SAQA ID 59201

NATIONAL CERTIFICATE: GENERIC MANAGEMENT

CLUSTER 8

LEARNER GUIDE

Accredited course information:

Unit Standard ID	NQF Level	Credits
252032	5	8

Develop, implement and evaluate an operational plan

Accredited course information:

Unit Standard ID	NQF Level	Credits
252025	5	8

Monitor, assess and manage risk

Accredited course information:

Unit Standard ID	NQF Level	Credits
252022	5	8

Develop, implement and evaluate a project plan

TRAINING FORCE
Linking Training to Industry

Investing in your talent!

TABLE OF CONTENTS

LEARNING UNIT ONE

1

ASSESSMENT CRITERIA

Develop, implement and evaluate an operational plan 252032

SPECIFIC OUTCOME 1 - 4

- Develop operational strategies for a unit
- Develop an operation plan for a unit
- Implement an operational plan.
- Monitor, measure and evaluate the achievement of goals and objectives.

OPERATIONAL PLANNING

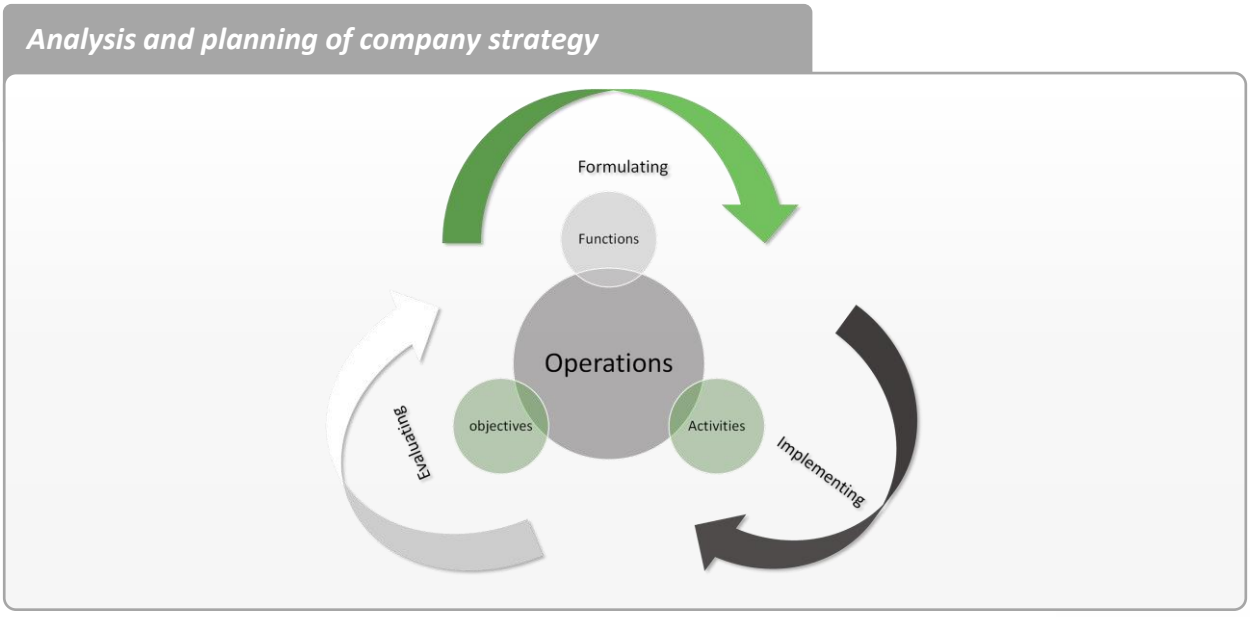
Operational planning is a process of linking strategic goals and objectives to tactical operational goals and objectives. It gives milestones, conditions for success, and explains how and what portions of plans will be implemented during a given period.

Operation plans are prepared by individuals involved in the implementation and must contain:

- Clear objectives
- Activities to be delivered
- Quality standards
- Desired outcomes
- Staffing and resource requirements
- Implementation timetable (Action Plan)
- A process for monitoring progress

STRATEGIC PLANNING

Strategic planning is the art and science of formulating, implementing, and evaluating cross function decisions that enable an organisation to achieve its objective.



Further it is the process of defining and clarifying an organisations values and mission, together with envisioning the future of the organisation. Then develops goals and action steps to move toward the future.

