RISK MANAGEMENT DEEP DIVE Guidance

CPCA Audit & Governance key considerations

THE POWER OF BEING UNDERSTOOD
AUDIT | TAX | CONSULTING

CAMBRIDGESHIRE & PETERBOROUGH COMBINED AUTHORITY

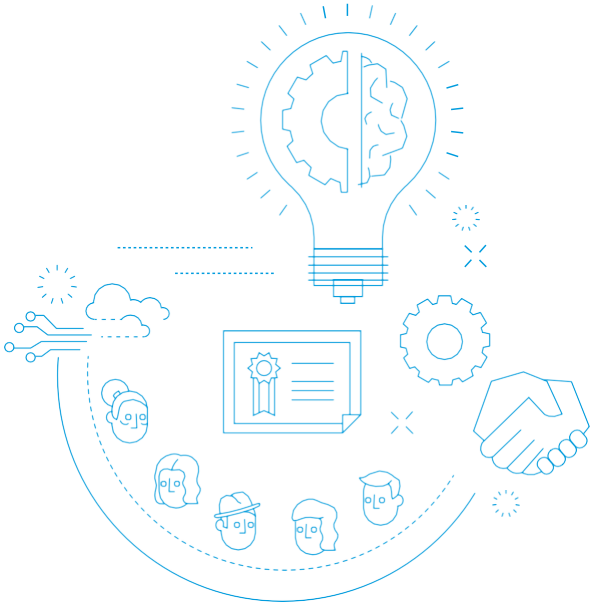
RSM

Risk Management Deep Dive Guidance

Key steps

1) Be clear on the purpose and approach of the deep dive.
2) Make suitable preparations for a deep dive.
3) Focus the deep dive on a strategic risk or matter.
4) Understand the strategic risk.
5) Understand (explore) the effectiveness of current controls.
6) Understand (explore) the effectiveness of planned actions.
7) Understand (explore) the basis of assurance
8) Provide appropriate challenge.

Document outcomes – actions to be taken, communicate and follow up.

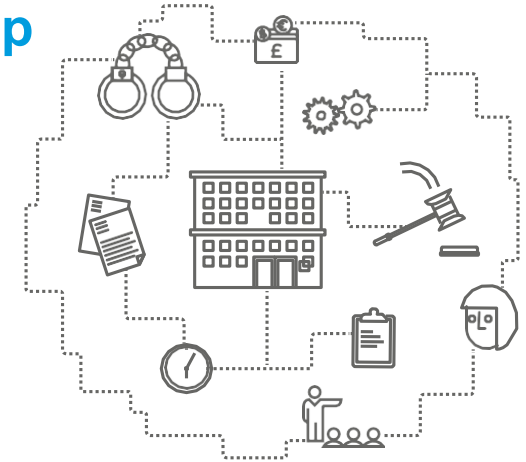


CAMBRIDGESHIRE & PETERBOROUGH COMBINED AUTHORITY

RSM

Why perform risk management deep dives?

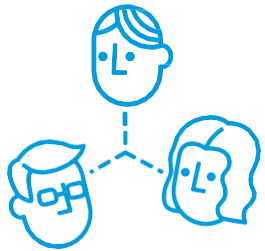
1. Be clear on the purpose and approach of risk deep dives



- Allow CPCA Audit & Governance Committee to undertake a comprehensive review of a strategic risk.
- Allows for information in the strategic risk register to be elaborated upon, such as details on assurances around controls, as well as implications on the objectives, strategies and plans that are being pursued.
- Provide the opportunity to challenge the contents on the strategic risk register to ensure it is appropriate, in particular the effectiveness of the controls in place and the progress of actions to better improve the management of risk.
- Assists in identifying further steps that may be required.
- Demonstrates that the Audit Committee take the management of risk seriously.

Undertaking risk management deep dives

2. Make suitable preparations for a deep dive



- Where does the deep dive take place? – as part of the Audit Committee meeting or outside?
- Agree strategic risks or topics to be discussed at Audit Committee (this can be undertaken in conjunction with the Board). Usually one per committee meeting and scheduled in advance.
- Audit Committee members to refresh themselves on the organisations current risk appetite prior to each risk deep dive. This will ensure that discussions and questions remain relevant and to the point.
- Agree who should attend the Audit committee and participate in the deep dive and why.
- Ensure the strategic risk information is up to-date.
- Audit Committee members to review the latest risk register in advance of the committee meeting to familiarise themselves with the particular risk subject to facilitate the deep dive.

Risk management deep dive – the area of risk

3. Focus the deep dive on a strategic risk or matter

- Why was this strategic risk chosen for a deep dive?
- Why is the risk on the strategic risk register?
- **Context of the risk:**
  - alignment with corporate plan, projects, audit findings
  - recent problems/incidents
  - other underlying issues
  - consider the risk in context of sub risks, i.e. causes and consequences
  - emerging events or matters elsewhere (within / outside of the sector) that are a cause for concern.
- Have there been any changes to the above that have impacted the risk positively / negatively recently?
- Consider are assumptions realistic and can they be substantiated?
- How did the elements above influence the scoring of the risk? And does the risk score remain reasonable – inherently? residually and target?

