



**Murdoch**  
UNIVERSITY

# IT Project Management

Topic 9

## Risk Management



# COMMONWEALTH OF AUSTRALIA

Copyright Regulations 1969

## WARNING

This material has been reproduced and communicated to you by or on behalf of Murdoch University pursuant to Part VB of the Copyright Act 1968 (the Act).

The material in this communication may be subject to copyright under the Act.

Any further reproduction or communication of this material by you may be the subject of copyright protection under the Act.

Do not remove this notice.

# READING

Schwalbe Chapter 11



# LEARNING OBJECTIVES

At the end of this topic you should be able to:

- ✓ **Define** what risk is & the importance of good project Risk Management
- ✓ **List** common sources of risks in ICT projects
- ✓ **Describe** the risk identification process & the main outputs (Risk ID/Register)
- ✓ **Discuss** key elements involved in risk management planning
- ✓ **Discuss** the qualitative and quantitative risk analysis processes
- ✓ **Explain** how to calculate risk factors & create probability/impact matrices
- ✓ **Understand** issues such as the use of decision trees, simulation, and sensitivity analysis to quantify risks
- ✓ **Provide examples** of different risk response planning strategies
- ✓ **Discuss** what is involved in risk monitoring and control.

# TODAY'S SESSION IS IN 3 PARTS

## INTRODUCTION

(What is Risk Management  
& Why is it important?)

## KEY TERMS & PRINCIPLES

## THE RISK MANAGEMENT PROCESS



# INTRODUCTION

## WHAT IS RISK MANAGEMENT & WHY IS IT IMPORTANT ?

### INTRODUCTION

(What is Risk Management  
& Why is it important?)

KEY TERMS &  
PRINCIPLES

THE RISK  
MANAGEMENT  
PROCESS



# WHAT IS A RISK ?

What is  
Risk  
Management?

**Individual Risk** is defined as:

- ✓ 'an **uncertain event or condition** that, if it occurs, has a **positive** or **negative** effect on one or more project objective'

**Project (Overall) Risk** is defined as:

- ✓ 'the effect of uncertainty on the project as a whole... **more than the sum of the individual risks** within a project... & represents the **exposure of stakeholders** to the implications of variations in project outcomes'

A **Risk Event** occurs when that risk happens

# WHAT IS RISK MANAGEMENT?

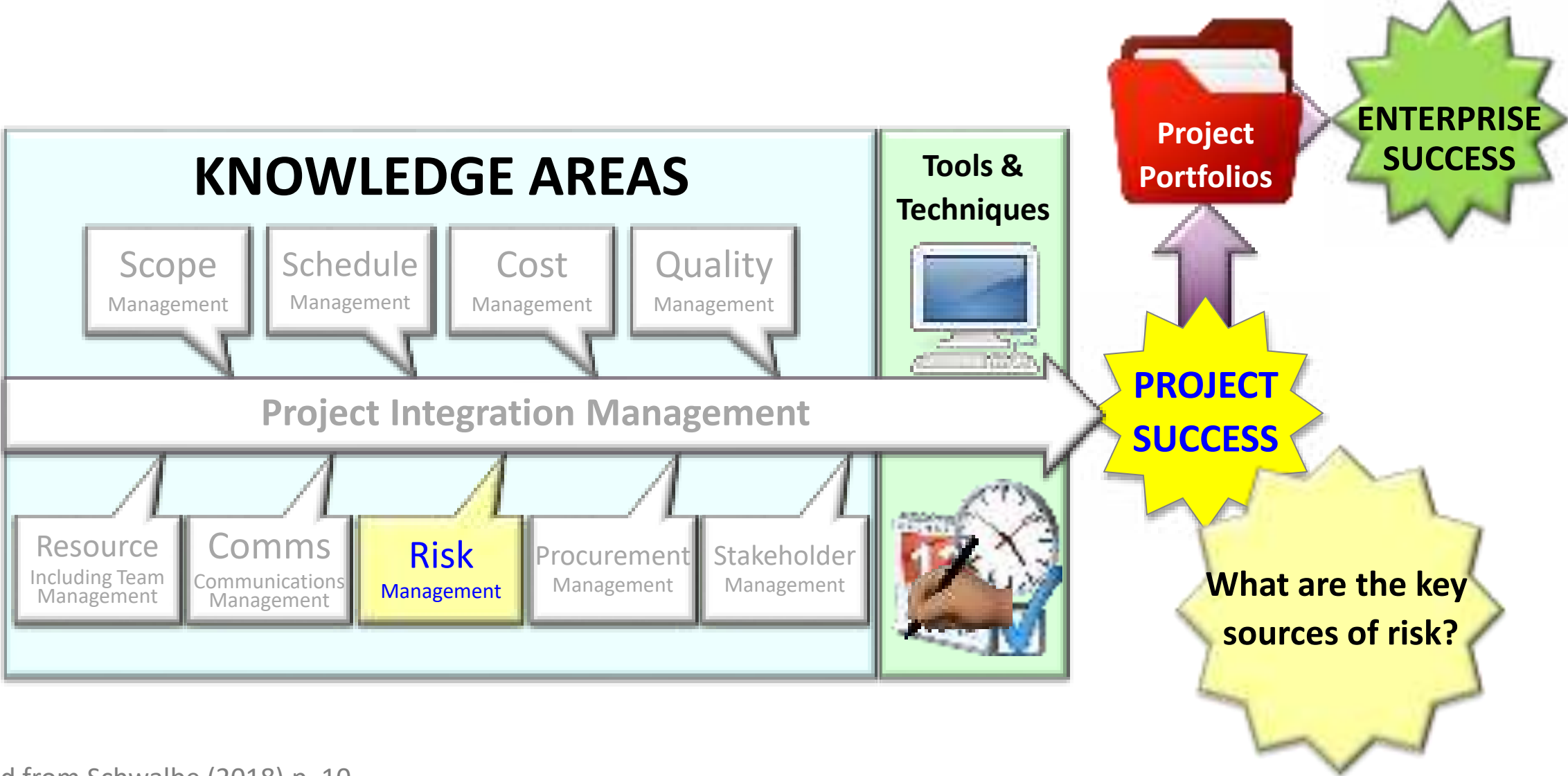
*Risk management is ...*

- ✓ An **iterative process** for identifying, analysing, handling (responding to) and monitoring/controlling risks.
- ✓ Each facet of Risk Management must be **planned and applied consistently throughout a project**

**How does this  
fit into PMBoK?**

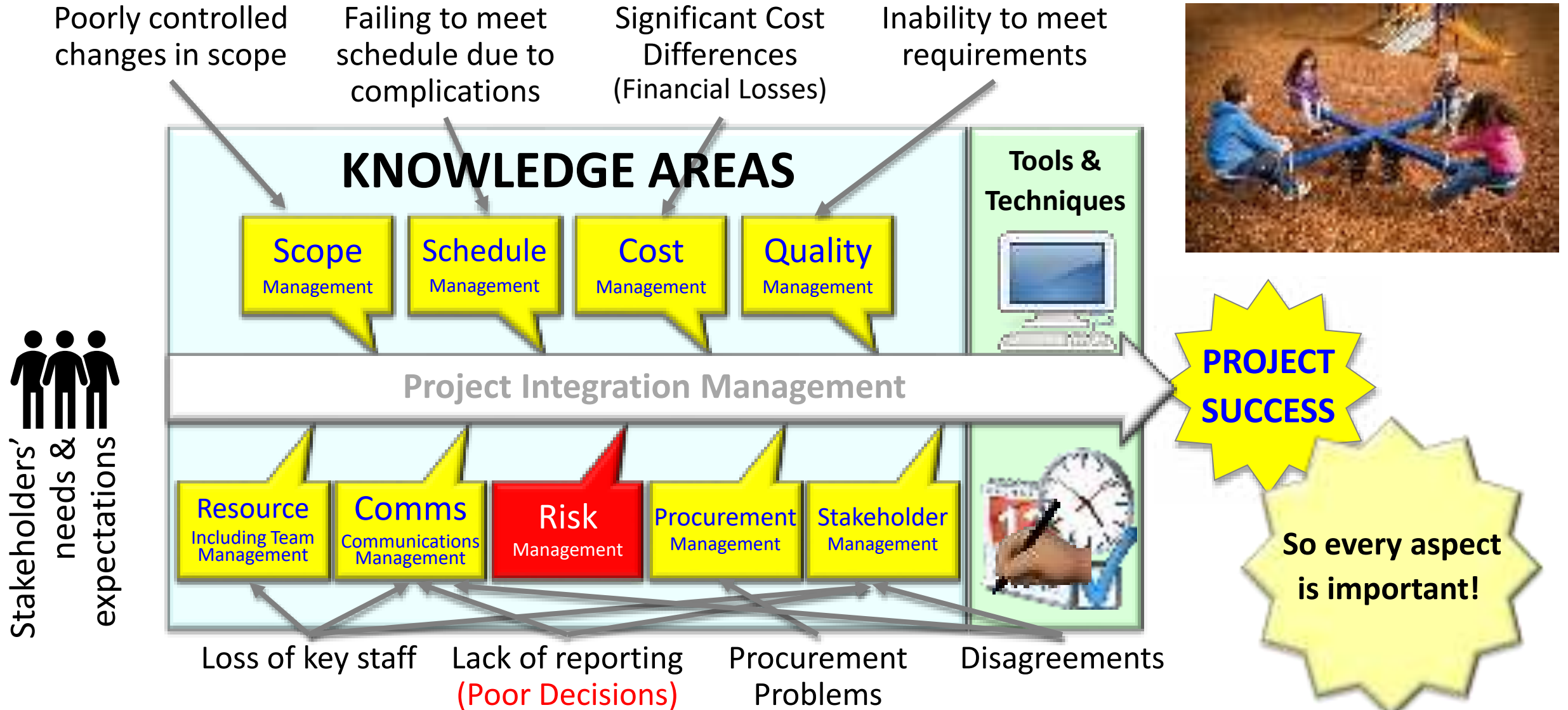


# OVERVIEW - PMBOK APPROACH

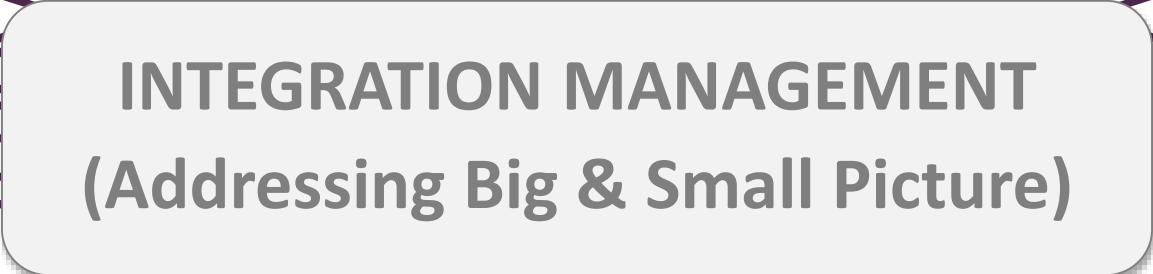
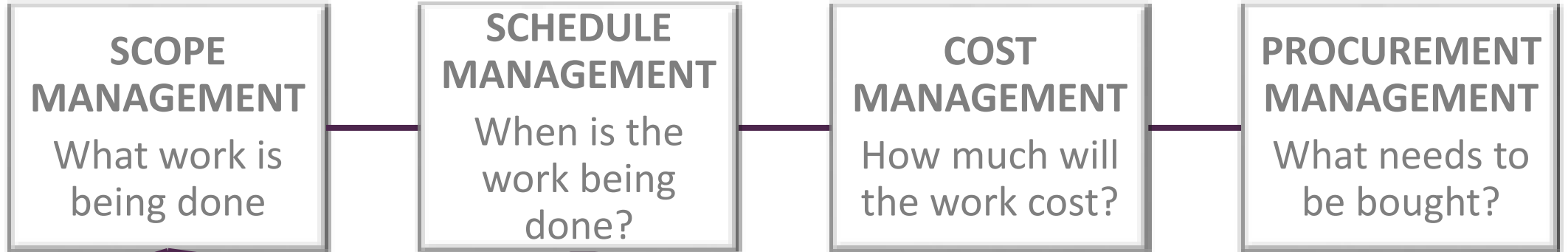


Source: Adapted from Schwalbe (2018) p. 10

# KEY SOURCES OF RISK



# THE KNOWLEDGE AREAS



# KEY TERMS & PRINCIPLES

## INTRODUCTION

(What is Risk Management  
& Why is it important?)

