Restoring trust through risk management and internal control

pwc

Companies are facing more diverse, fast-moving and unpredictable risk than ever before – from climate change, economic uncertainty and societal inequality to cyber threats and systemic global disruption. The constantly evolving regulatory landscape adds further complexity to grapple with.

When faced with uncertainty and risk, the companies that are most successful are those with robust systems of governance, risk management and internal control that are designed not just to meet regulatory or compliance standards, but to add value and ensure that they can thrive safely. Strong internal controls, especially in areas of most risk and vulnerability, are essential for shoring up the system, and have significant benefits on many levels, not least in rationalising operations, combating fraud and enhancing the quality of reporting.

For questions, please contact:

Jayne Kerr
Director, Public Policy
jayne.l.kerr@pwc.com

Sotiris Kroustis
Partner, UK Head of Public Policy
sotiris.kroustis@pwc.com

Richard Bailes
Partner, UK Leader for Governance Risk and Compliance
richard.j.bailes@pwc.com

Katie Griffin
Director, Risk and Enterprise Control
katie.griffin@pwc.com

The board has responsibilities under the UK Corporate Governance Code (the Code) for establishing and overseeing a company's risk management and internal control systems. Also, the board is responsible for monitoring and reviewing the systems' operating effectiveness and reporting on this in the annual report. In this Restoring Trust guide, we have provided our view on what we think are the key elements of a robust process for oversight, monitoring and review of systems of risk management and internal control, together with a worked example about how the elements would come together in practice.

Key elements of a process for oversight, monitoring and review of the systems of risk management and internal control

- A defined strategy and governance, with clear ownership and accountability
- Risk management and materiality at the core
- A focus on the material controls that address the material risks
- Controls that are clearly articulated, and are designed and operating effectively
- A well thought out approach to assurance
- Detailed and transparent reporting

Contents

Risk management and internal control - key elements of a process for oversight, monitoring and review

Many organisations have systems of risk management and internal control already established as part of the normal functioning of their business. For some this will be based on well recognised frameworks such as COSO.

A process should also be in place for boards to oversee, monitor and review the operating effectiveness of their systems of risk management and internal control - covering reporting (financial and non-financial), operational and compliance systems and controls. We believe there are six key elements to such a process. This is a point of view and will need to be adapted to individual companies' facts and circumstances and any process that is used should be well-documented and have a clear basis and rationale. The six elements are as follows:

Element 1 - Defined strategy and governance, with clear ownership and accountability

The board is ultimately responsible for establishing and maintaining effective systems of risk management and internal control; monitoring the systems and reviewing their effectiveness (often via the audit committee); and reporting on the effectiveness of the systems in the annual report.

As well as the board, management, internal audit and possibly also external audit or other advisors, will all have a role to play, so it will be key to consider the following:

- Duties and day-to-day responsibilities of management for the operation of the systems of risk management and internal control, including any self assessments.
- Any reviews or compliance testing of the systems carried out by individuals other than the control operators.
- The role of internal audit and its reporting to the board and the management on the design and effectiveness of the systems of risk management and internal control.
- The role of the external audit or other external advisors or providers of independent assurance.

These are effectively the 'lines of defence' that ensure the risk management and internal control systems are working effectively, and are explored further below. Allied to this, a clearly defined vision and strategy for risk, control and assurance defined by the board and management and aligned to the businesses' objectives will help ensure the

activities of each line of defence are coordinated and focused on a common set of goals. This will enable effective prioritisation of resources and effort when making capital allocation decisions and project scoping.

