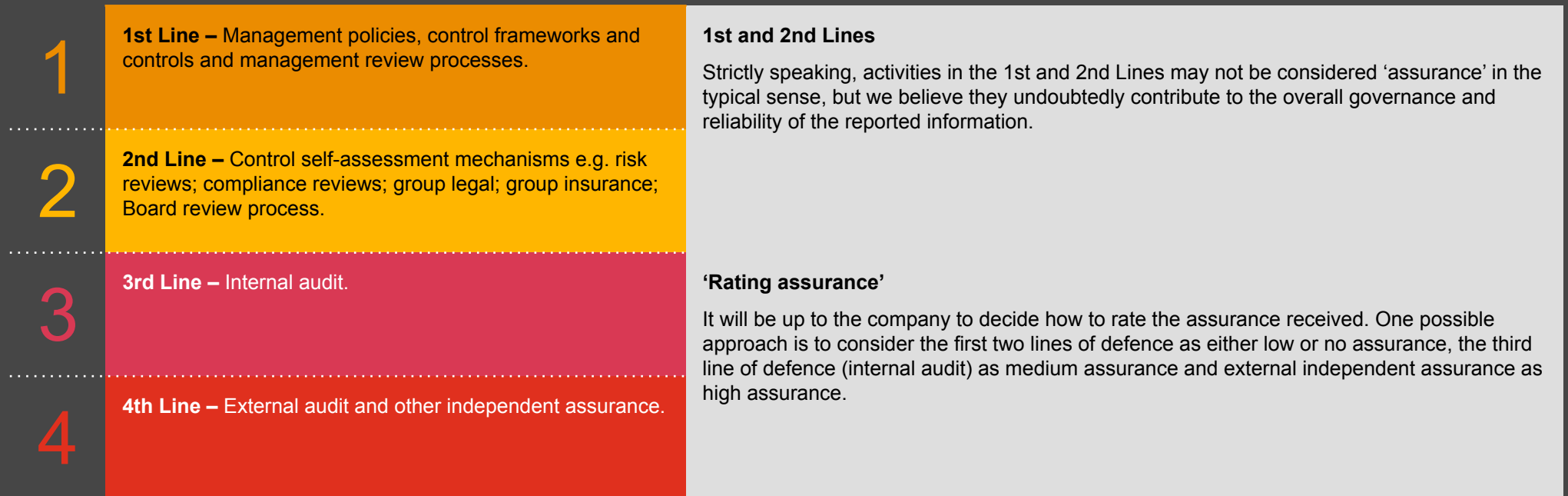
3 Analyse and report

- Once the forms of internal and third party assurance being provided have been assessed, they would be compared to the desired level of assurance to see if there are gaps (or indeed if excess assurance is being provided).
- Understand root causes, which may include:
 - resource constraints.
 - lack of coordination between assurance providers.
 - skills/knowledge gaps.
 - incomplete identification of risks.
 - lack of strategic oversight of assurance activity and minimal challenge of assurance plans.
- Consider the remedial actions to achieve the optimal assurance provision and help management to prioritise these actions.
- If it is determined that additional assurance is needed, the next step will be to consider the form of that assurance and the appropriate provider.



What are the different forms of assurance?

However you plan to use an assurance map, it is important to establish up front the different forms of assurance that might be included. One way to approach this is to use the Lines of Defence model from the Institute of Chartered Accountants in England and Wales (ICAEW):



Starting point for the assurance map

One of the most critical parts of the assurance mapping process is determining what information you plan to include.

AAP – when considering the reported information to be included, the following might help:

Principal risk disclosures

The principal risk disclosures in the annual report are, by their very nature, important reported information so should be considered for inclusion in the Assurance Map (BEIS suggests minimum content that includes 'disclosures relating to risk').

KPIs linked to principal risks

There are a number of critical disclosures a company makes which are not usually subject to external audit, such as key performance indicators (KPIs) and alternative performance measures (APMs), that should be considered for inclusion in the Assurance Map.