## KEY TERMS & PRINCIPLES

THE RISK  
MANAGEMENT  
PROCESS



# KEY TERMS & PRINCIPLES

- ✓ There are different *categories/dimensions* of risk (these affect the Knowledge Areas)

## Internal/Direct

- ✘ Structure/Process/Method
- ✘ Technical/System
- ✘ Stakeholder & Comms
- ✘ Financial/Costs

APPLY DIRECT CONTROLS

## External/Environmental

- ✘ **PEST** (*P*olitical, *E*conomic, *S*ocial, *T*echnology)
- ✘ Market Forces/Competitors
- ✘ Clients (*D*emands/*U*sage/*e*tc.)

OFTEN LITTLE CONTROL

# KEY TERMS & PRINCIPLES

- ✓ Risks can be **positive** or **negative**



Positive risks open up **opportunities**

They are handled by:

- ✓ **Accepting the risk** & **helping to make it happen**
- ✓ **Exploiting the opportunity**
- ✓ **Sharing the risk** – so the impact is increased
- ✓ **Enhancing the risk** to increase its positive impact

# KEY TERMS & PRINCIPLES

- ✓ *Risks can be positive or negative*



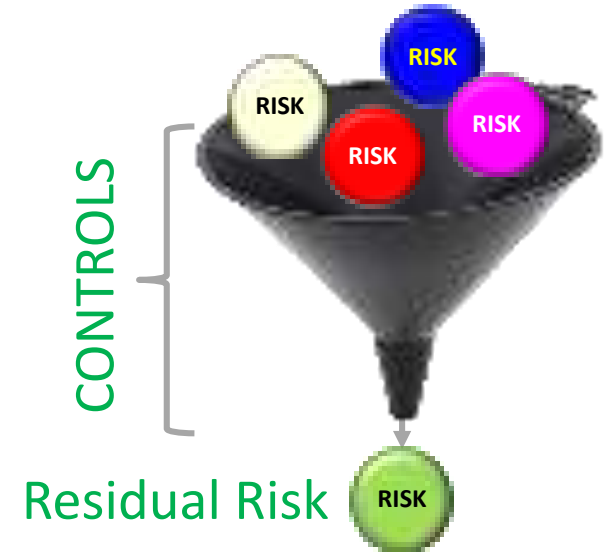
*Negative risks are **problems/threats***

*They are managed with these strategies:*

- ✓ **Avoid** – *Eliminate the threat to protect the project*
- ✓ **Transfer** – *Shift the risk to another party*
- ✓ **Control** – *Manage variables that lead to the risk*
- ✓ **Mitigate** – *take steps to reduce the impact*
- ✓ **Accept** – *Understand the risk & only take action if it happens*

# KEY TERMS & PRINCIPLES

- ✓ ***Residual Risks.*** Risks that remain after all of the management strategies have been implemented
- ✓ ***Secondary Risks.*** Risks created by implementing the risk response/management





# KEY TERMS & PRINCIPLES

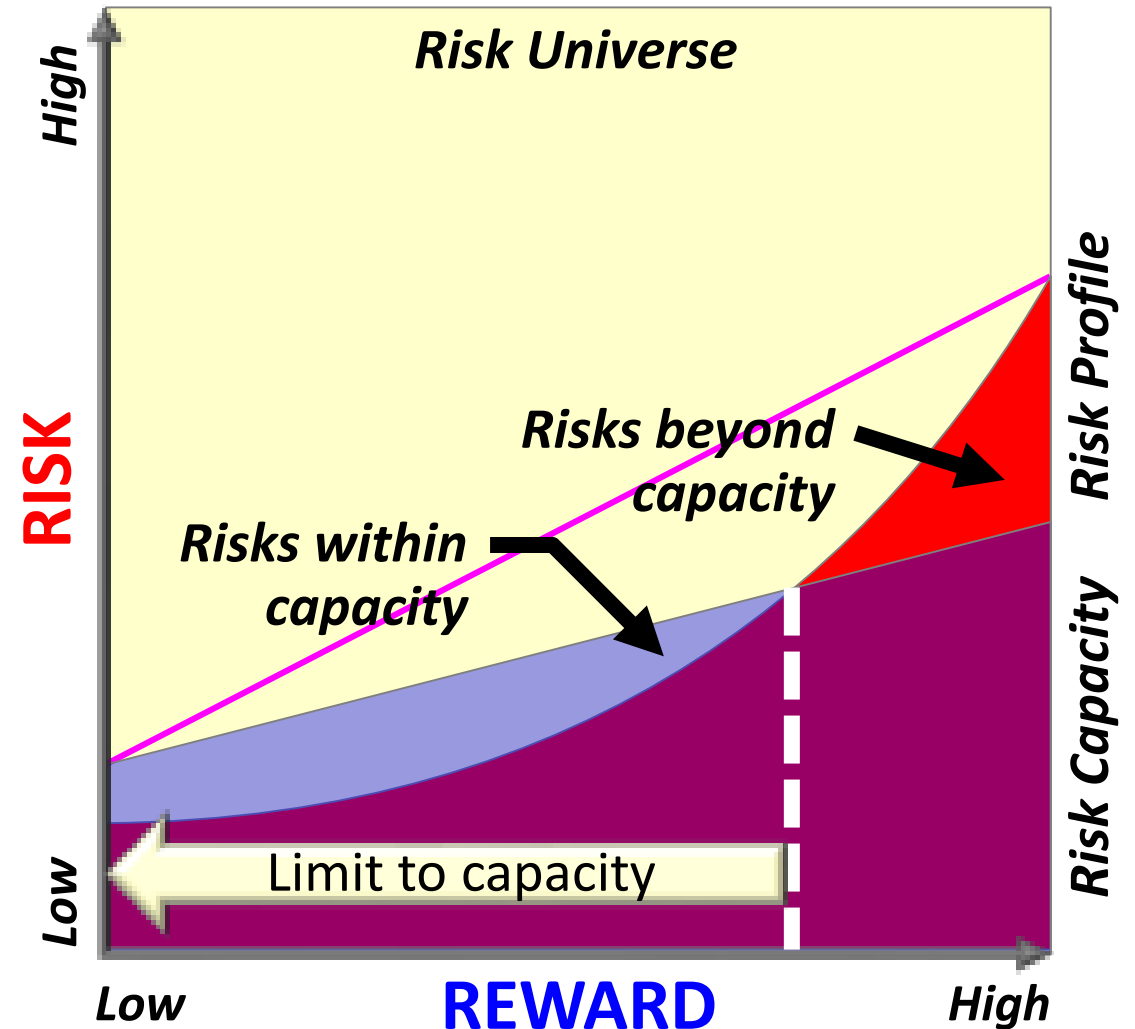
- ✓ *Risks are managed in the following framework*



# KEY TERMS & PRINCIPLES

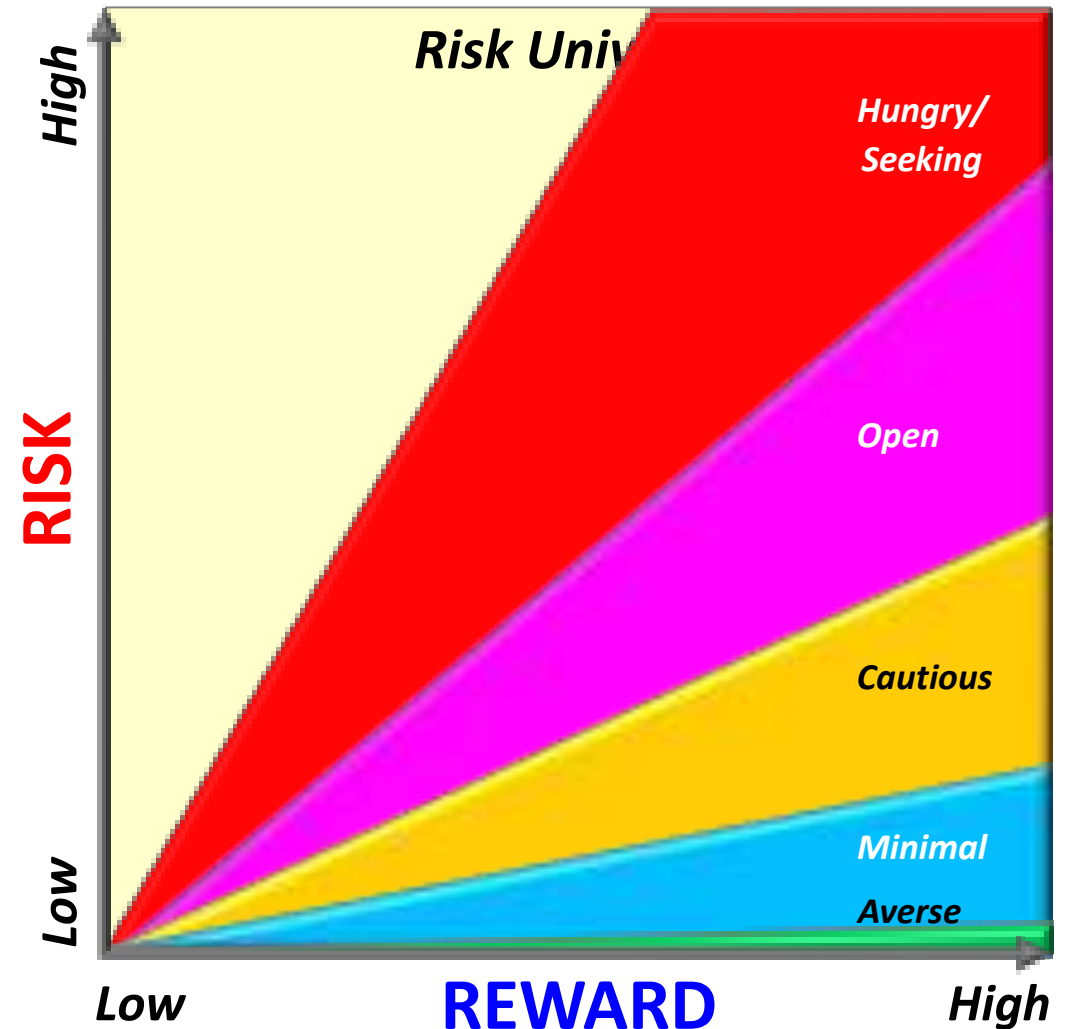
- ✓ **Risk Universe.** All of the possible risks that could affect a project or entity
- ✓ **Risk Profile.** An analysed indicator of the level of risk for a project/task
- ✓ **Risk Capacity.** The expected ability of the organisation (team) to manage the associated risks

The capacity is influenced by the organisation's (team's) **Appetite** and **Tolerance** for risk