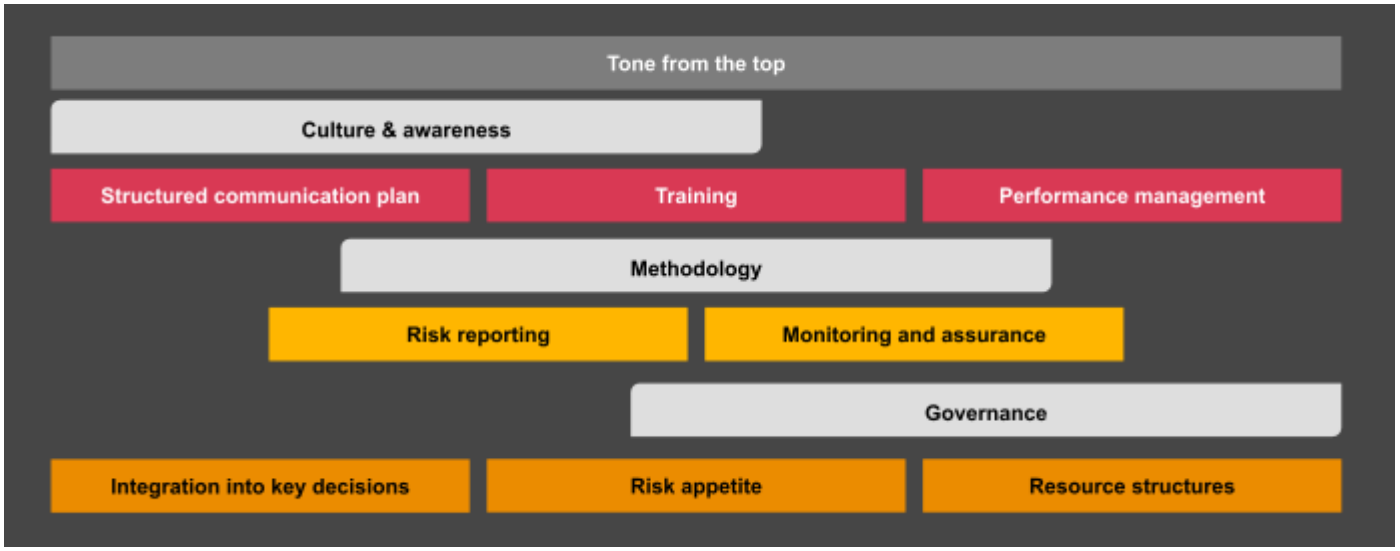
Winning hearts and minds and building a 'controls conscience' will be essential. Whatever the model used, ownership and accountability to make sure the changes stick, will be a vital consideration. Embedding systems of risk management and internal control is ultimately a change management programme - organisations need their people and their business to buy-in and to act and behave differently to achieve long-term, sustainable change and meet the requirements. A lot of organisations focus on training to help their people understand the change but training alone is not enough, people need direction, fresh perspective and the support around them to change the way they go about doing their day to day work.

Element 2 - Risk management and materiality at the core

A comprehensive risk management programme

A comprehensive risk management programme will ensure that the board's process for assessing effectiveness of the systems of risk management and internal control is risk and materiality focused, and therefore proportionate.

In our view, effective risk management can be organised into three broad categories (culture & awareness; methodology; and governance) alongside an effective 'tone from the top'. We have set out the components which then align to these categories below:



The components can be characterised as follows:

1. Leadership that regularly provides a **strong tone from the top**, with clear messaging on the importance and value of risk management and visibly leads by example.
2. A **structured communication plan** that reinforces key messaging on risk to all employees.
3. Formal business-focused **support and training** that promotes understanding of the practice and value of risk management in meeting objectives.
4. **Measurement of staff performance** in risk management and controls, and linkage to reward and career progression.
5. Dynamic and insightful **risk reporting** that drives management decisions and is a part of wider business performance reporting.
6. Robust mechanisms in place to **monitor and provide assurance over compliance** with minimum risk management requirements and quality expectations.
7. Consideration of risk and return, bearing in mind the business's risk appetite and tolerance, that is **built into all key decisions** made.
8. Key decisions are made and operations are **conducted in line with the articulated risk appetite,** and leadership is notified when there are any deviations with risk appetite.
9. **Risk resources** that provide risk management support throughout the business.

Identifying material risks

A robust but proportionate effectiveness assessment will focus on **material** controls and it is logical that these would be the controls that address material risks. So, identifying those material risks as part of the risk management programme described above, is essential.

A robust risk assessment should practically be performed at least annually, but also when there was a significant change in the objectives or structure of the business, for example, a material acquisition, or a significant external shock. The risk assessment would most likely be performed for different aspects of the business and owned by leadership in those areas, but should be brought together and reported to the board in a comprehensive and consistent way.

The initial step is to identify the areas of reporting, compliance and operations that could be most at risk of being incorrect or would have the most significant impact, if they were wrong.

In terms of what could be considered ‘material’, it will be different depending on whether it relates to reporting (financial and non-financial reporting), operational or compliance risks.