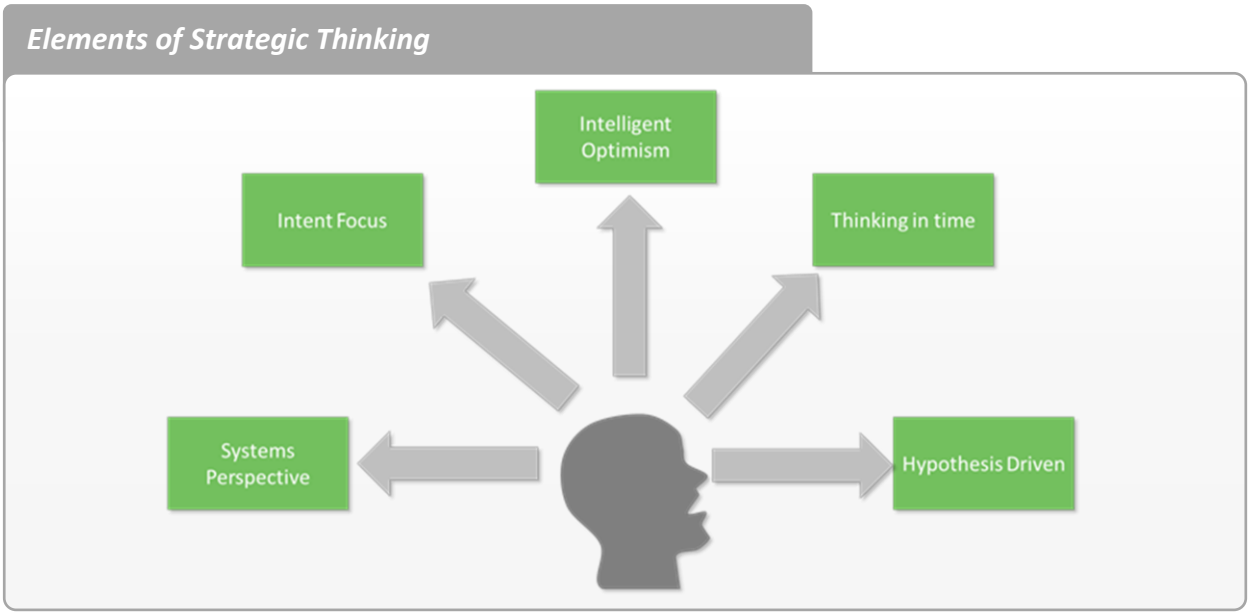
Corporate strategy plans are concerned with the overall purpose and scope of the organisation to meet needs and expectations of the major stakeholders. Examining the plan will require full understanding of purpose with the processes involved in achieving the purpose.

Business unit strategies are concerned with identifying and creating new opportunities in the markets.

Operational strategy is another level of strategy which is concerned with the elements of the organisations, the resources, processes, people, skills to effectively deliver the corporate and business level strategic direction.

Given the change management process it requires for all levels of an organisation to apply strategic thinking as opposed to it being limited to management as the old way dictates.

Liedtka (1998) developed a model to define strategic thinking as a specific way of thinking.



The elements of the model are System Perspectives – which dictates that a strategic thinker has a mental model of the complete system, The next element intent focused which is a strategic

intent that provides the focus that allows individuals in an organisation to govern their energy and focus attention and resist distraction.

The 3rd element of strategic thinking is intelligent opportunism, the idea of openness to new experience, that allows individuals to take advantage of alternatives.

The 4th element referred to as thinking in time, means that strategy is not solely driven by the future, but the gap between current and future goals and the 5th element recognises that strategic thinking is hypothesis driven, which poses the question of What if scenarios and that hypothesis testing follow up with critical questioning, what if, then …

In the first phase of developing this plan it is essential to understand the company's vision and mission. The vision explains the preferred future and the mission the purpose and function. From the vision and mission operational inputs, activities and individual outputs are planned as individual goals and objectives, the plan then implemented and reviewed, reflecting how well the plan met with each individual objective together to reach the overall objective.

MISSION STATEMENTS

The **mission statement** describes why the business exists **today**. It reflects the goals of a business and how it sees its responsibilities to the customer and community. The mission statement describes the purpose of the business's existence.

A good mission statement is made up of three parts:

- The **key market** is defined.
- The company's **contribution** is stated.
- A distinction is made between your company and others.