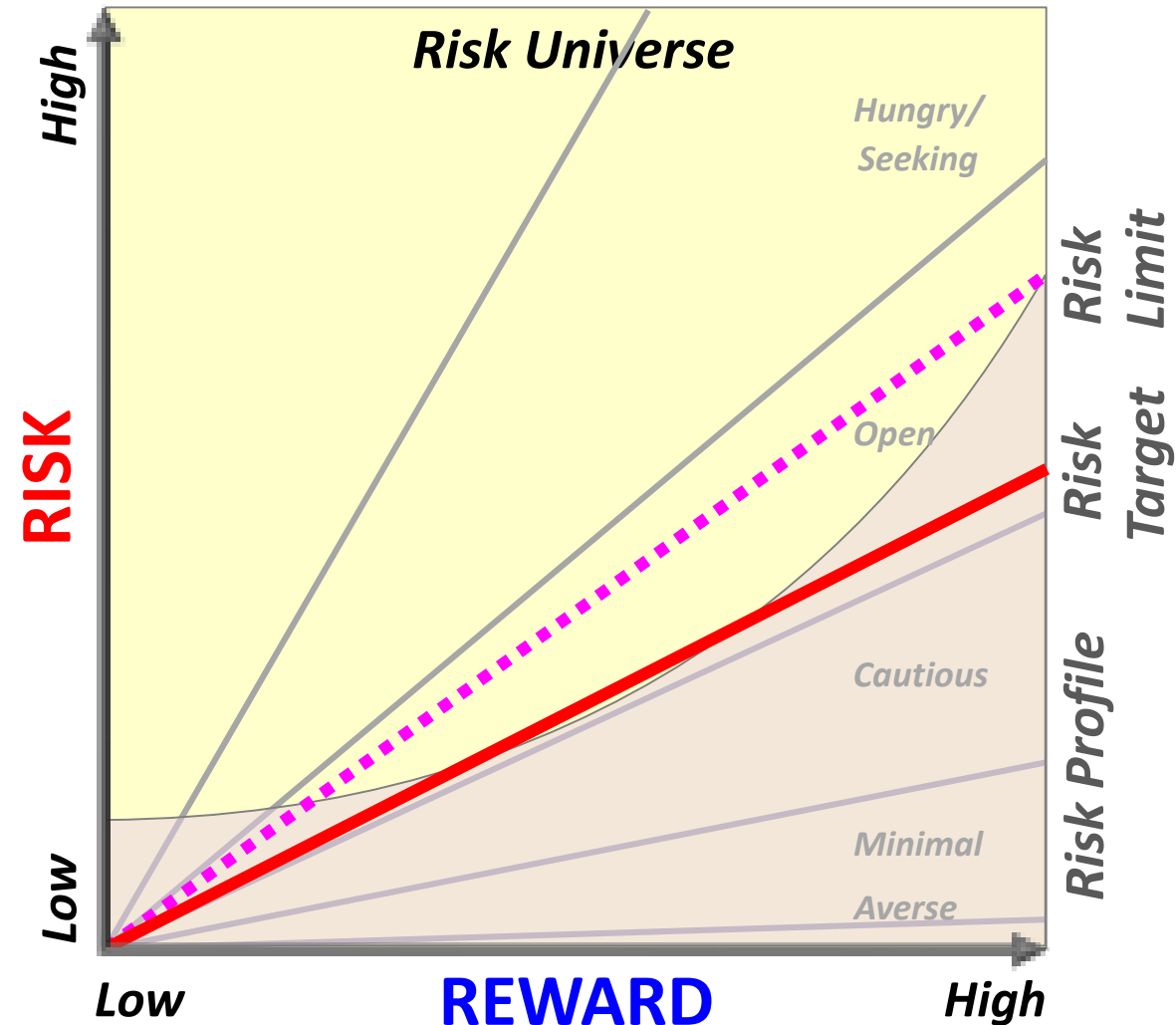
# KEY TERMS & PRINCIPLES

- ✓ **Risk Appetite.** The amount and types of risks that an organisation is willing to take to meet **strategic objectives** – Can be classified as...
- **Averse.** Avoids risk & uncertainty
  - **Minimal.** Will take some minimal risks if the reward is very high
  - **Cautious.** Will take some risks if there are clear rewards & controls
  - **Open.** Willing to take risks if there is a chance of strong reward
  - **Hungry/Seeking.** Actively chasing risk for high reward



# KEY TERMS & PRINCIPLES

- ✓ **Risk Tolerance.** The specific maximum risk that an organisation is willing to take regarding **each relevant risk**
- ✓ This is defined by:
  - **Risk Profile** (*risk level, known-unknowns & unknown unknowns*)
  - **Risk Appetite** (*how far are they willing to go to achieve the objective*)
  - **Risk Target** (*the optimal level of risk that organisation wants to take*)
  - **Risk Limit** (*identified thresholds beyond which risks should not deviate*)



# KEY TERMS & PRINCIPLES

✓ **Defining Risk Limits.** These can be numeric or ordinal

Some examples

Element	Very Low Limit	Low Limit	Moderate Limit	High Limit	Very High Limit
<b>% Difference in Outcome</b>	<= %2.5	2.5% - 5%	5% - 7.5%	7.5% - 10%	> 10%
<b>Cost</b> ( <i>what is acceptable</i> )	Very small increase (<5% of profit)	Small increase (< 10% of profit)	Significant increase (< 20% of profit)	Significant increase (< 40% of profit)	Large increase (< 60% of profit)
<b>Scope</b> ( <i>what is acceptable</i> )	Barely noticeable changes	Minor noticeable changes	Some significant scope changes	Numerous significant scope changes	Very significant changes in scope required
<b>Time</b> (Schedule) ( <i>what is acceptable</i> )	No change to key milestones	Minor changes but not for end date	Minor change to end date	Significant change to end date	Very significant change to end date
<b>Quality</b> ( <i>what is acceptable</i> )	Quality variance barely noticeable	Only affects very intensive use	Differences would be noticeable	Differences would be very noticeable	Does not meet key requirements

✓ These have to be agreed by the key stakeholders (**formally**)

# KEY TERMS & PRINCIPLES

- ✓ **Workaround.** Unplanned responses to unforeseen risk events that must be done without pre-planning (contingency/fallback)



Now that we've covered the key terms and principles –  
**Let's look at the Risk Management Process**

# THE RISK MANAGEMENT PROCESS

## INTRODUCTION

(What is Risk Management  
& Why is it important?)

## KEY TERMS & PRINCIPLES

## THE RISK MANAGEMENT PROCESS



# RISK MANAGEMENT PROCESS

- 1. Plan Risk Management.** Defining and documenting how risk management activities will be managed in the project
- 2. Identify Risks.** Detecting possible risks and documenting them as appropriate, so they can be investigated as necessary
- 3. Analyse Risks.** Determining the likelihood and effect of risks through **Qualitative** and **Quantitative** methods





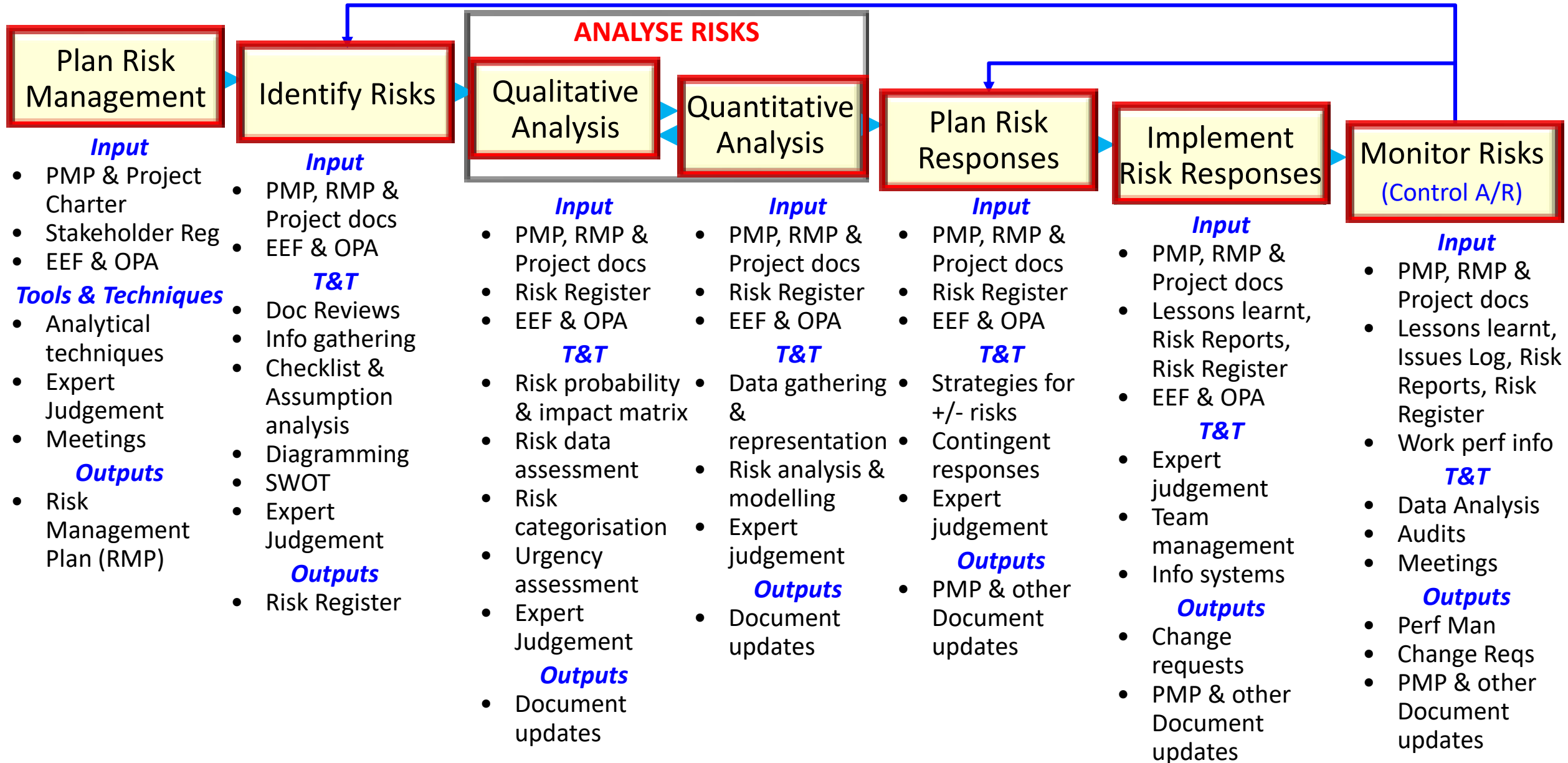
# RISK MANAGEMENT PROCESS

4. **Plan Risk Response.** Developing options & actions to reduce/manage the risks appropriately
5. **Implement Risk Responses.** Take appropriate steps to manage risks
6. **Monitor Risks.** Implement monitoring and control activities required to manage the risks

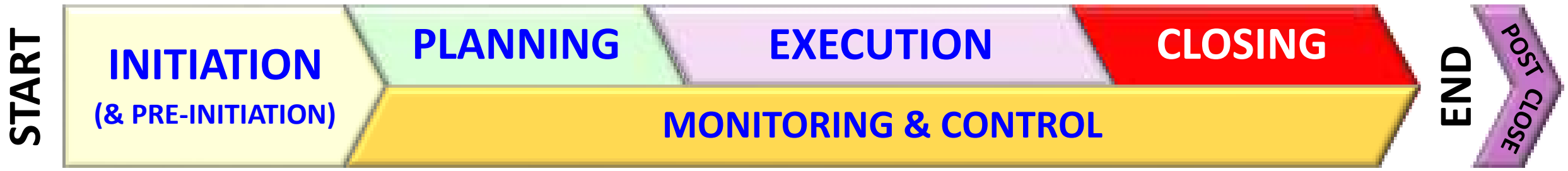
To maximise positives and minimise negatives throughout the project



# HOW DO THEY INTERACT?



# WHEN DO THESE STEPS GET DONE?



Plan Risk Management

Identify Risks

Analyse Risks (Qualitative/Quantitative)

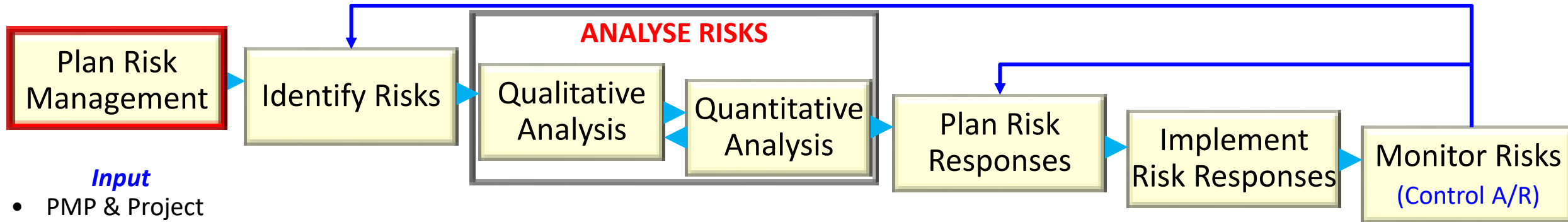
Plan Risk Responses

Implement Risk Responses

Monitor (and Control) Risks

Let's look at the steps in more detail

# PLAN RISK MANAGEMENT



## Input

- PMP & Project Charter
- Stakeholder Reg
- EEF & OPA

## Tools & Techniques

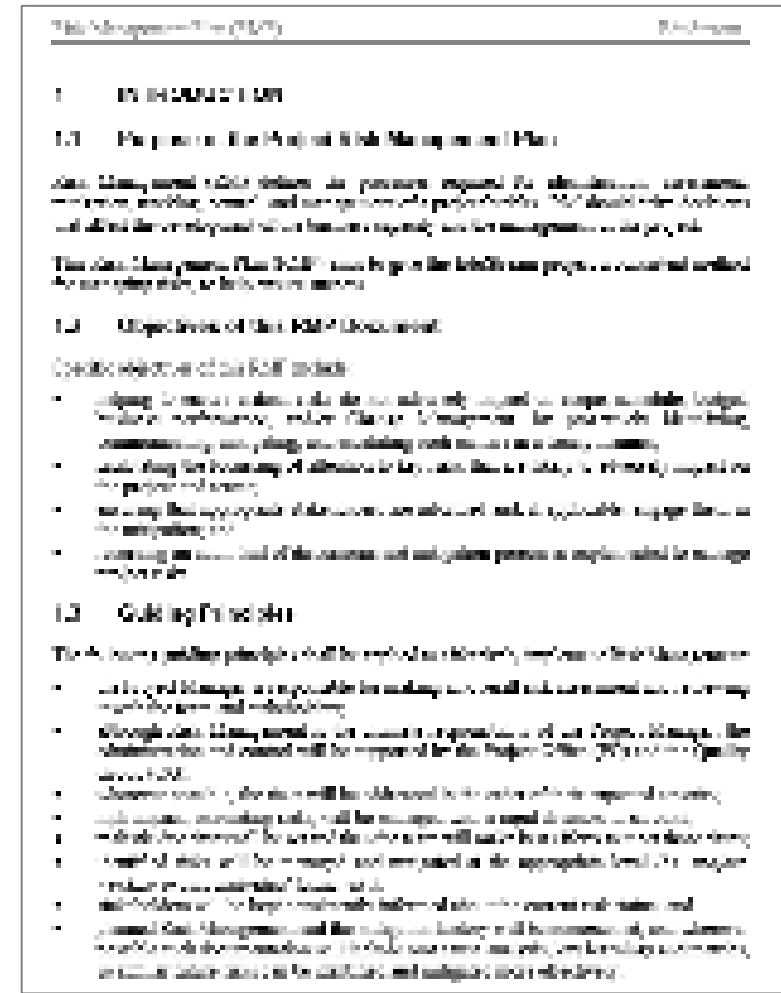
- Analytical techniques
- Expert Judgement
- Meetings