Financial reporting

Businesses are generally familiar with how to determine financial reporting materiality through the statutory audit or other regulatory regimes such as the Sarbanes Oxley Act in the US, better known as SOX. UK entities could adopt some of the core principles of the SOX regime when determining their material financial reporting, although they don’t necessarily need to go to the same depth of detail.

In practice, this means setting a financial materiality level, and then applying it to identify financially significant areas of the business, both in terms of material account classes and any group entities considered significant. Materiality levels are typically based on profit, revenue or balance sheet criteria, such as asset values, depending on the purpose of the business. A profit-driven business would often apply an initial materiality basis of 5% of profit before tax, whereas a not-for-profit entity might take an initial basis of 1% of turnover.

Businesses should also take into account any additional qualitative risk factors, such as complexity in accounting, judgemental areas, or historical errors, which elevate the inherent risk to any account class or group entity.

Non-financial reporting

Material non-financial reporting and related risks will be less straightforward to identify than financial reporting as it is not always a quantitative measure. The key considerations could include:

- What information reported by the business do investors and other key stakeholders rely on and what could the potential impact or implications of misstating it be. This will need to involve engaging with key stakeholders and users of the information to determine what is material to them.
- The potential impact (for example, to reputation or through financial penalties) that could occur if the information is incorrect or misleading.
- Whether there are existing, new, or anticipated, relevant reporting standards.
- Whether the information contains significant estimates or judgements.

For areas of reporting in which published guidance already exists to determine materiality such as the double materiality guidance in the European Sustainability Reporting Standards, businesses should follow the relevant guidance. Where this is not the case, businesses could consider adopting the principles from standard-setters and other relevant bodies which may be helpful to them. For example, the Global Reporting Initiative (GRI), suggests that, “Particular information is considered 'material' - or relevant - if it could influence the decision-making of stakeholders in respect of the reporting company”.

Another useful guide when considering materiality around all areas of reporting is the FRC Lab’s publication “Materiality in Practice: Applying a Materiality Mindset”.

Operational and compliance

Operational areas, in this context, are those that relate to effectiveness and efficiency of the entity’s operations, including operational goals and safeguarding assets against loss. For example, businesses may apply cyber security controls to reduce the risk of a ransomware attack occurring, or reduce the potential impact if an attack were to occur,

such as maintaining an air-gapped backup of critical information which would allow them to restore operations.

Compliance areas, in this context, are those that relate to adherence to laws and regulations. For example, businesses could recalculate wage rates based on actual staff hours worked and pay disbursed to ensure that individuals' hourly wages are greater than the statutory minimum wage.

At a practical level, most companies with a mature risk management programme will have a process to assess risks and determine their principal risks based on probability and quantum, as disclosed in the annual report, so are in effect already doing an assessment of material compliance and operational risks. Often, principal risk disclosures will be summarised or aggregated for the purpose of the annual report. Work will therefore be required to disaggregate the principal risks to a level at which specific control activities can be identified and assured. This might be done via risk registers that contain the more detailed elements of risk that form the basis for the principal risks. It could consider, for example, the part of the risk that is most likely to occur, it could be the part for which the impact is least understood or it could be the most complex or pervasive element.

The following might also need to be considered:

- Risks that may be more operational or commercially sensitive in nature that might not be included in the principal risks disclosure, but could be material to the business if not well controlled.
- Material risks to the resilience of the business and material risks related to fraud that may be disclosed in other sections of the annual report.

Below, we give an example of how a principal risk can be disaggregated into its material risk components.

A business has identified Cyber Security as one of its principal risks, articulated as, "External or internal threats executed by malicious actors, leading to a loss of data or ability to operate our systems or technology". Beneath this are a number of more detailed factors which aggregate to form the principal risk, but not all of these might be considered material. As an example, we might consider the 'material' element of the principal risk to be, "Inadequate incident monitoring or communication means the business lacks ability to detect when it has been affected by a cyber attack. This allows a malicious threat actor to infiltrate and compromise our systems undetected, and either extract data or place ransom demands". A less material element to the risk could be, "Out-of-support systems are compromised due to increased vulnerability and inadequate cyber security protection leading to compromised asset operation" if they relate to relatively isolated and immaterial elements of the business, for example.

It's worth emphasising that what is material to one business may be different to what is material for another. However, by considering principal risks in this way, the most material element(s) of the principal risk can be identified to a sufficient degree of detail that allows the relevant material controls to be subsequently identified.