Information important to stakeholders and reputation

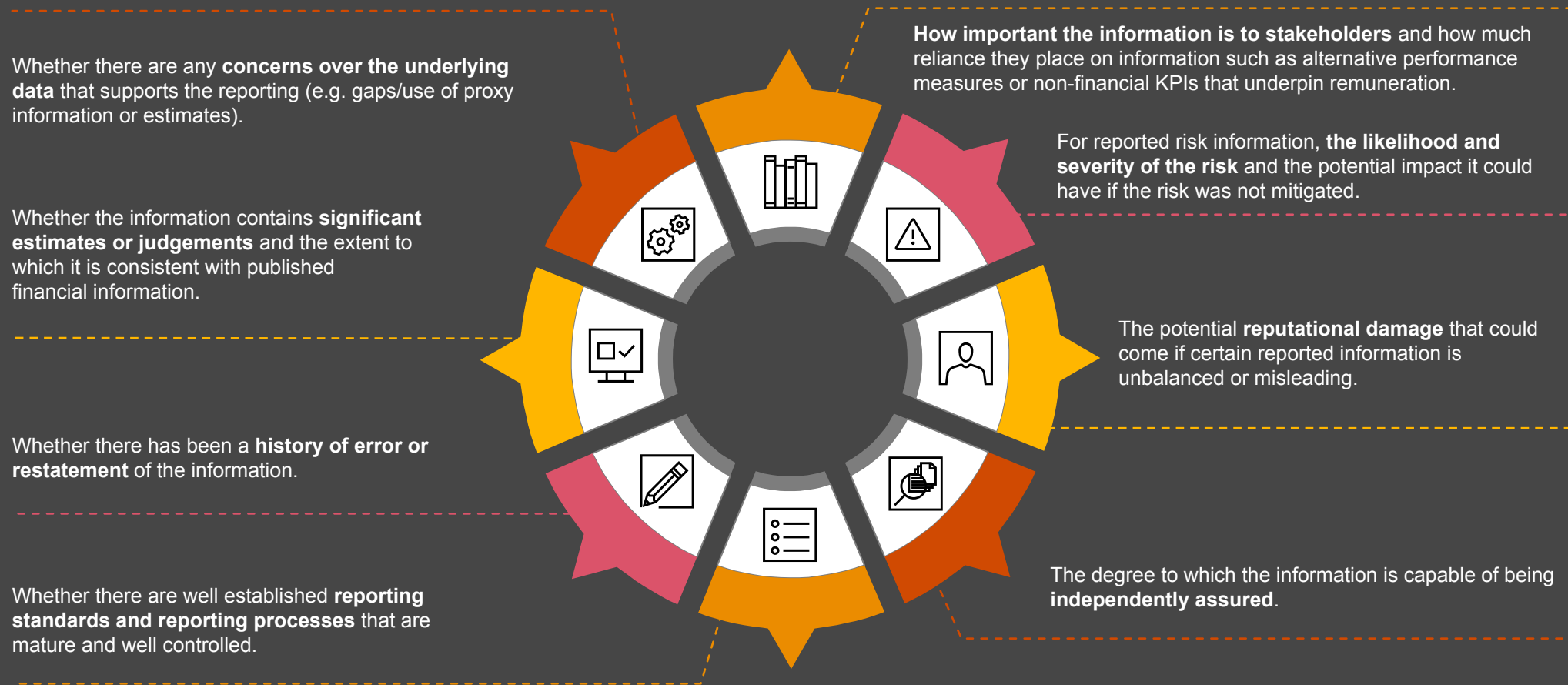
Reported information that might not link to a principal risk but is important to stakeholders or to the reputation of the company should also be considered. For example, ESG disclosures or diversity data; KPIs that underpin executive remuneration.

Additional content as suggested by BEIS

- The directors' statement on the effectiveness of internal controls over financial reporting; and
- The Resilience Statement and other disclosures relating to risks.

Assessing the level of assurance for the AAP

A key part of the assurance mapping process is determining what is the desired level of assurance and comparing that to the assurance being provided to identify any gaps or, indeed, areas where there is too much or the wrong type of assurance being provided. There is no magic formula – it will largely come down to the judgement and appetite of the Board/Audit Committee. However, for the AAP the desired level of assurance over reported information could reflect:



Illustrative example of an Assurance Map to support the AAP

This is an illustrative example of how the Assurance Map might be developed for the AAP. It will be up to individual companies to decide how much of this they want to report publicly, over and above the minimum requirements in the BEIS proposal. It would also be up to individual companies to determine what they consider to be High/Medium/Low (H/M/L) levels of assurance. This is just an extract for illustrative purposes and so does not reflect every piece of reported information (including all principal risks) that would most likely be included in the Assurance Map. It also focuses on disclosures in the annual report and not on any additional company disclosures that might be included.