## Outputs

- Risk Management Plan (RMP)

# PLAN RISK MANAGEMENT

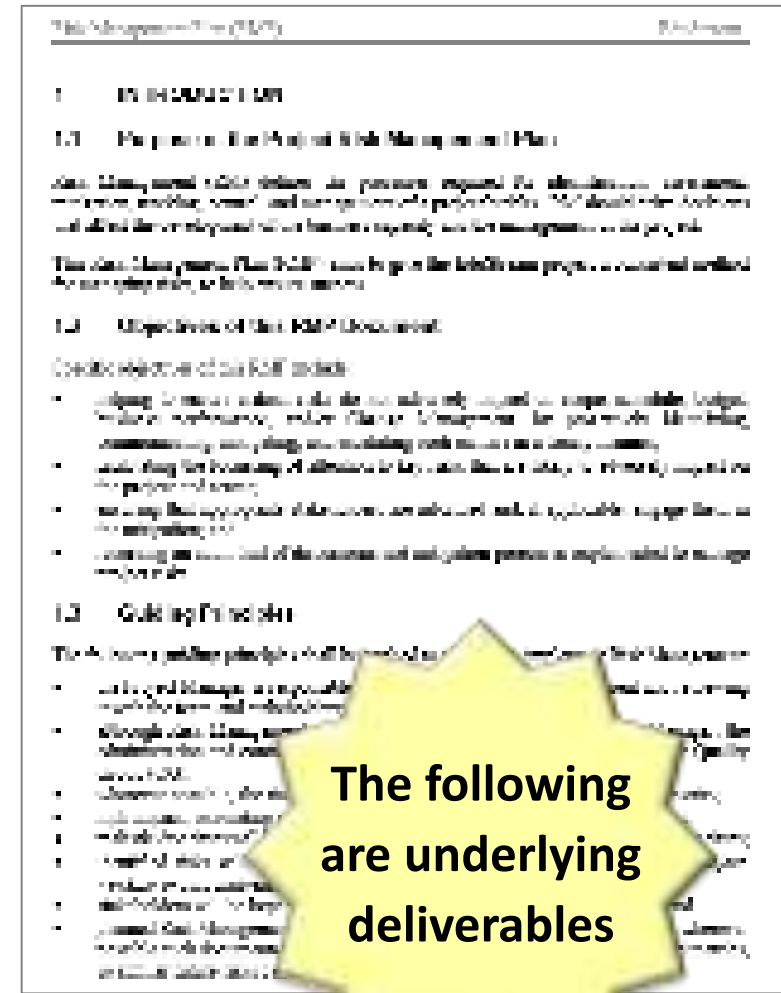
- ✓ The key deliverable is the **Risk Management Plan** (RMP)
- ✓ Sections in the RMP are dependent on:
  - The organisation
  - Type of project
  - Stakeholder requirements



# PLAN RISK MANAGEMENT

- ✓ Standard sections in an RMP include:
  - Objectives & Principles
  - Project Scope
  - Risk Management Organisation (**Roles & Responsibilities**)
  - Risk Categories/Types (**Broad framework**)
  - Risk Management Process (**Methodology**)
  - Tolerances and Limits (**General Principles**)

These are **determined by the following** & define frameworks used in the **Risk Register**

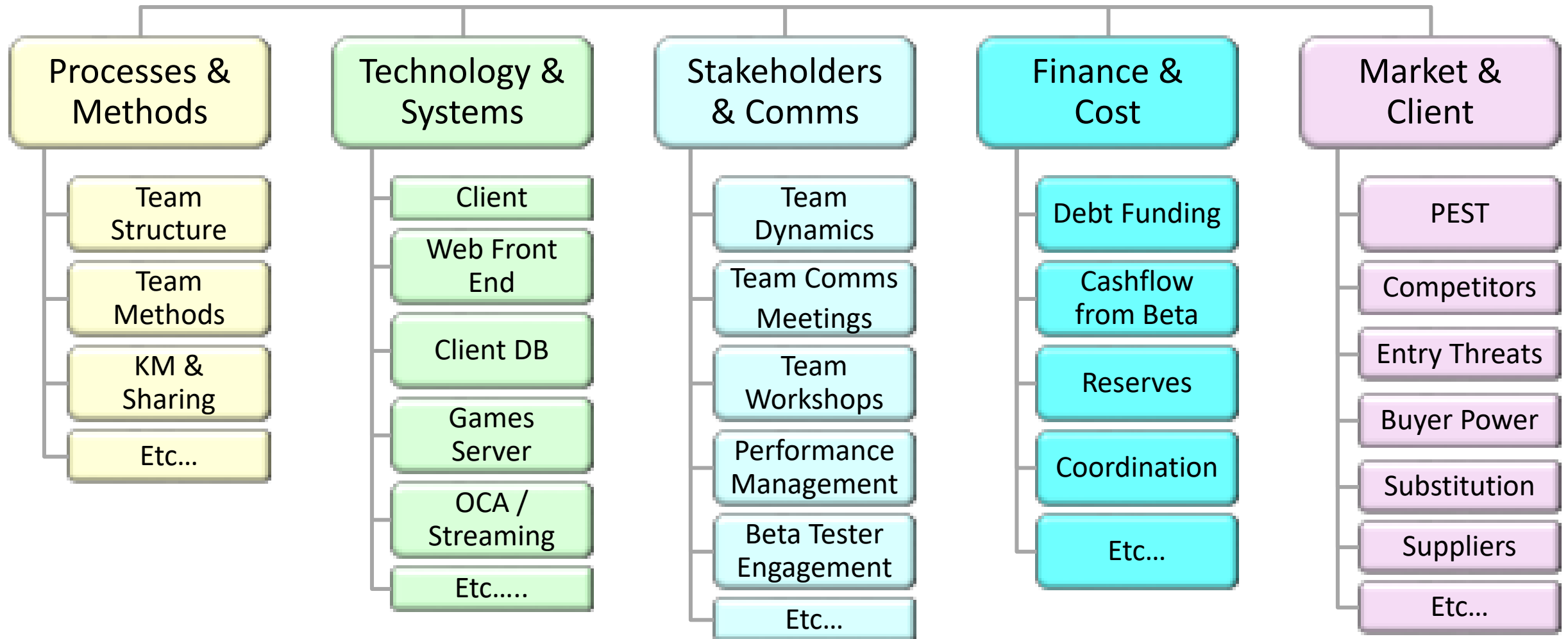


# RISK BREAKDOWN STRUCTURE

- ✓ This is a fundamental approach for identifying risks
- ✓ It should happen very early in the Initiation & then get updated at key points during the project
- ✓ Develop your RBS in a stakeholder workshop - use these steps:
  - Identify the categories & dimensions of risk associated with this project (*makes it easier to identify risks*)
  - For each category/dimension of risk
    - Identify what has gone wrong in the past
    - Identify what could go wrong in the future for this project

# RISK BREAKDOWN STRUCTURE

✓ They are often depicted graphically like this...





# RISK BREAKDOWN STRUCTURE

- ✓ But they are typically developed as Word or Excel Templates – Like this...

	A	B	C	D
1	Client Application	OCA/Nodes Streaming	Web Front End	Client Database
2	Multiple Platforms	Netfile control of OCA	utilizing PHP	rest of using code
3	Network connection variables	legal implications	User element for Passthrough	Table security
4	User interface	Standards	Calls on Client Database	Personal Security (users)
5	Security	SMTP issues	Calls on OCA (Passthrough)	Interface to OCA/Streaming
6	Deployment systems	Security	Security	Interfaces to various HTTP

This template is provided in the LMS – Topic 9

Lays the framework for the following processes

# CONTINGENCY PLANS

- ✓ Plans for **predefined actions** if an identified risk event **OCCURS** (*often a spreadsheet or database*)

## CONTINGENCY PLAN (PLAN A)

CONTINGENCY PLAN (PLAN A)	
Contingency Identification Number	1001
Description of Potential Problem	Netflix not providing rights to utilise OCA equipment
Probability and impact	Currently low (but negotiations are ongoing) & negative impact could be high
Main impact of potential problem	Require a replacement video streaming solution (core technology)
Solution for the problem	Deploy through Netflix (become a content provider or source specialist)
Consequences of implementing this contingency	(1) Limitation on growth and risk of being replaced (2) Lower risk deployment & possible larger market penetration
Preparation	Have negotiation options available & investigate the <i>Fallback option (2001)</i>
Activation	Implement preparations now – Activate if negotiations with Netflix fail

# FALLBACK PLANS

- ✓ These are action plans if the **Contingency Plan fails**/or cannot be achieved (*Normally linked to Contingency Plan*)

FALLBACK PLAN (PLAN B)	
Contingency Identification Number	2001
Description of Potential Problem	Removal of rights to utilise OCA equipment
Probability and impact	Currently low (but negotiations are ongoing)
Main impact of potential problem	Require a replacement video streaming solution (core technology)
Solution for the problem	Utilise another video streaming solution
Consequences of this approach	Scope and schedule impacts / Cost impacts / Contract impacts
Preparation	(1) Identify costed options for other systems (2) Request options for non-OCA solution in RFT
Activation	Activate if negotiations with Netflix fail (do preparations early)

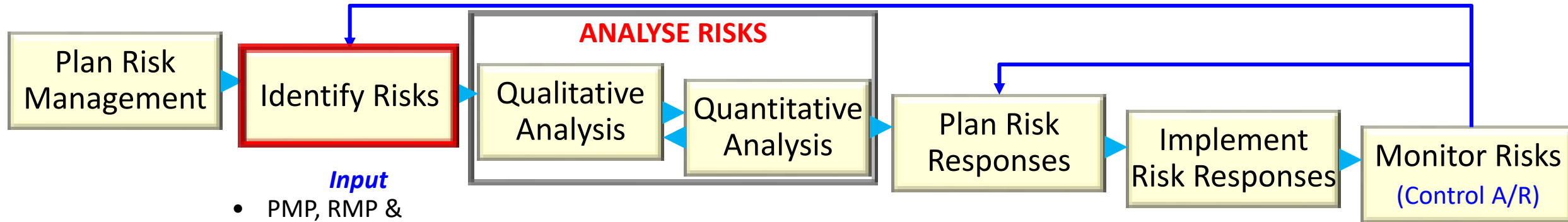
# RESERVES / ALLOWANCES

- ✓ Money set aside to manage/cover risks/changes
- ✓ Two categories are typical:
  - Contingency (normally included in the Baseline) – Known Unknowns
  - Management (normally not included in the Baseline) – Unknown Unknowns

Typically set as a percentage value in the initial cost modelling – It influences profit



# IDENTIFY RISKS



### *Input*

- PMP, RMP & Project docs
- EEF & OPA

### *T&T*

- Document reviews
- Information gathering
- Checklists & Assumption analysis
- Diagramming
- SWOT
- Expert Judgement