Linkage with the concept of an Audit and Assurance Policy (AAP)

If companies have decided to develop an AAP or have a similar assurance mapping process, the risk assessment for the purposes of assessing the effectiveness of the systems of risk management and internal control could be done in conjunction with the scoping for the AAP. An AAP will include what is the most important reported information to the business, so could be a good starting point for determining what financial and non-financial reported information should be in scope. It would also, for most, if not all companies, include the reported principal risks, resilience information and information on fraud risks, so would also help frame the scoping of operational and compliance risks and controls.

Element 3 - Focused on the material controls that address material risks

Each material reporting, operational or compliance risk, even when disaggregated, could have a potentially large number of controls to mitigate that risk. To ensure a strong yet proportionate assessment process, businesses will need to identify the controls they consider **most** effective in addressing the risks; in other words, their 'material' controls.

Following the example material risk given in Element 2, a number of potential controls to mitigate this risk could be identified, including: the implementation of security information and event management software; the daily review of security alerts; monthly review of firewall rules and configurations to ensure they reflect new and emerging risk vectors.

For each of these controls, management will need to form a judgement as to which control, or controls, it considers the most effective at reducing the level of risk to a tolerable level. This control, or controls, would therefore be considered 'material'.

It is worth noting that Entity Level Controls (ELCs), if designed and performed to the right level of precision, can be very successful in mitigating a broad range of risks, so could be a more efficient and effective option in certain circumstances. More on ELCs in the next element.

Element 4 - Controls that are clearly articulated, and are designed and operating effectively

Material controls, once identified, should be reviewed to ensure they are designed to a sufficient level of detail. The following could be incorporated into a review of design effectiveness to determine if the control would mitigate the risk:

- The objective of the control and whether it would sufficiently mitigate the risk.
- Whether the control is preventative or detective in nature and whether it satisfies the information processing objectives of completeness, accuracy, validity and restricted access.
- The level of precision (e.g. a monetary threshold) the control will be performed to.
- Who performs the control and whether they are appropriate (clear roles and responsibilities for risks and controls should be defined, to embed accountability and ensure appropriate segregation of duties).
- How frequently the control operates and whether this is appropriate.
- Whether the control relies on a system or report and whether appropriate controls are in place over that system or report (see further discussion below on IT controls).
- Whether sufficient evidence is being retained to support ongoing monitoring and review.

The following approaches are typically adopted in undertaking a review of design effectiveness of controls:

1. Deep-dives or process walkthroughs represent an effective way of developing an understanding of end-to-end cycles or processes, and the key controls that currently exist.
2. Capturing processes and controls in flowcharts helps to visually show how controls support the process, and is an effective method of validating that information shared in walkthroughs is accurate.
3. Documenting risks and controls in a 'risk and control matrix' (RCM) to provide a clear view of the link between processes, risks and controls (as well as IT dependencies), and a clear log of the material controls relied upon and any deficiencies identified.

Entity level controls

If appropriately designed, entity level controls (ELCs) such as policies and procedures, governance structures, codes of conduct and performance management can set the tone across the organisation and help reduce the need for lower level transactional controls. As an example, to be proportionate, businesses may determine that a combination of effective ELCs and clearly defined roles and responsibilities, alongside a monthly analysis of actual financial performance vs budget, and monthly reconciliation of key account balances, is sufficient to provide evidence that certain balances are not materially misstated and that material financial reporting risks are being mitigated. Provided these reviews are robust, precise, well documented and independently tested, it may be determined that more transactional level controls are less important to mitigating the relevant financial reporting risks. In a similar way,

robust ELCs could support other reporting, operational or compliance processes in combination with other suitably designed controls.

IT Controls

It is common for systems and IT processes to be used across the reporting processes as well as across operational and compliance processes. The role, therefore, of IT automated, IT dependent and general controls as part of an effective controls framework needs to be considered carefully. For systems that are material to the reporting, operational or compliance process and which will be substantially relied on to perform controls, management should consider documenting IT general controls for those systems, and incorporating them into assurance plans.