OBJECTIVES

What are Objectives?

We know that an objective is a target or something that must be achieved, which helps a business measure its successes. Let's look at objectives of strategic planning.

Strategic objectives can be classified into the four perspectives of what is called **Balanced**

Scorecard.

The four perspectives of the Balanced Scorecard are:

- Financial

The Financial Perspective helps a company to determine whether the strategy, implementation and execution are contributing to the bottom line.

- Customer

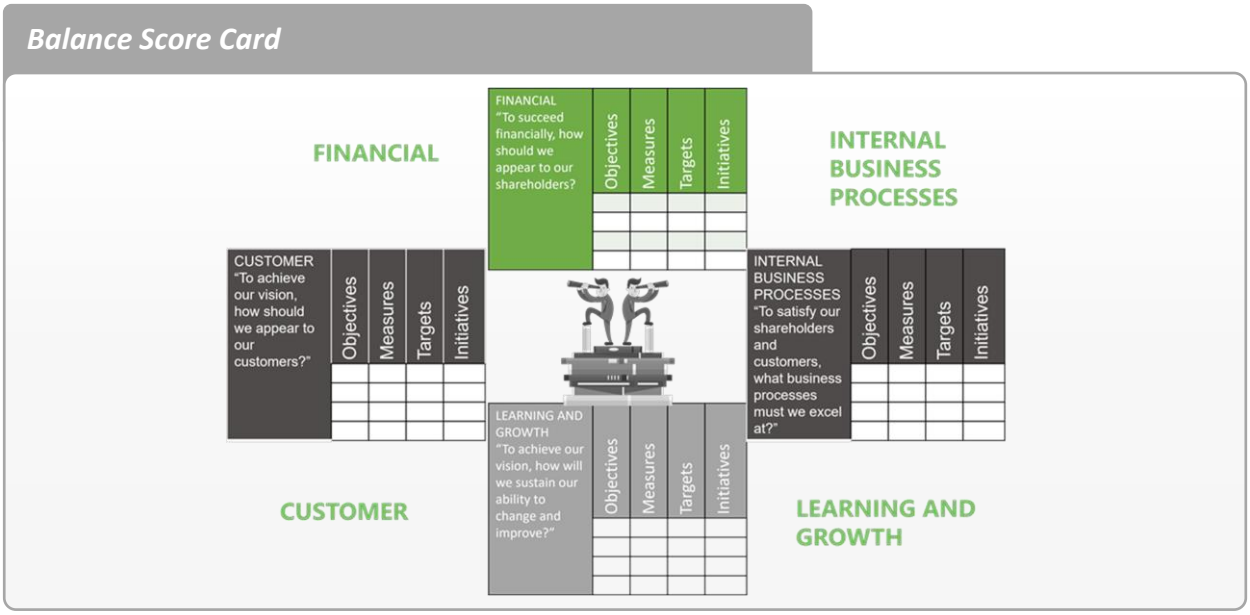
The Customer Perspective involves evaluating our client's needs such as time, quality, performance and service.

- Internal Business Process

The internal business process perspective involves applying measurements to internal operations to improve efficiency and effectiveness.

- Learning and Growth

The learning and growth perspective addresses the organisations' ability to innovate, improve, develop, and motivate staff.



The measures represent a **balance** between:

- **External measures** for shareholders and customers and **internal measures** of critical business processes and of learning and growth.

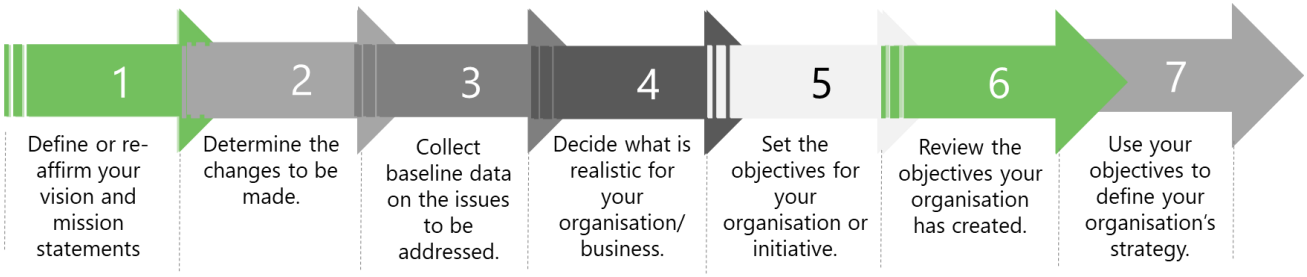
- Measures which report the **historical performance** of the organisation and measures intended to drive **future performance**.