### *Outputs*

- Risk Register

# IDENTIFY RISKS

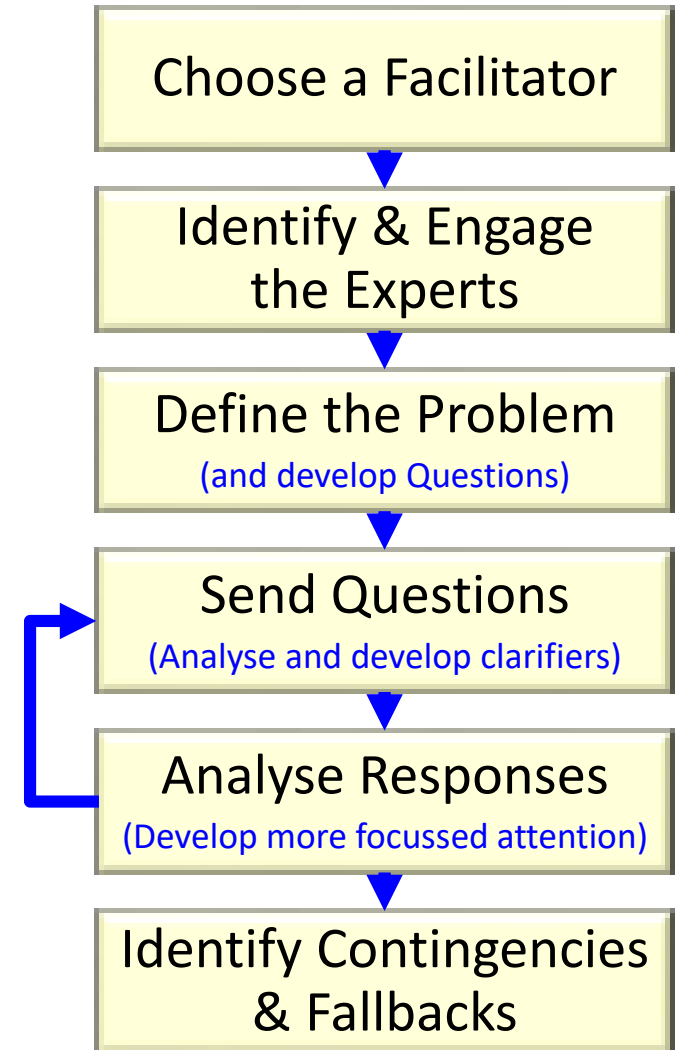
✓ This is an **ongoing process** - Risk identification tools and techniques include:

- Stakeholder feedback & ideas (**create a culture of proactive reporting**)
- Talking to stakeholders (**interviews, discussions & Management by Walking Around (MBWA)**)
- Expert judgement (**Brainstorming/Workshopping**)
- SWOT analysis (**generally best done as a workshop**)
- Delphi Technique (**uses experts who provide anonymous inputs to help avoid Groupthink**)



# THE DELPHI APPROACH

1. Choose a facilitator (must have an open mind)
2. Identify & engage the experts who will be used (they must understand the issues from different perspectives)
3. Define the problem and develop questions
4. Send Questions (send questions & get responses)
5. Analyse Responses (develop more focussed questions as needed and do Step 4 again as appropriate (typical 2 or 3 times))
6. Once the issues are clarified - identify actions



# IDENTIFY RISKS

- ✓ Once risks are identified using these types of approach:
  - Enter the content in the **Risk Register**
  - Analyse the Risks (**discussed soon**)
  - Take steps to manage the risks as necessary (**Plan Risk Responses, Implement Risk Responses & Monitor Risks**)



Let's begin by looking at the Risk Register



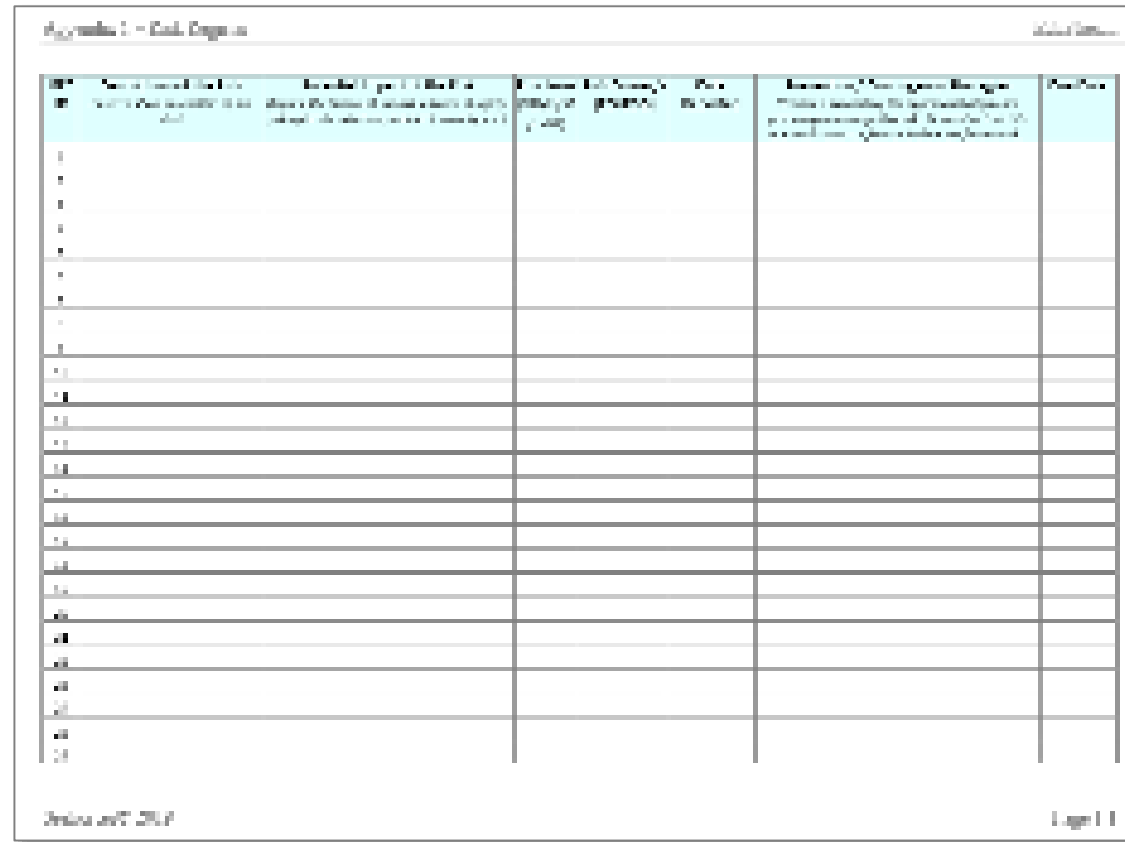
# RISK REGISTER

- ✓ Records **all identified risks** related to a project
  - Providing details of the risk (**as identified through the various processes**)
  - Providing ownership information
  - Identifying steps taken to manage the risk
  - Identifying whether the risk has been managed (**avoided, transferred, controlled, mitigated, or accepted**)



# RISK REGISTER

- ✓ Different organisations use different formats (typically managed electronically nowadays – Word, Excel, MS Project – Add-ins/Online)
- ✓ Here is one example...



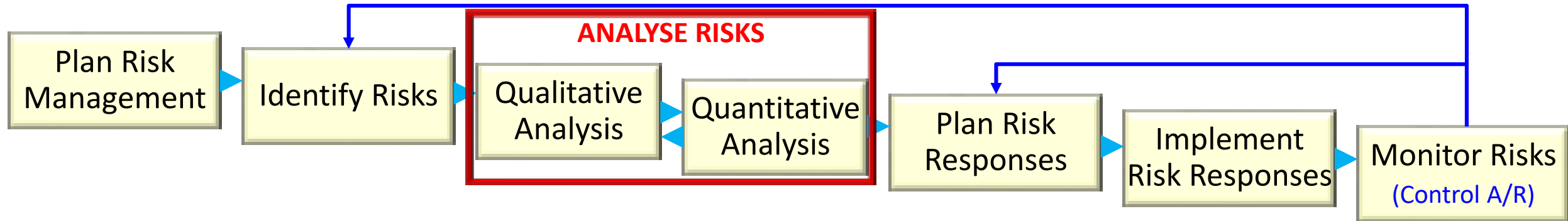
The image shows a screenshot of a spreadsheet titled 'Appendix 1 - Risk Register'. The spreadsheet has a header row with the following columns: 'Risk ID', 'Risk Description', 'Risk Category', 'Risk Rating', 'Risk Owner', 'Risk Status', 'Risk Mitigation Strategy', and 'Risk Score'. Below the header, there are 20 rows of data, each starting with a risk ID (e.g., R1, R2, R3, R4, R5, R6, R7, R8, R9, R10, R11, R12, R13, R14, R15, R16, R17, R18, R19, R20). The cells in the rows are mostly empty, indicating a template. The spreadsheet is displayed in a window with a title bar and a status bar at the bottom.

Risk ID	Risk Description	Risk Category	Risk Rating	Risk Owner	Risk Status	Risk Mitigation Strategy	Risk Score
R1							
R2							
R3							
R4							
R5							
R6							
R7							
R8							
R9							
R10							
R11							
R12							
R13							
R14							
R15							
R16							
R17							
R18							
R19							
R20							

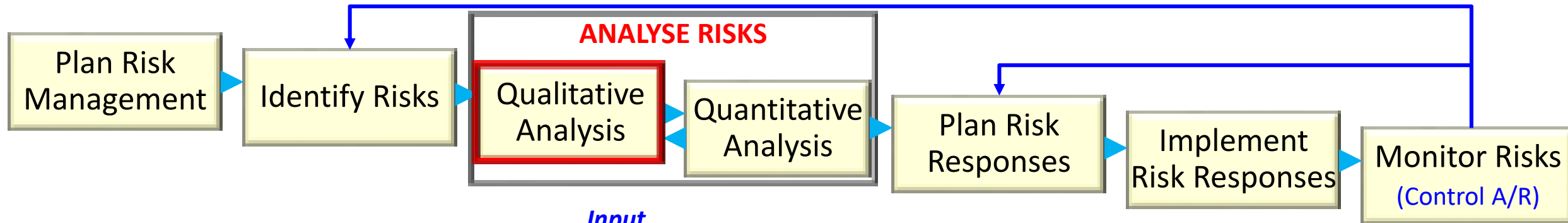
This provides a reasonable template for content

Use the format mandated by your ICT organisation

# ANALYSE RISKS



# QUALITATIVE ANALYSIS



## *Input*

- PMP, RMP & Project documents
- Risk Register
- EEF & OPA

## *T&T*

- Risk probability & impact matrix
- Risk data assessment
- Risk categorisation
- Urgency assessment
- Expert Judgement

## *Outputs*

- Document updates

# QUALITATIVE RISK ANALYSIS

- ✓ Assess the *likelihood* and *impact* of identified risks (determine their magnitude and priority for control)
- ✓ Common techniques include:
  - Probability/Impact matrices
  - Top Ten Risk Item Tracking
  - Expert judgement

Can be used jointly



Let's look at each of these techniques in turn

# PROBABILITY/IMPACT MATRIX

- ✓ Used to assess the probability and impact of various risks
- ✓ Often used to identify risk factors (a numeric **Severity Weighting**)
- ✓ Numerous different frameworks and systems are used (you will need to use the one supported by your organisation)



Let's look at one example (the one used in Assignment 2)






# PROBABILITY/IMPACT MATRIX

## IMPACT OF OCCURRENCE

Low (1)    Medium (3)    High (5)

PROBABILITY OF OCCURRENCE	High (5)	Moderate Risk (5x1=5)	High Risk (5x3=15)	Very High Risk (5x5=25)
	Medium (3)	Low Risk (3x1=3)	Moderate Risk (3x3=9)	High Risk (3x5=15)
	Low (1)	Very Low Risk (1x1=1)	Low Risk (1x3=3)	Moderate Risk (1x5=5)

## WHAT TO DO

	Very High – Escalate & resolve quickly
	High – Proactive steps ASAP
	Moderate – Manage with caution
	Low – Proceed but monitor
	Very Low – Monitor but little risk

## PROBABILITY OF OCCURRENCE

- High (5)**
  - Major uncertainty remains
  - No or little prior experience or data/information
  - Significant infrastructure, systems & resources not in place
- Medium (3)**
  - Some uncertainties remain
  - Some experience and data/information exists
  - Infrastructure, systems, resources in place but not complete
- Low (1)**
  - Few uncertainties remain
  - Significant experience and data/information exist
  - Infrastructure, systems & resources in place

## IMPACT OF OCCURRENCE

- High (5)**
  - Performance, technical, quality, costs or safety impacts can result in **major** injury, redesign/program delay
- Medium (3)**
  - Performance, technical, quality, costs or safety impacts can result in injury, or **significant** redesign/program delay
- Low (1)**
  - Performance, technical, quality, costs and safety impacts are likely to be **minimal** & requirements should still be met

# PROBABILITY/IMPACT MATRIX

Typically more detailed guidance is provided [\(such as the table in the RMP\)](#)

Score	Definition/Actions to be taken
<b>Very High</b> <b>(25)</b>	Anything classified as <b>Very High</b> indicates that this risk is extremely or very likely to occur. Additionally, the occurrence could have a profound impact on the project's safety, technical, cost, and/or schedule, which may cause the project to be terminated or can cause significant cost/schedule changes ( <i>e.g. increases of more than 5 percent</i> ) for the project. The management of this level of risk should be escalated, and that aspect of the project must be implemented with <i>extreme care</i> until the risks can be mitigated/controlled effectively.
<b>High Risk</b> <b>(15)</b>	<b>High Risks</b> may cause significant safety, technical, cost, and/or schedule increases ( <i>e.g. increases of 2 to 5 percent</i> ) for the project. These risks are to be managed proactively, and a priority must be applied to mitigate/control the risks as soon as practicable. In the meantime, the elements of the project associated with this risk must be managed with due care.
<b>Moderate Risk</b> <b>(5 or 9)</b>	This refers to risks that are <b>Moderate</b> , because they may have a relatively small but significant impact on the project's safety, technical, cost, and/or schedule ( <i>e.g. less than 2 percent</i> ). Appropriate mitigation/control strategies should be implemented when practicable. Obviously, risks with a score of nine (9), should be addressed with higher priority than those with a score of (5). While awaiting mitigation/controls to be implemented, the team should still manage this aspect of the project with care.
<b>Low Risk</b> <b>(3)</b>	A <b>Low Risk</b> refers to an event that is relatively unlikely to occur, or the impact would be low if it did occur. In other words, this refers to situations in which the combination of likelihood and impact means that this risk would not be expected to have a significant impact on the project's safety, technical, cost and/or schedule. Typically, consolidated risk management is not applied to these types of risks. However, the team associated with this aspect should keep it in mind while implementing the project and monitor the issue with an appropriately level of caution.
<b>Very Low Risk</b> <b>(1)</b>	A <b>Very Low Risk</b> refers to matters where it would be unlikely for the risk to occur and even if it did, the impact is expected to be minimal. In these circumstances, consolidated risk management would not be applied. However, as with all aspects of Risk Management, those involved with the project should continue to monitor evolving levels of risk and take proactive action when considered appropriate.