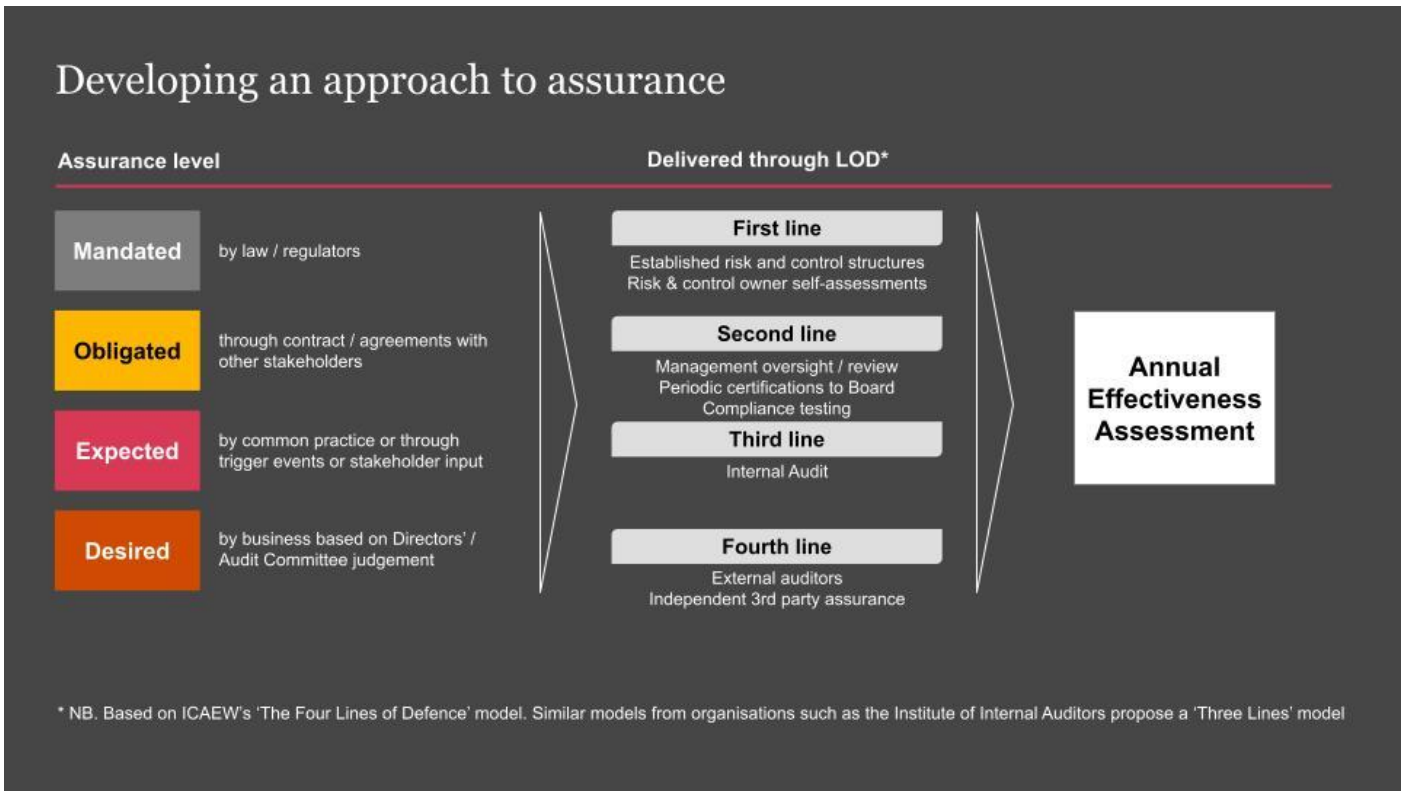
Evidence of operating effectiveness

As part of their process for monitoring and reviewing the effectiveness of their systems of risk management and internal control, as described below, it is likely most companies will implement some form of independent testing. Therefore,
it will be important to retain evidence of the controls operation. Transactional level controls might be capable of being tested in real time, but for other controls where this is not the case, evidence will need to be retained to evidence that the control has been performed.

Element 5 - A well thought out approach to assurance

Up to this stage, it is likely the control operators and management have been involved in the identification and operation of the material controls. As part of their monitoring and review process, the board will need to consider the level and mix of process and assurance, both internal or external, which they consider sufficient. They will need to consider how comfortable they are relying on self certification of controls design and operation and the extent of independent testing and assurance (internal or external) needed.

It is important to note that, while still contributing to the overall evidence of the effectiveness of the systems of risk management and internal control and providing a source of assurance, activities performed at the first, second and third lines of defence will not provide assurance against a formal assurance standard in the same way that an external audit provider or other independent 3rd party assurance provider does. For these reasons, as part of their monitoring and review process, care will need to be taken by the board when considering the nature and extent of the work being performed under the four lines of defence as part of their monitoring and review process.