	Step 1: Identity reported Information to be mapped	Step 2: Desired assurance (H/M/L)	Step 3: Determine forms of assurance provided – internal	Step 4: Determine forms of assurance provided – independent	Step 5: Determine if additional assurance would be beneficial and by whom	
	Annual report or other company disclosure		Risk response (1st and 2nd LoD)	Internal assurance provided (3rd LoD)	Independent assurance provided (4th LoD)	Additional assurance that would be beneficial and potential provider
	Principal risks and related KPIs in the annual report					
Non-financial and regulatory	Environmental, Social and Corporate Governance (ESG) impact: Unfavourable coverage regarding the company's ESG impact means that consumers take their custom elsewhere, leading to declining brand value and financial performance. Related KPIs in annual report: <ul style="list-style-type: none"> Carbon footprint Water usage Waste to landfill rates 	H	<ul style="list-style-type: none"> Clear ESG Strategy signed off by the board Policies and processes aligned to strategy List of approved suppliers, manufacturers and contractors Benchmarking against industry External communication over steps taken 	None	Other assurance provider performs limited assurance procedures over the reported KPIs.	Additional assurance to be commissioned over reported information and KPIs from external assurance provider to a 'reasonable' assurance level. Internal audit to also undertake a review of the internal policies and procedures around compiling ESG information.
Operational	Cyber: A cyber attack or failure could result in system outage, disrupting the business and leading to major data loss and reputational damage.	M	<ul style="list-style-type: none"> Specific IT policies in place Internal controls over cyber risks Disaster recovery plans Routine system 'penetration testing' Staff training over risks The IT department issues a monthly report to the Board outlining any cyber issues identified in the period 	Internal audit test the operating effectiveness of cyber controls on a sample basis throughout the year.	None	None – Internal audit procedures considered sufficient to reach desired level of assurance.
Financial	Capitalised software: Investment in capitalised software to support programme delivery may be not be recoverable where it does not deliver on the investment. Related KPIs in the annual report <ul style="list-style-type: none"> Return investments ratio Carrying value and write offs of capitalised software 	M	<ul style="list-style-type: none"> Financial and IT controls over approval, acquisition and development of new software Appropriate delegation of authority in place Review of actual progress against projected plans Annual impairment review 	Internal audit test the operating effectiveness of controls on a sample basis throughout the year.	External audit team review the operating effectiveness of key controls on a sample basis, and assess the recoverability of significant balances at the year end. External auditor performs reasonable assurance procedures over the capitalised software balance in the Financial Statement, and limited assurance procedure over the related reported KPIs.	None – internal and external audit procedures considered sufficient to reach desired level of assurance.

Illustrative example of an Assurance Map to support the AAP (cont'd)

	Step 1: Identity reported Information to be mapped	Step 2: Desired assurance (H/M/L)	Step 3: Determine forms of assurance provided – internal	Step 4: Determine forms of assurance provided – independent	Step 5: Determine if additional assurance would be beneficial and by whom	
	Annual report or other company disclosure		Risk response (1st and 2nd LoD)	Internal assurance provided (3rd LoD)	Independent assurance provided (4th LoD)	Additional assurance that would be beneficial and potential provider
	Disclosures and KPIs in the annual Report not directly linked to principal risks but of importance to stakeholders					
Strategic	<p>Failure to innovate: Failure to successfully invest, develop and deliver innovative products and services which meet the changing needs of consumers may inhibit ability to grow the business and impact financial performance.</p> <p>Related KPIs in the annual report</p> <ul style="list-style-type: none"> Customer surveys Effectiveness/impact of existing product portfolio 	H	<ul style="list-style-type: none"> Ongoing market research and surveys to understand consumer preferences and trends Dedicated innovation team trialling new products to be launched in coming years Diversification through acquisition of new business Internal review of the continued impact of existing services (compared to competitors and previous years) 	None	None	<p>Independent assurance to be commissioned over the customer surveys measure.</p> <p>Internal audit to test the data supporting the effectiveness/impact of existing product portfolio measure.</p>
Non-financial and regulatory	<p>Gender and diversity KPIs in the annual report:</p> <ul style="list-style-type: none"> Senior management headcount by gender Board membership headcount by gender Diversity of employees vs application pool Diversity of employees at senior management level Diversity of employees at Board level 	M	<ul style="list-style-type: none"> Clear objective signed off by the board for improving gender and diversity within the company, particularly in senior positions Recruitment and progression policies in place to support this objective Benchmarking against industry 	None	None	Internal audit to undertake a review of the implementation of this objective in practice.