# TOP TEN RISK ITEM TRACKING

- ✓ Uses **Severity Scores** to identify the Top 10 (or sometimes more) risks
- ✓ List these in **order of priority**
- ✓ Implement **periodic reviews** for these high probability/impact risks (**as appropriate to the circumstances**)
- ✓ **Monitor and update** the listing as appropriate (**e.g. monthly, or when new risks are identified**)



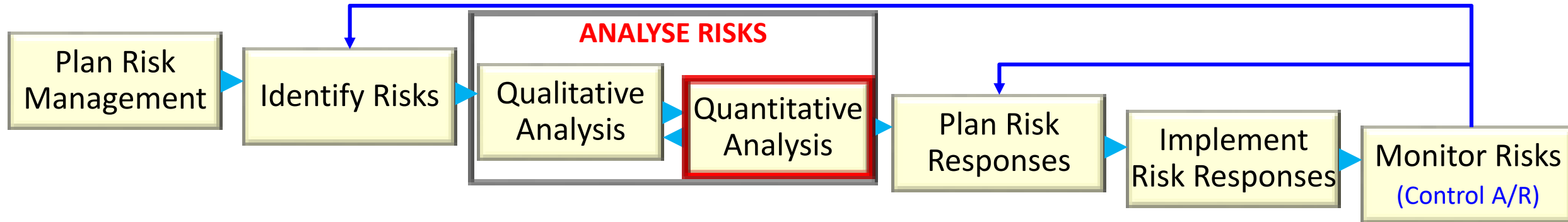
This **does not mean that you only focus on these** – you need to assess/monitor/control all identifiable risks

# EXPERT JUDGEMENT

- ✓ This approach is used by many organisations
- ✓ This typically involves a **workshop or meeting during which experts:**
  - analyse and prioritise risks **(based on their experience)**
  - create watch lists of risks **(so they can be monitored)**

In addition to these qualitative approaches – Quantitative Analysis is also often implemented

# QUANTITATIVE ANALYSIS



## *Input*

- PMP, RMP & Project docs
- Risk Register
- EEF & OPA

## *T&T*

- Data gathering and representation
- Risk analysis & modelling
- Expert judgement

## *Outputs*

- Document updates

# QUANTITATIVE RISK ANALYSIS

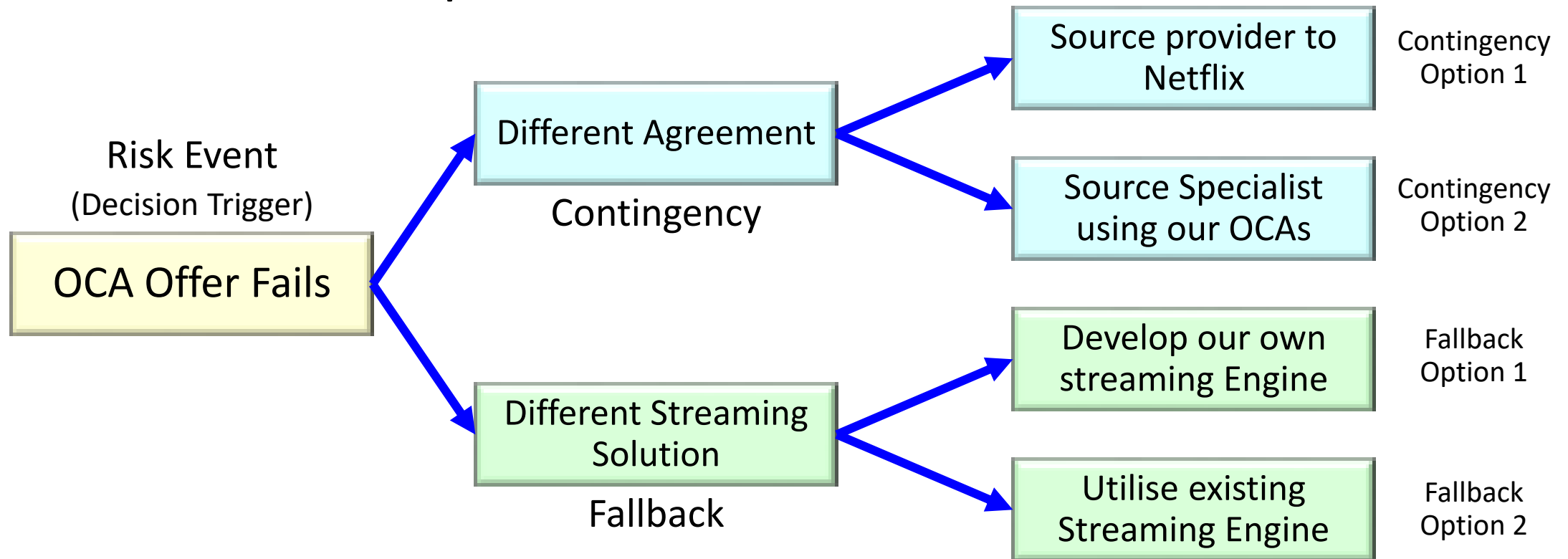
- ✓ This entails using different techniques to help **quantify risks**
- ✓ Some of these techniques include:
  - Decision tree analysis & Expected Monetary Value (**EMV**)
  - Simulation (**e.g. Monte-Carlo**)
  - Sensitivity Analysis



Let's look at these

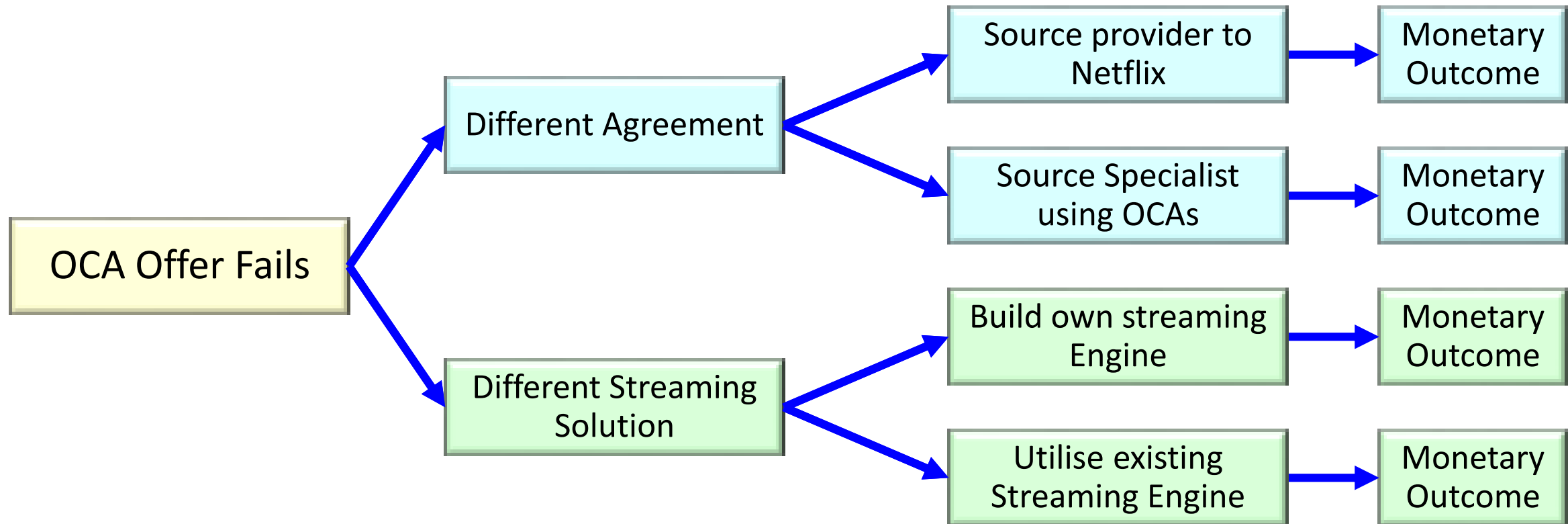
# DECISION TREE

- ✓ This is an approach used to determine the most appropriate course of action (e.g. for risk/reward analysis)
- ✓ Here is an example of a Decision Tree



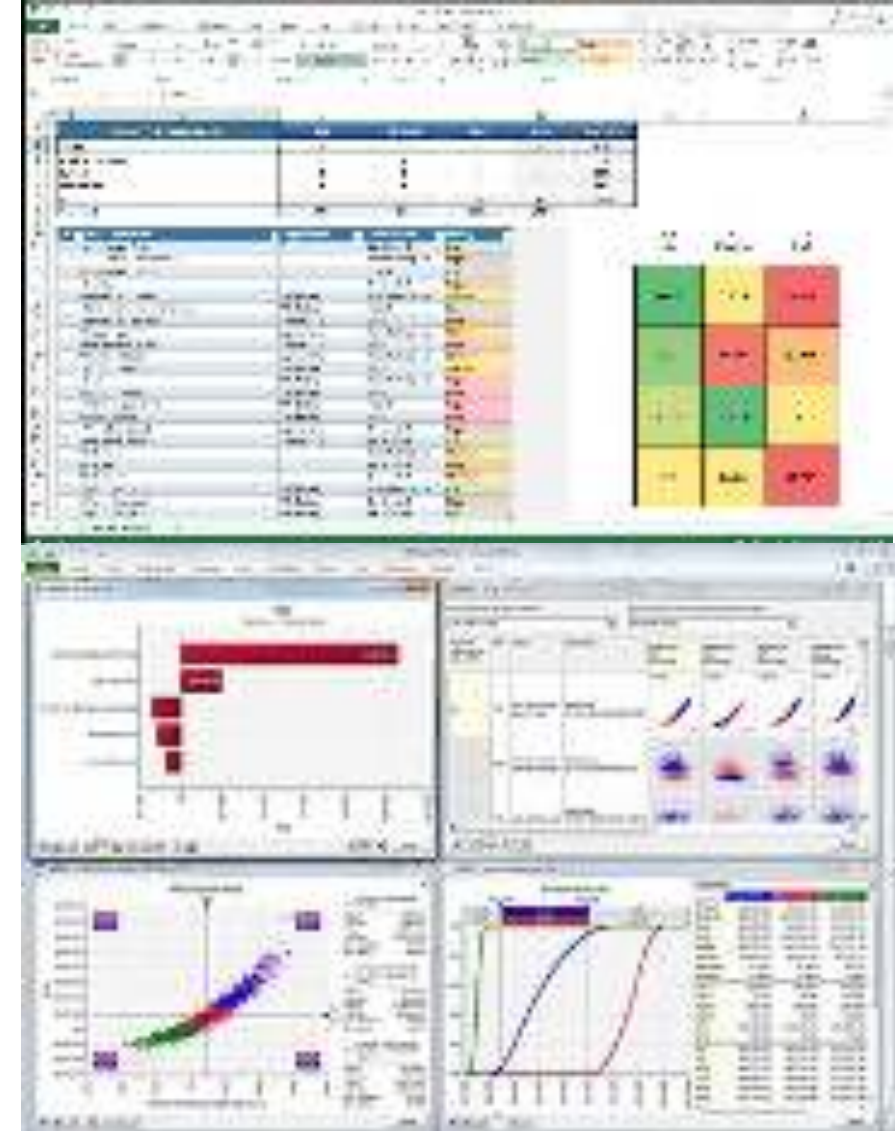
# EXPECTED MONETARY VALUE

- ✓ This is a variation that allows costed options to be assessed
- ✓ This will be explained during the Topic 9 Workshop