In determining their assurance needs, boards will need to consider whether there are areas of reporting or operational or compliance risk that they will be required or could be expected to have assurance over, as well as areas where they, as a board, would like assurance, for example:

- **Mandated assurance** which is required of the business by law or regulation.
- **Obligated assurance** which the business is required to obtain by virtue of contracts or other arrangements that it has entered into that include a requirement for assurance over some aspect.
- **Expected assurance** which the business *should* obtain as, whilst there is no obligation to do so, it is considered common practice in its particular sector or industry, or may be expected by virtue of recent events triggering a need, or through stakeholder demands.
- **Desired assurance** which the directors and/or audit committee want to obtain based on their judgement. This could be based on:
  - The relative immaturity of the process underpinning the reported information or risk mitigation.
  - The impact on resilience of the business should a risk event happen.
  - The likelihood of the risk event happening.
  - The likelihood of reported information being incorrect and the impact this could have on shareholder decisions.

Once the assurance needs have been established, an effective assurance plan can be developed. An effective approach could be to follow the Line of Defence model as outlined by the ICAEW that comprises a combination of activities across the four lines of defence. Under this model, as an example, a potential assurance plan could comprise:

- **1st line of defence**
  - Established risk management and control structures - The basic line of defence will be the risk management and internal control structures in place. These should be well documented and understood throughout the organisation.
  - Regular self assessment by control owner - First line control owners assess the operating effectiveness of the risk management system and material controls in their area of the business, retaining evidence of control operation that supports their assessment, and attests to their Heads of Department.
- **2nd line of defence**
  - Review of the risk and control self assessment - The self assessments are reviewed by Heads of Department and issues followed up on a timely basis. How often this happens could be determined by factors such as the relative maturity of controls; the regularity with which they are performed; or whether weaknesses or issues have recently been identified or remediated.
  - Control indicator monitoring - Key indicators of effective risk management and internal control operation are agreed and reported to and monitored on a periodic basis by Heads of Department.
  - Periodic certification - Heads of Department make a periodic certification to the board confirming applicable controls are operating effectively or if failures have been identified.
  - Compliance reviews - Material controls are subject to sample testing, performed by a 2nd line compliance or assurance team. This could focus on whether controls continue to be designed and operated in line with the related risk.
- **3rd line of defence**
  - Internal audit - Independently determined internal audit programme including cyclical testing of the risk management and control systems as a whole, and specific testing performed over material controls (including particular higher risk areas in the year, such as transformation projects or new accounting standard).
- **4th line of defence**
  - 3rd party independent assurance - A 3rd party provides assurance over the specific reported information or risks in line with relevant reporting standards.

Independent testing

As we describe above, in our view, a robust process for evaluating the systems of risk management and internal control should include some degree of independent testing by internal audit or even, potentially, an external assurance provider when there is an increased need for assurance. Independent testing performed by internal audit should use a targeted, risk-based approach and could include some degree of cycle testing, so as to remain proportionate. Controls which could be considered for more regular testing might include:

- Where there have been previous issues or control failures.
- Areas where there is significant change (new processes, systems or controls).

The key will be that the testing is not performed by individuals who are in the same function or reporting line. The testing should also focus on design of controls and robustness of documentation as well as evidence of proper operation.

Sample sizes

The number of samples tested should be linked to the instances of control operation. This will depend on management or the board's judgement, but there is some publicly available guidance that could help. For example, ICAEW technical release AAF 01/20 (Appendix 6) provides, amongst other things, sample size guidance for testing controls at a service organisation. It states that, where a control operates on a daily basis, 20, 30 or 40 samples could be tested to prove operating effectiveness; for monthly controls this could be a sample of 2-5; quarterly could be 2; and annual could be 1. The specific number of samples required will align with the assessed level of risk. It is key, however, that samples should be obtained at intervals throughout the reporting period.

External assurance over internal controls

As we describe above, assurance needs might include formal assurance to a recognised standard, provided by an external assurance provider. This could be over the actual operating effectiveness of the risk management and internal control systems, but care must be taken in determining the scope of this type assurance. The scope of the board's responsibilities is far reaching and goes beyond that of financial reporting (which is the limit of the scope of US SOX) and into non-financial reporting, operational and compliance areas.

