Audit Planning risk assessment

Presentation to PEMPAL meeting 22-24 April

Richard Maggs

Some background on me

- I have worked in audit all my main career which I finished as the Director General for the UK National Audit Office responsible for international work
- My work has included many development projects in central and Eastern Europe with both external and internal audit
- I have also helped developing countries and United Nations Organizations to develop COSO based internal control and accountability frameworks
- I have written a lot of guidance for auditors and managers on risk assessment and internal control in general
- I think that PEMPAL is a great initiative for sharing best practice and I am happy to support it!

What I was asked to do

- I was asked to:
  - Review the Document – periodic risk assessment by internal audit – produced by working group
  - Review the comments of the members of the group on the document (to be covered in a separate presentation)
  - Provide my own comments on the document to the working group
  - Suggest changes to the document based on the views of the working group

My overall conclusions

- The draft document is very good and has clearly been subject to a lot of thought and input
- I agree with many of the issues and suggestions contained in the document and the further comments for change from the working group
- I think that some small changes to the proposed steps for risk assessment would make the subject easier to follow and apply
- I have therefore suggested a new set of steps for audit risk assessment to be used in a new draft document

The draft document

- This is a good piece of work. The main changes suggested that would improve the document are:
  - Small changes in the conceptual framework (the five steps) to make these easier to follow and apply
  - More precise definitions of risk, risk factors risk criteria and the categorization of risk
  - The addition of examples and tips for auditors drawn from public sector examples
  - The use of simpler language that is easier to understand
  - A clearer link to planning
  - A recognition that there will be limited risk management processes in Departments

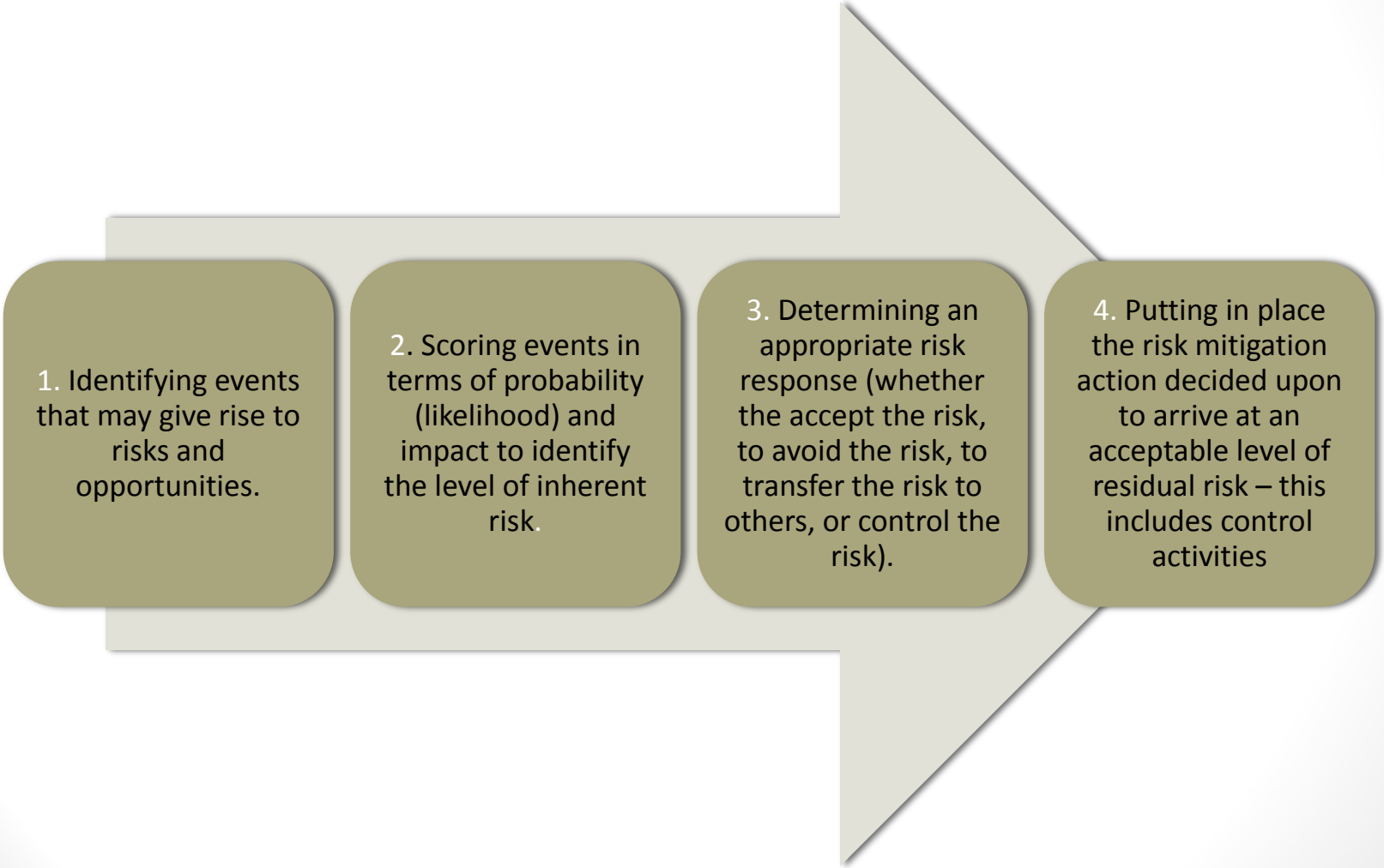
A few general comments about risks -1

- Risk is a concept that is fundamental to both good management and good audit.
- But (a) it is easier to understand from an event perspective
  - Most people understand what an event is – these are things that happen e.g. a power failure, flooding, etc
  - Risk is a word that always has to be defined to be understood
- And (b) it must be considered against an objective
  - You cannot identify risks unless you know what you are trying to achieve.
- The risk definition in your paper makes this clear
  - *"**Risk** is the possibility that an event will occur and adversely affect the achievement of an objective"*