# RISK SIMULATION

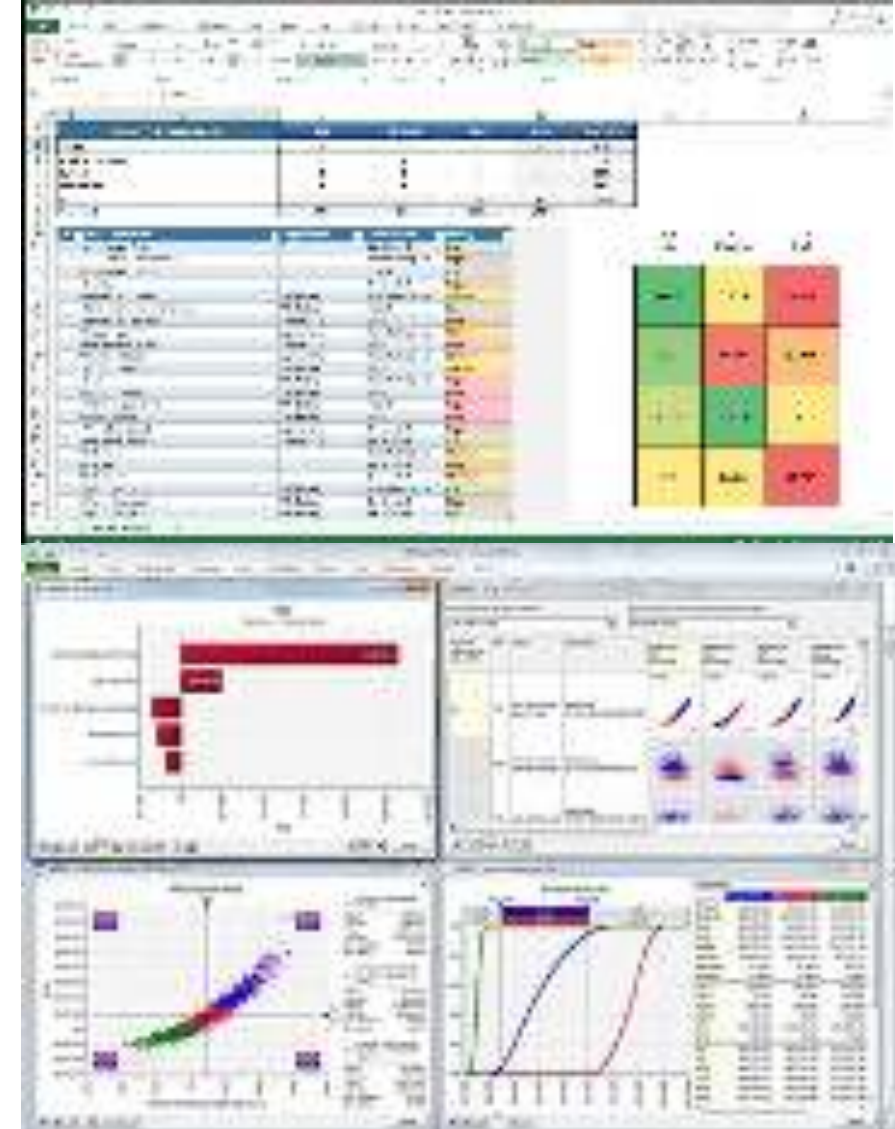
- ✓ Uses **mathematical modelling** of **risk parameters** and **variables** to determine things like:
  - The scope of the risk
  - Risk probability (**likelihood**)
  - Risk impacts (**cost, time, etc.**)
  - Which variables are likely to be most important (**what do we need to watch?**)
  - The risk limits that should be set
  - Contingency (**known unknowns**)



# RISK SIMULATION

- ✓ A common approach applies **Monte Carlo Analysis**, which uses a range of variables to:
  - Determine the most likely effect of variable changes across a range of circumstances (**multiple run analysis**)
  - Define/apply three outcome estimates (**most pessimistic, most likely, most optimistic**)
  - Apply the probability of the most likely being between in the optimistic/pessimistic range (**to create a numeric weighting model**)
  - Develop Quantitative risk parameters (**Probability, Impact, Risk level, etc.**)

**Often this is linked to Sensitivity Analysis**

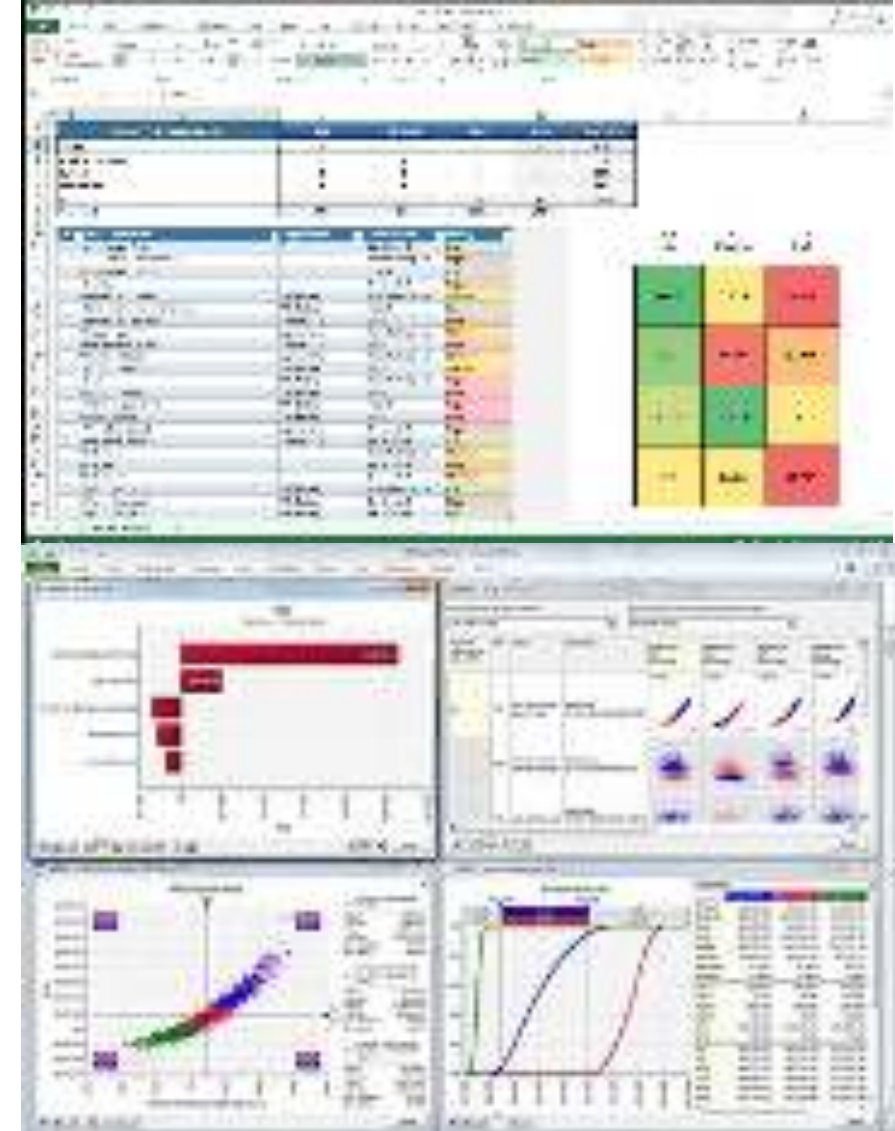




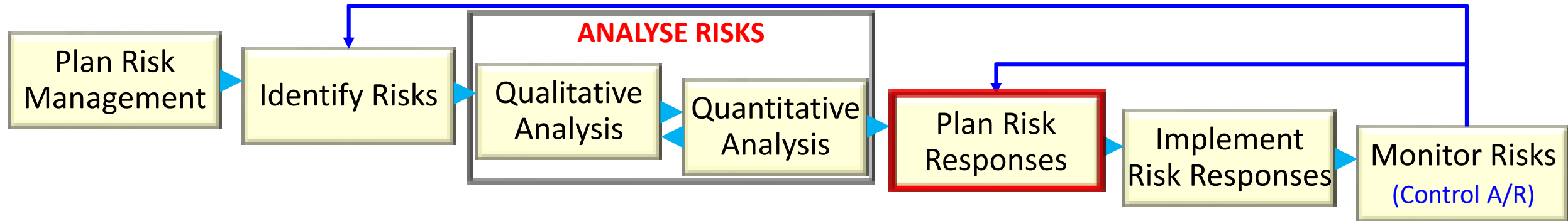
# SENSITIVITY ANALYSIS

- ✓ This is a **form of simulation** which allows **specific variables to be manipulated directly** to determine what the likely outcomes would be
- ✓ It is particularly useful for **'what if'** analysis
- ✓ Such models are specifically built for likely high impact risks **(both + & -)**

**Provide key insights for response planning**



# PLAN RISK RESPONSES



### *Input*

- PMP, RMP & Project docs
- Risk Register
- EEF & OPA

### *T&T*

- Strategies for +/- risks
- Contingent responses
- Expert judgement

### *Outputs*

- PMP & other Document updates

# PLAN RISK RESPONSES

Identified risks that have been analysed as being of import are delegated to:

- ✓ A Risk Owner (RO) (who is responsible for taking appropriate actions)
- ✓ An appropriate number of Risk Co-Owners (RCO) (who assist the RO)



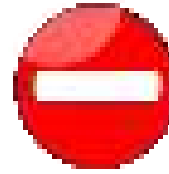
They are responsible for:

- ✓ Identifying options for managing the risk
- ✓ Presenting the options to the PM (or their delegate) for approval
- ✓ Preparing contingency/fallback plans for appropriate options
- ✓ Implementing any activities that are required

# PLAN RISK RESPONSES

The options may include the following strategies *(for negative risks)*:

- ✓ **Avoid** – Eliminate threats to protect the project
- ✓ **Transfer** – Shift the risk to another party
- ✓ **Control** – Manage variables that lead to the risk
- ✓ **Mitigate** – take steps to reduce the impact
- ✓ **Accept** – Understand the risk & only take action if it happens



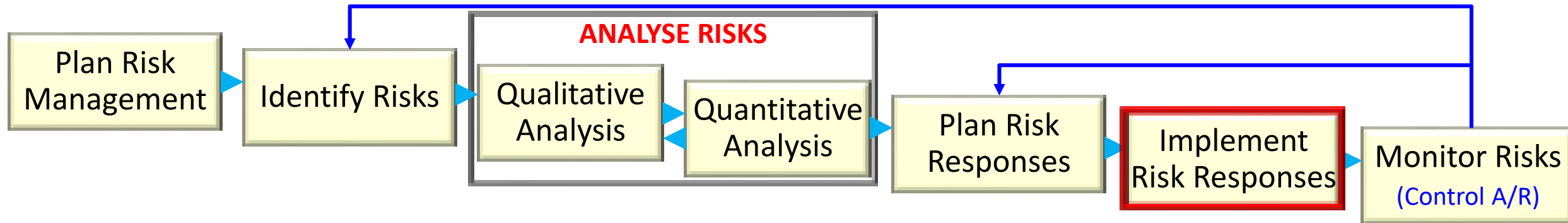
Or for positive risks:

- ✓ Accepting the risk & helping to make it happen
- ✓ Exploiting the opportunity
- ✓ Sharing the risk – so the impact is increased
- ✓ Enhancing the risk to increase its positive impact



This helps to ensure that management is effective

# IMPLEMENT RISK RESPONSES



## *Input*

- PMP, RMP & Project docs
- Lessons learnt, Risk Reports, Risk Register
- EEF & OPA

## *T&T*

- Expert judgement
- Team management
- Information systems

## *Outputs*

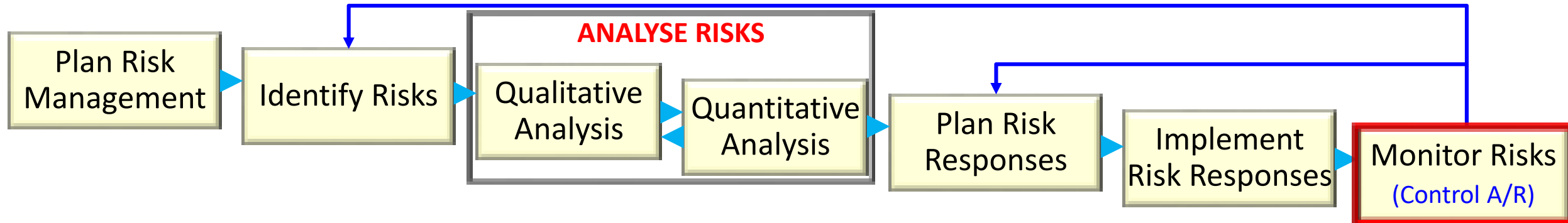
- Change requests
- PMP & other Document updates