Therefore in seeking external assurance in this area, the scope of the assurance activities would also need to go beyond that of financial audit. A more likely scenario is that management may determine that external assurance will be obtained over certain aspects of the internal control system e.g. cyber security, company or industry specific regulatory compliance or indeed reporting (financial or wider). In any case, before external assurance can be provided, the assurance provider must be confident that the subject matter is 'assurable'.

Robust systems of risk management and internal control would certainly go a long way towards establishing an assurable outcome, and in the case of financial reporting assurance, would not necessarily have to be as prescriptive as US SOX. Whether additional assurance scope or evidence would need to be provided, however, will depend on individual companies' facts and circumstances.

Element 6 - Detailed and transparent reporting

When the board reports on the outcome of its monitoring and review process in the annual report, and the basis for its conclusion on effectiveness, in our view, this would include:

- A detailed description of the process undertaken, including how materiality was determined; how material reporting, risks and related controls were identified; the board's approach to assurance; and how the lines of defence have been deployed, including any use of independent testing.
- A description of why this process is considered appropriate for the company's circumstances.
- An explanation of any material failures identified and actions taken by the board to address them.

At a practical level, the results of monitoring and review activities across the lines of defence will need to be reported in an integrated way, to provide a 'big picture' view of whether material risks are being managed effectively, and to identify any material failures.

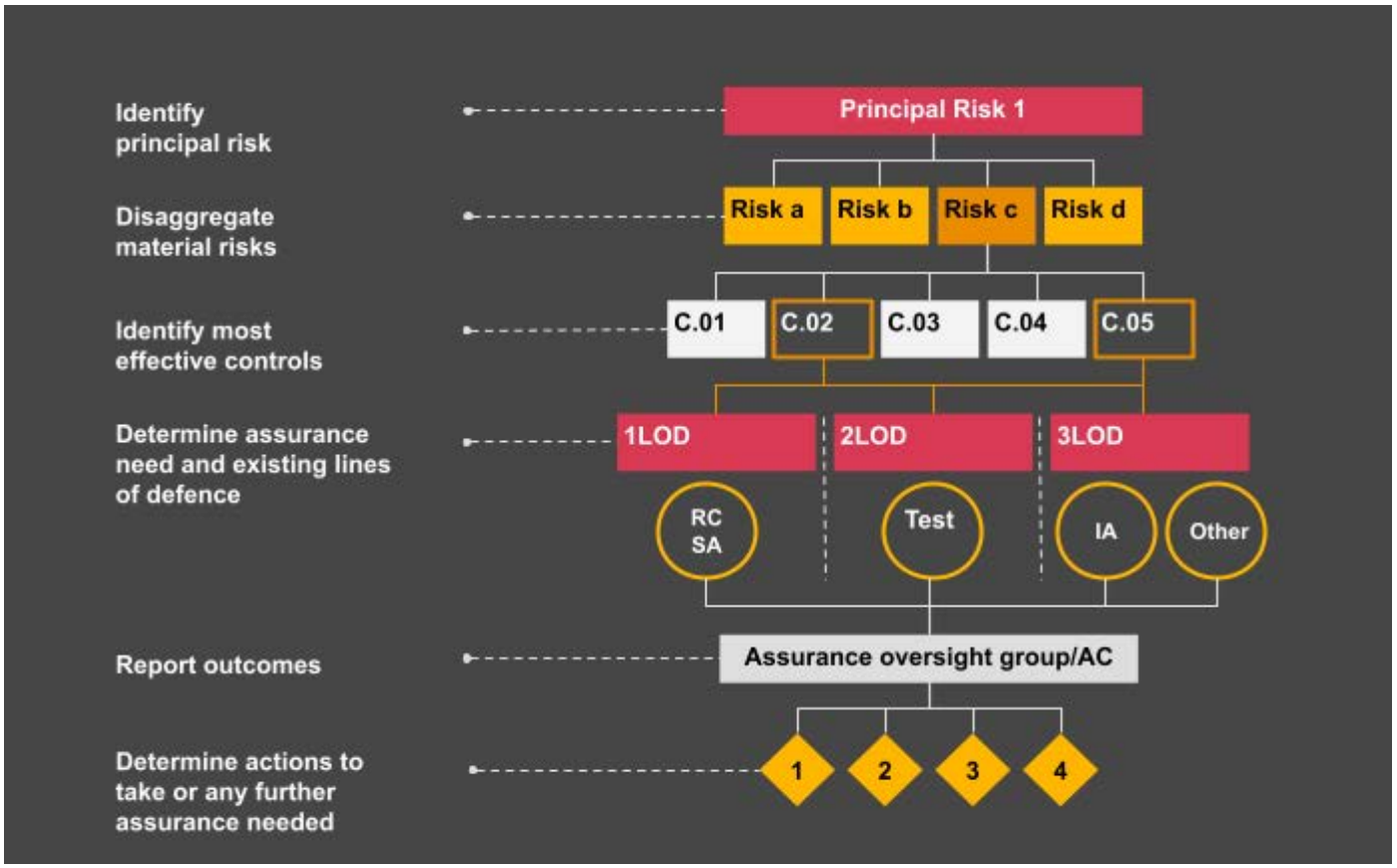
Risk management and internal control and the statutory audit