A few general comments about risks – 2

- Managers and auditors look at risks for different reasons
  - **Risk management** is (or should be) an integral part of internal control and is the responsibility of management. It is a structured process where managers examine likely future events and the risks and opportunities these represent to the achievement of their objectives.
  - **Periodic audit risk assessment** is part of planning and a process where auditors consider likely future events and the risks and opportunities these represent to the achievement of the objectives of elements of the audit universe. This is done to ensure that audit resources are addressed to the audit of areas of highest risk to the organisation.
- If there is good risk management and risk registers these can be used by the auditor in their own audit risk assessment
- If these do not exist the auditor still needs to assess risks

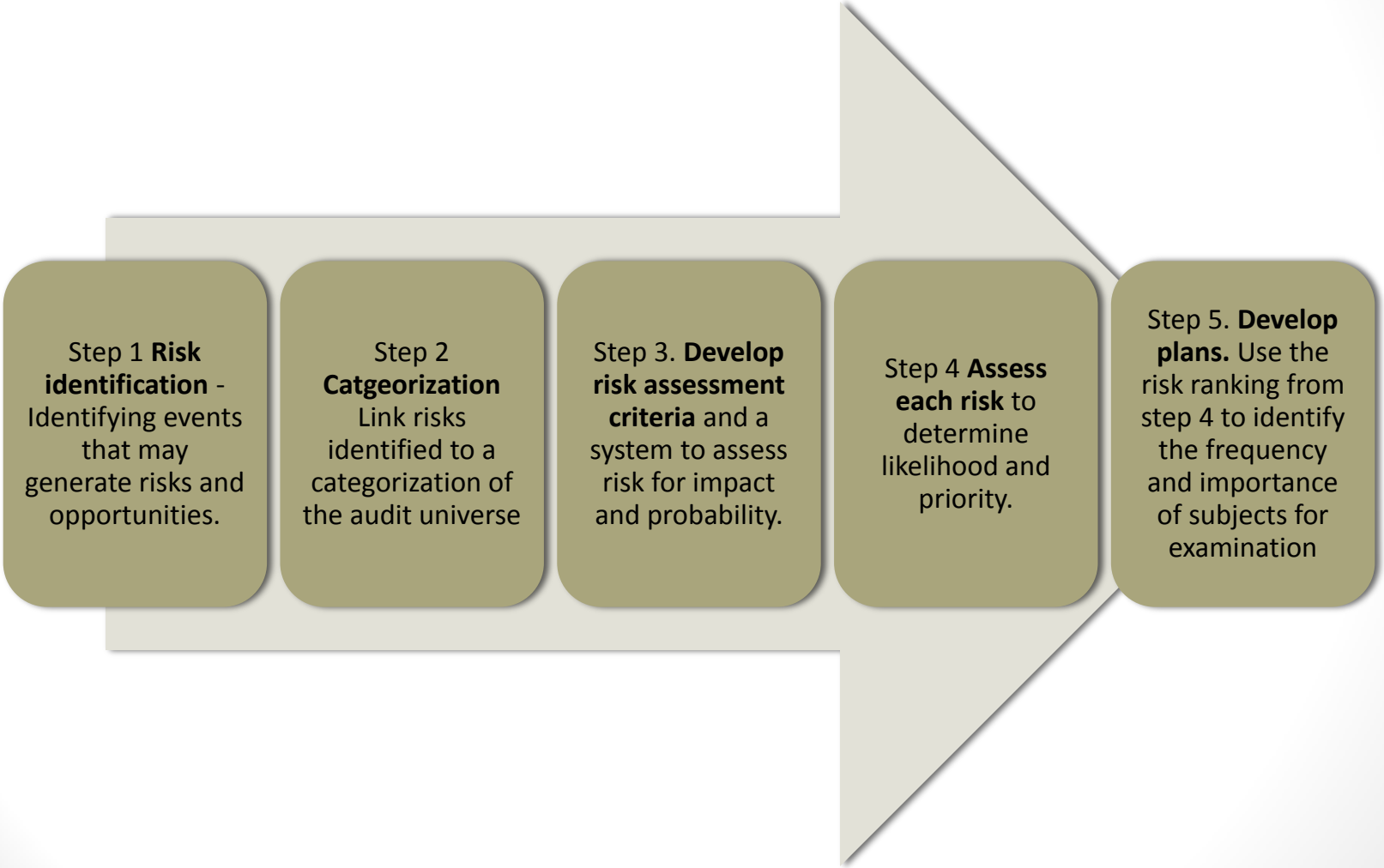
Risk management is a process with four distinct elements



Conceptual framework (five steps) proposed for managing audit risk assessment

- The conceptual framework is the five steps proposed in the document
- My review of the working group's comments suggest that these steps could be changed for the following reasons
  - To relate the steps more clearly to the common steps used for risk management
  - To include a specific first step on identifying risks
  - To link better to the audit universe in terms of categorisation of risks
  - To combine the two steps proposed for measuring impact and probability
  - To include a final step on how the results of the assessment are turned into risk based
- The next slide shows the new steps I would propose

Proposed conceptual framework (five steps)



Impact on the document

- The use of different steps would require a redrafting of the document and moving some of the text already prepared
- The addition of tips and examples for auditors would make the document easier to understand and to use as a template for CHU general guidance and for heads of IA units in terms of planning work
- I would be happy to work with the Internal Audit CoP to make these changes

Thanks

- Many thanks for the opportunity to work with old friends and make new friend through PEMPAL
- Sorry I could not be with you in person but I hope to join you on Skype to answer questions