Assurance Mapping to deliver broader risk management benefits

Background

Assurance Mapping is regularly used for broader risk management purposes beyond compliance with the AAP requirements. This involves the identification of any gaps or overlaps in assurance coverage by mapping assurance providers and their activities to key risks rather than reported information.

Assurance is critical to informing stakeholders (internal and external) that the organisation's risk management framework is robust, as it provides confidence that controls and other activities designed to manage risks are functioning effectively. By understanding whether the level of assurance is appropriate, management can build a more efficient, robust and cost effective assurance framework.

There is an increasing need to improve risk management and assurance capabilities beyond that relating to financial risk. Assurance mapping can be performed over several categories of risk classification including operational, compliance and financial risks. With many organisations experiencing greater volume and complexity of risks and regulations, assurance mapping provides insights into whether the assurance model enables the organisation to proactively adapt assurance focus as new risks emerge.



Organisations have been using assurance maps for many years to deliver the following benefits beyond compliance

Supports an **integrated risk and assurance model** where assurance is valuable and relevant to risks and objectives.

1

Greater focus of assurance activities on the areas that matter most and strengthened protection against risk.

2

Facilitates dialogue and transparency with stakeholders e.g. Audit Committee in relation to assurance coverage and depth.

3

Better understanding of effectiveness of the assurance model to support evolution of the assurance landscape.

4

Promotes collaboration that enhances value through opportunities for reliance and coordination with other assurance providers.

5

Opportunities for improving the consistency, efficiency and quality of risk monitoring across the business can be identified.

6

Improvements to governance of assurance capabilities e.g. clarity over accountability and responsibility for how each risk is assured against.

7

Determines whether **assurance coverage (scope of assurance) and depth (type of assurance conducted)** is fit-for-purpose.

8

Starting point for the assurance map

The 'starting point' for the Assurance Map will be different when assurance mapping is used for broader risk management. This 'starting point' will be the risks faced by the business. When considering the risks to be included, the following might help:

Scope of risk categories

Management should discuss and agree the key 'risk categories' to be in the scope of assurance mapping. Categories could be operational, strategic, finance, compliance or other non-financial risk categories.

Risk class selection

Once the risk category to be in scope is agreed, such as strategic, it is important to define the risk classes, e.g. for the strategic category, a risk class under the sub-category of markets and consumer risk could be consumer quality and safety. It is at the level of risk class that mapping is performed.

The assurance mapping process is similar whether it is used as part of the AAP or for broader risk management purposes but there are different criteria to consider when assessing the level of assurance, and different ways the output could be presented. The following slides go into more detail.

Assessing the level of assurance for broader risk management

When using assurance mapping for broader risk management purposes, the actual level of assurance will be compared to the desired level of assurance. In doing so, the following could be considered:

Relevance

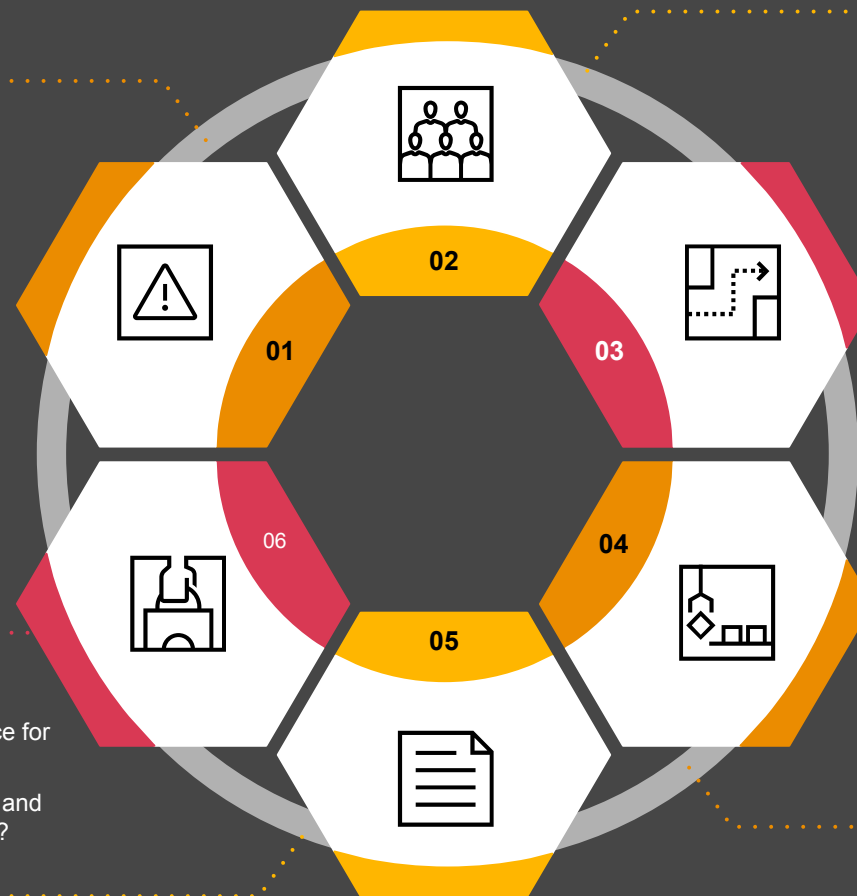
- Does the assurance activity address the relevant risks in full?
- A broad high level, or narrow deep dive may result in differing levels of assurance and complete or partial coverage of the relevant risk.