# IMPLEMENT RISK RESPONSES

- ✓ Implement appropriate strategies
  - **Negative:** Avoid, Transfer, Control, Mitigate, Accept
  - **Positive:** Accept, Exploit, Share, Enhance
- ✓ **Build the implementation around:**
  - **The schedule** – When do controls need to be in place
  - The **level of risk and impact** – More severe risks/impacts should be addressed sooner
  - The **ability and willingness of your organisation** to manage the risks (**being proactive**)
  - Factoring in **Contingency** (Plan A) and **Fallback** (Plan B) from the outset



# MONITOR RISKS



### *Input*

- PMP, RMP & Project documents
- Lessons learnt, Issues Log, Risk Reports, Risk Register
- Work performance information

### *T&T*

- Data Analysis
- Audits
- Meetings

### *Outputs*

- Performance Management
- Change Requests
- PMP & other Document updates

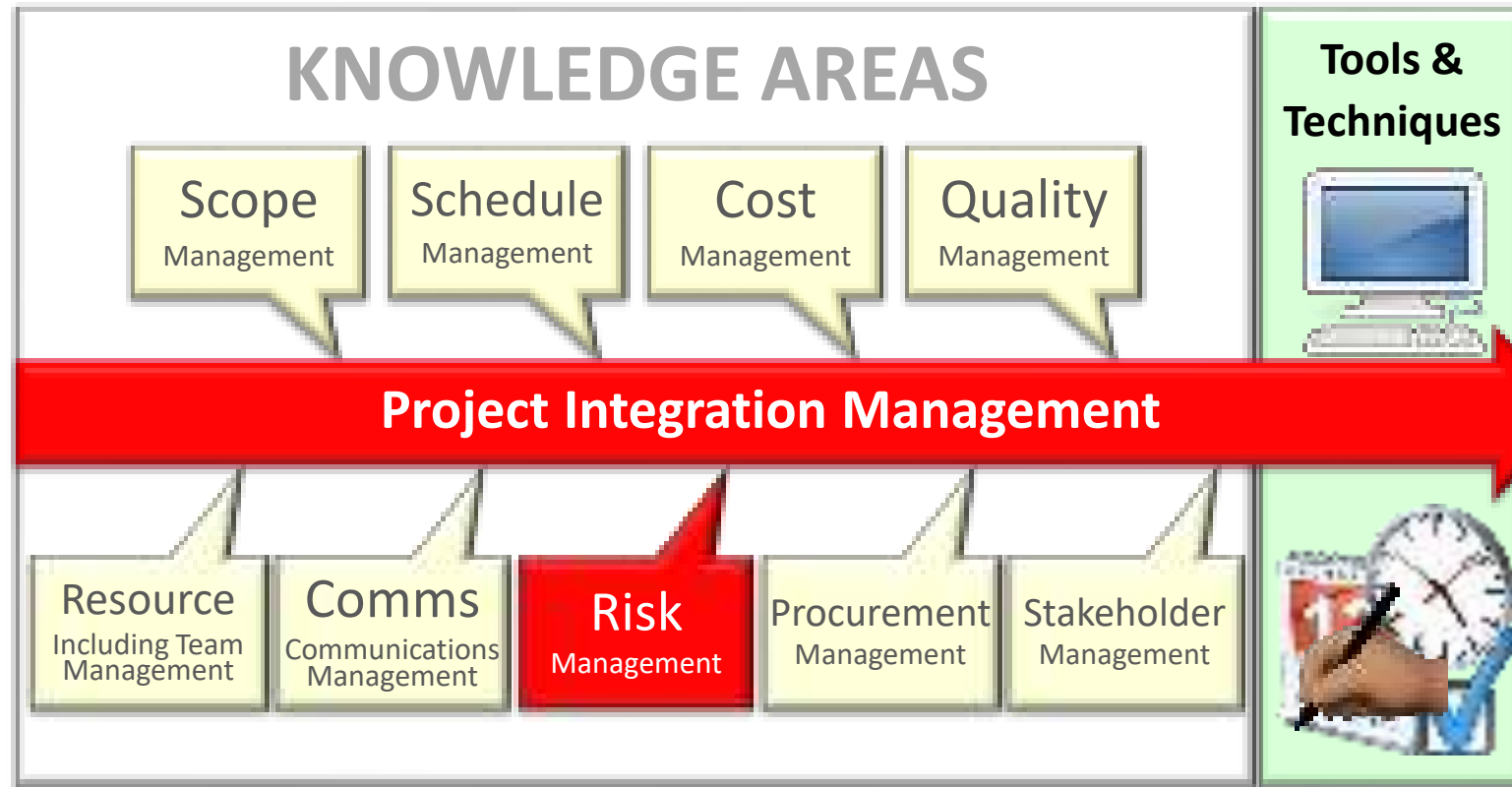
# RISK MONITORING & CONTROL

- ✓ This is an **iterative and ongoing** process to:
  - **proactively monitor** risks & status
  - **identify changes** in risk profiles/situation
  - implement/modify appropriate management strategies
- ✓ **Main outputs** of risk monitoring and control are:
  - Change Requests (**to trigger Change Management**)
  - **recommended** corrective and preventive **actions**
  - **updates** to the Risk Register, Contingency/Fallback plans, Project Management Plan, WBS, other project documents and organisational processes/assets

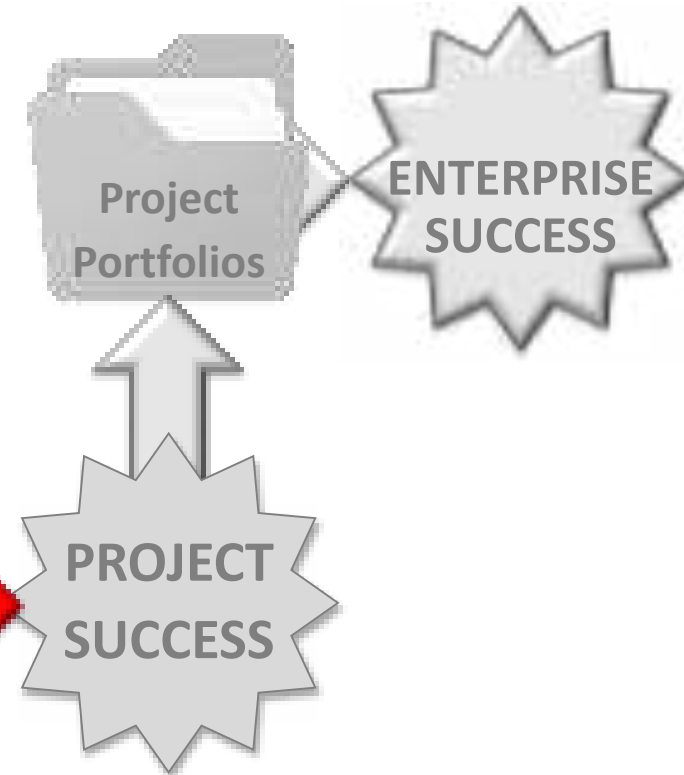




# SOFTWARE



Stakeholders' needs & expectations



# RISK MANAGEMENT SOFTWARE

- ✓ Commonly used Risk Management software includes:
  - MS Word/Word Processors – For documents/Plans/Risk Register
  - MS Excel/Spreadsheets – For documents/Risk Breakdown Structure/Contingency-Fallback plans/Risk Register/**quantitative modelling**
  - MS Access/Databases – For Risk Breakdown Structure/Contingency-Fallback plans/Risk Register, etc.
  - Statistical Analysis Modelling Programs (Excel/SPSS/Other specialist programs)
  - Microsoft Project (Custom Fields, Add-ins & Project Online)
  - Numerous other packages



# THESE PROVIDE RISK DASHBOARDS



AND MANY OTHER TOOLS

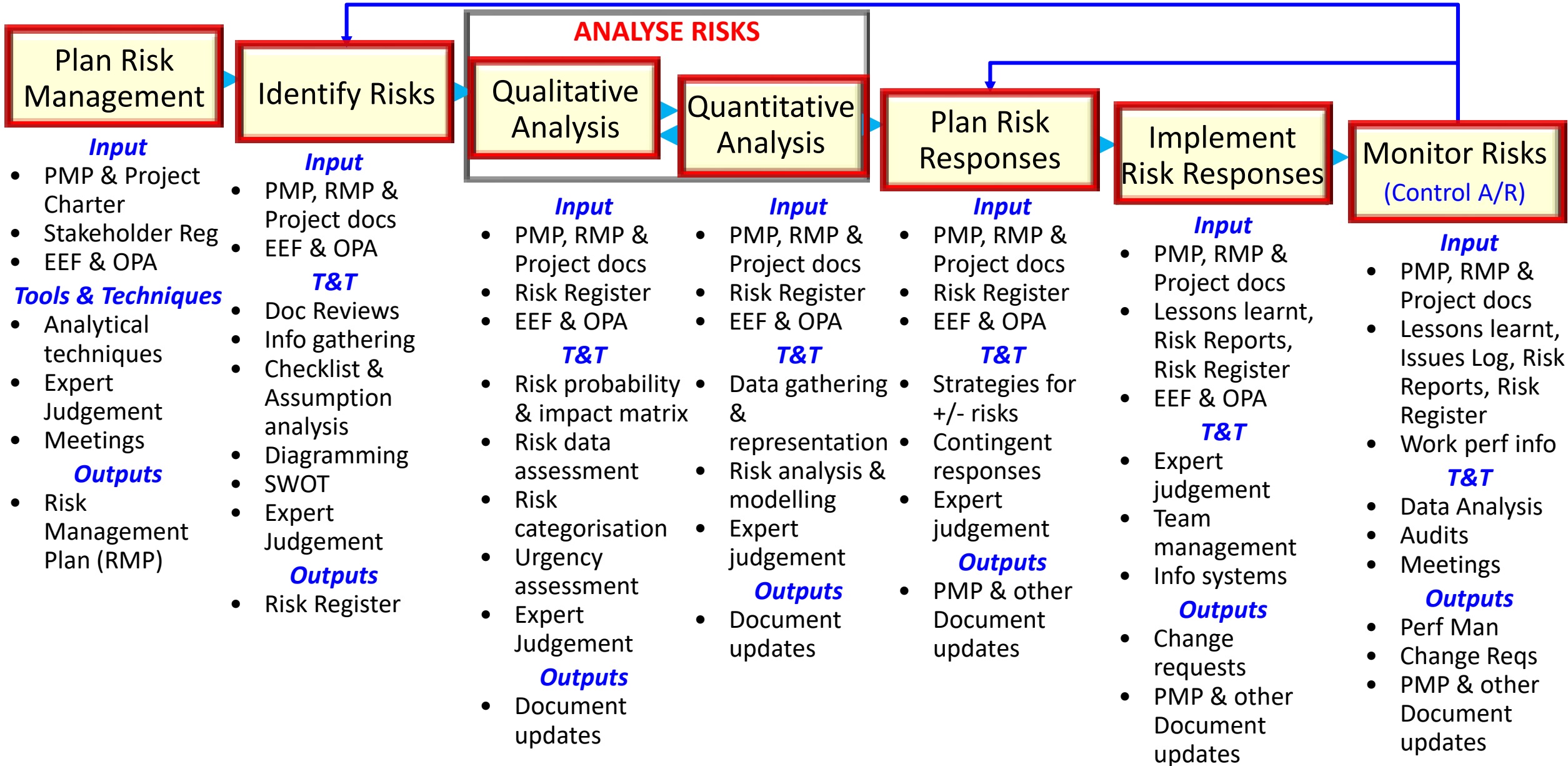
(GET USED TO APPLYING WHAT IS PROVIDED BY YOUR ORGANISATION)

# TOPIC SUMMARY

# TOPIC SUMMARY

- ✓ Project Risk Management is critical (it affects everything)
- ✓ It is used to:
  - Identify risks
  - Analyse risks (qualitative & quantitative methods)
  - Plan methods for managing the risks (contingency & fallback)
  - Implement methods to manage risks (monitoring & controlling)
- ✓ When done properly it is almost invisible to people outside the project, but when not done it can be catastrophic

# IT IS MANAGED THROUGH...



**ANY**

**QUESTIONS**

A large, 3D green question mark graphic is positioned on the left side of the slide, partially overlapping the word 'QUESTIONS'. The question mark has a thick, rounded stem and a circular top with a small dot. It is rendered with a slight shadow on the surface below it.