It is worth reiterating that while auditing standards require that the statutory auditor assess the design and implementation of certain financial reporting controls in specific circumstances, for example, if the controls relate to a significant risk, they do not require that the auditor test the operational effectiveness of those controls (unless they plan to rely upon the controls as part of their audit approach).

However, it is possible that auditors will want to check the consistency of the board's reporting on risk management and internal control with their knowledge from the audit. They might also request evidence of appropriate design and implementation of entity level controls surrounding this reporting. It is likely this would be limited to financial reporting controls as financial reporting is the focus of the audit, although auditors might also consider controls around fraud risk and resilience. Where the auditor has performed work over internal controls, challenges will arise if the auditor has a different view of the design, implementation and operating effectiveness of controls, arising from their audit work, in particular if they believe there are deficiencies that could be considered material but management does not agree.

Worked example

The following illustration is a worked example of how the six elements outlined above might come together in practice.



Taking our earlier example of a cyber security risk, the following process may be applied:

A. The relevant **principal risk** which we are focussing on (cyber security) has been identified as "External or internal threats executed by malicious actors, leading to a loss of data or ability to operate our systems or technology".

B. The risks, or risk elements, which underpin this top-level principal risk are then identified: this may be through reviewing function-level risk registers, or those which contain the underpinning information which principal risks are aggregated from. For the purpose of our example, we have identified a number of risks elements:

Risk (a) - Inadequate incident monitoring or communication means the business lacks ability to detect when it has been affected by a cyber attack. This allows a malicious threat actor to infiltrate and compromise our systems undetected, and either extract data or place ransom demands.

Risk (b) - Out-of-support systems are compromised due to increased vulnerability and inadequate cyber security protection, leading to compromised asset operation.

Risk (c) - Intentional or unintentional errors in software security configuration renders the business more vulnerable to threats which could result in data loss.

Risk (d) - Appropriate physical security is not implemented around assets rendering them vulnerable to being compromised by malicious actors on site.

C. As there are several risk elements underpinning the principal risk, management must consider their business's circumstances and judge which, possibly based on impact and likelihood, are 'material' and focus on these. In our example, we will assume that Risk (c) is our 'material' risk as this is the risk which the business has determined is most likely to occur, and would have the greatest impact.

D. Controls that mitigate the material risk are then identified and documented. Each of these controls should be evaluated to consider which is the most effective in terms of mitigating the material risk: in turn, these will be considered to be the material controls. In context of the material risk, the following control areas are identified, with the second and the fifth considered 'material':

C.01. Restricted access to out of support systems

C.02. Changes to security configurations are reviewed and approved before being effected

C.03. Restricted access to adjust security configurations

C.04. Rolling programme of penetration testing

C.05. Regular backup of critical data to air-gapped devices (ie. devices that are physically segregated and incapable of connecting wirelessly or physically with other computers or network devices)

E. Management should define their assurance need in respect of material controls, outlining what this means in practical terms with respect to the types of assurance which could be gained, and from which line of defence, and how frequently.

F. They should then consider the assurance sources that are already in place (internal and external), and consider additional assurance (again, internal or external) if needed.

G. Once performed, the outcomes of assurance provision and any recommendations for actions to take should be reported to the relevant oversight body, according to the established governance and accountability structure. This could be the audit committee or a working sub-group to whom responsibility has been delegated to oversee assurance arrangements for a particular area (or areas), and who are authorised to instruct management to take additional actions.

.

RITM14452612