Assurance not delivery

- Is the activity definitely assurance? It may be a delivery task, e.g. filling out a template, and these do not qualify as assurance. An element of review, challenge and consideration takes place before declaring assurance.

Reporting

- Is there a robust and consistent process in place for reporting on internal assurance?
- Is progress of the business in addressing audit and assurance outcomes monitored and supported?



People

- Is the assurance provision structured with appropriate independence and objectivity?
- Are capacity/staffing levels appropriate to address all aspects of the risk?
- Do the team have the requisite skills and experience to conduct assurance effectively and receive appropriate training and development?

Process

- How formalised are the assurance activities in addressing the risk?
- Are assurance activities performed with an appropriate frequency relevant to the risk, and reactive to changes and issues arising?

Technology

- Does the assurance function use technology and tools effectively to support the delivery and management of their activities, including data analytics where relevant?

Example output from risk based Assurance Mapping

Here is an example of the potential output from an assurance map used for broader risk management. Assurance mapping is a useful tool to help management better understand whether the right 'amount' of assurance is being provided in relation to risk tolerance and appetite. Such clarity of the current assurance landscape and how it is to evolve and be fit for purpose can inform the Assurance strategy of an organisation particularly when sustained as a 'live tool'. Assurance mapping also provides the necessary understanding of the governance structures/key roles. In the illustration below it would be a priority to address the assurance gap that mapping has identified in the product risk area as a high level of assurance is required here with only a medium level being provided currently.

Risk classes	Current assurance			Recommended assurance	Priority
	Second line	Third line	Overall level of assurance		
Business portfolio risk					
Major change programmes	No assurance identified	L ●	L ●	L ●	●
Organisation and governance risk					
Culture and behaviours	L ●	M ●	L ●	M ●	●
Investor and external communications	L ●	No assurance identified	L ●	M ●	●
Product risk					
Sales and Operations Planning	M ●	M ●	M ●	H ●	●
Sourcing and procurement risk					
Human Rights non-compliance	L ●	No assurance identified	L ●	M ●	●
Ethical sourcing	M ●	M ●	M ●	H ●	●
Supply business continuity planning	M ●	M ●	M ●	H ●	●
Human resources risk					
Labour law compliance	L ●	No assurance identified	L ●	M ●	●

Level of assurance	
High level of assurance	H ●
Medium level of assurance	M ●
Low level of assurance	L ●

Priority	
Critical priority (High level of recommended assurance with a current low level of assurance)	●
High priority (High level of recommended assurance with a current medium level of assurance)	●
Medium priority (Medium level of recommended assurance with a current low level of assurance)	●
Adequate level of assurance recommended (The current level of assurance is in line with the recommended level)	●

Thank you

[pwc.com](https://www.pwc.com)

This publication has been prepared for general guidance on matters of interest only, and does not constitute professional advice. You should not act upon the information contained in this publication without obtaining specific professional advice. No representation or warranty (express or implied) is given as to the accuracy or completeness of the information contained in this publication, and, to the extent permitted by law, PricewaterhouseCoopers LLP, its members, employees and agents do not accept or assume any liability, responsibility or duty of care for any consequences of you or anyone else acting, or refraining to act, in reliance on the information contained in this publication or for any decision based on it.

© 2022 PricewaterhouseCoopers LLP. All rights reserved. 'PwC' refers to the UK member firm, 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.

RITM7433908