Risk management deep dive - coverage

4. Understand the strategic risk

Understand the strategic risk

- The strategic risk description, the current circumstances, drivers (or causes).
- The implications or effects of the strategic risk on the objectives of the business.
- Why the risk is scored as it is.

Understand the effectiveness of the current controls and planned actions

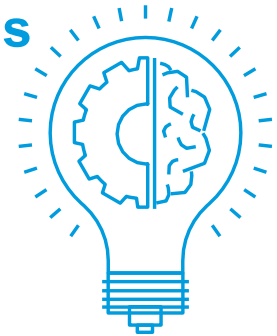
- What current controls exist, how they are used to manage the risk and their effectiveness.
- What actions or planned activities are to be undertaken to help better manage the risk, progress made and outcomes.

Understand the basis of assurance

- What assurances and evidence is available to support conclusions reached around controls effectiveness and progress / outcomes of actions.
- The cycle of management monitoring and review arrangements that are applied to the risk as part of reporting and oversight.
- Provide a forwards look, to the best of knowledge, as to how the risk and the controls etc might be affected by events on the horizon.

Risk management deep dive – current controls

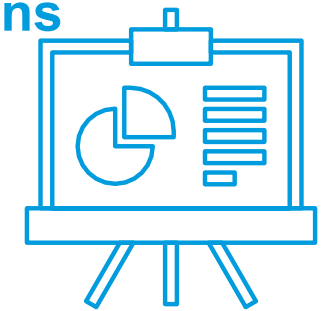
5. Understand (explore) the effectiveness of current controls



- What existing mitigating activities and / or controls are already in place? – if there are many focus on those that are key.
- Be clear about whether the mitigating activities/controls affect the likelihood of the risk occurring or if they help address the impact.
- Explain how you are assured that the mitigating activities take place and controls are in operation.
- Further explain how effective the mitigating activities and controls are by referencing to the risk assessment scores.
- Reference how the current risk assessment scores fit in with current risk appetite,
- Provide examples of realised benefits to demonstrate the effectiveness of the mitigating activities/controls.
- Be mindful if scores have changed since the last time Audit Committee reviewed the register, explain why.

Risk management deep dive – planned actions

6. Understand (explore) the effectiveness of planned actions



- How will these actions help improve the management of the risk?
- Reference how the current risk assessment scores fit in with current risk appetite and explain whether there is need for further activities or controls?
- And if not, why not?
  - Reference to realised benefits
  - Does effort/resources not outweigh further benefits, i.e. the risk assessment doesn't reduce significantly
  - Are there any limitations or constraints?
- If the risk assessment score needs to be reduced further, explain:
  - What you are going to do, and by when?
  - How will this affect the risk assessment scores both in terms of likelihood and impact?
  - What assurances will be available to confirm that the new mitigating activities / controls are effectively managing / minimising the occurrence of the risk?

Risk management deep dive - assurances

7. Understand (explore) the basis of assurance

What assurances exist?

- Who provides the assurance? What is the evidence base? How reliable is this?
- What is the frequency of this assurance?
- What are the outcomes of assurances provided? What does this tell us about the effectiveness of controls?
- What action is being taken to address weak levels of assurance? Or no where there are assurance gaps?

What is the cycle of management monitoring and review of the risk, controls and actions?

- When does this occur?
- Who is involved? Is this management? Sub-committee?
- How does this take place? And what enquiries are made?
- What have been the outcomes to-date?

How could this assurance provision change in the future?

- What future events within the business might impact on the risk, controls and actions? And what will be the impact? when?
- What changes will be required to ensure the on-going management of the risk or assurance provision?
- How will this affect the risk assessment scores both in terms of likelihood and impact
- What will this mean to the business risk appetite? And decision making in the future?

Risk management deep dive – challenge

8. Provide appropriate challenge (examples)

- How satisfied are you that the strategic risk is accurately described?
- What is the risk appetite for this risk? And why?
- How well is this risk understood within the wider business? How can this be evidenced?
- How content are you that the controls identified manage the risk? And what is this based on? How can this be evidenced?
- How satisfied are you that the planned actions will improve the management of the risk? And how content are you with the progress of actions? How can this be evidenced?
- What changes do you foresee that could impact on this risk and how?
- What further assurances could be obtained / would you like to obtain?
- Beyond what is already identified what further could be done to better manage or control the risk?

Document outcomes, assign actions, follow up - completed through Audit & Governance meetings, with action log and minutes produced.

CAMBRIDGESHIRE & PETERBOROUGH COMBINED AUTHORITY

RSM