- **Objective, quantifiable measures** (i.e., we can put a number to them) and **subjective measures** (i.e., we make a value judgement about them).

DEVELOP GOALS, OBJECTIVES, AND PERFORMANCE STANDARDS

The best objectives have several characteristics in common. They are all **S.M.A.R.T. + C.:** By setting and evaluating goals to being smart, provides and shows direction, initiates quality, and overall business benefit in achieving the mission and visional objective.

Turning strategy into specific objectives for the business unit:



DEVELOP THE OPERATIONAL PLAN

The framework for your action plan is recommended as follows:

• Departmental objectives (aligned to organisational strategy)
• Potential risks and contingencies to address these
• Tasks
• Responsibilities
• Timeframes
• Performance measures
• Resource needs

Complete the plan and include provision for contingencies, which requires identification of potential risks and then defining what will be done in the case of risk occurring.

Operational plans are documented to show tasks, responsibilities, timeframes, performance measures and resource needs.

Tasks

List all the tasks with activities that need to be carried out to achieve each departmental objective. This is an important step in the process as it is these tasks that will be cascaded to an individual level. Break down each objective into logical bite size steps or actions.

Responsibilities

Allocate responsibilities to resources for each of the tasks. This is likely to be line management's responsibility and they will then cascade the tasks to their respective staff members.

Timeframes

A start and finish date supply you with definitive measures for performance. They also assist in defining predecessor and successor relationship between the tasks. Some actions may be dependent on others before they can commence. Line and staff should understand the knock-on effect of not achieving specified timelines.

Performance Measures

Performance measures should cover cost, quantity, and quality. All too often, organisation focus on one element, and neglect the others.

Resource Needs

Resource needs may include people, equipment, machinery, vehicles, IT systems, or money, to name a few. Ensure that in your plan you define specific resource needs that are required to achieve the objectives. In instances where there is limited budget available, develop contingencies to address shortfalls. In addition, create a benefit case for the "spend". Define the future cost or impact of securing versus not securing the resources.

The following tools can be used to determine the strengths and weaknesses:

- The Situation Analysis - SWOT
- ***The PEST Analysis***

The PEST analysis considers the business environment of the political, economic, social and technological factors of the business before beginning the strategic planning process.

Monitors evaluate and reflect through feedback on the implementation of the plan.

Outline of an Operational Plan

Organisational Objective	Departmental Objective	Risks and Contingencies	Tasks	Responsible?	Timeframes	Performance Measures	Resource Needs	Supporting Organisational Tools

MONITORING IMPLEMENTION OF THE PLAN

Implementation is the process of ensuring that execution of the plan takes place. Monitoring the implementation is based on performance indicators or standards as set out in the plan.

Performance indicators and standards can only be achieved if progress is being monitored against the timelines, finances, and the other indicators. Time and cost are commodities that are readily recorded and measured while other standards may need other monitoring systems to be established.

Project Management as we will learnt about in the next Learning Unit, is a great tool to help develop a plan, that includes monitoring and evaluation tools to ensure that all areas of the performance standards are being met.

A monitoring and evaluation plan is a document that can be developed together with the operational plan to track and assess results of the project or operation throughout the life of the program. These documents will include some elements already created during the planning process and others that may need to be developed.

A monitoring plan will include the following elements:

1. Introduction
    - Goals and Objectives
    - Logical Framework
2. Indicators or Standards
    - Tabulated data sources, collection timing, and responsible team member
3. Roles and responsibilities
    - Description of each team members role in the monitoring and evaluation data collection analysis and or reporting.
4. Reporting

- Analysis plan
- Reporting templates

5. Dissemination plan
    - Description of how and when monitoring and evaluation data will be disseminated internally and externally.

LEARNING UNIT TWO

2

ASSESSMENT CRITERIA

Develop, implement and evaluate a project plan 252022

SPECIFIC OUTCOME 1 - 4

- Select a work-based project for a unit
- Scope a work-based project for a unit
- Develop a project plan
- Develop tools to measure key performance parameters

Monitor, assess and manage risk 252025

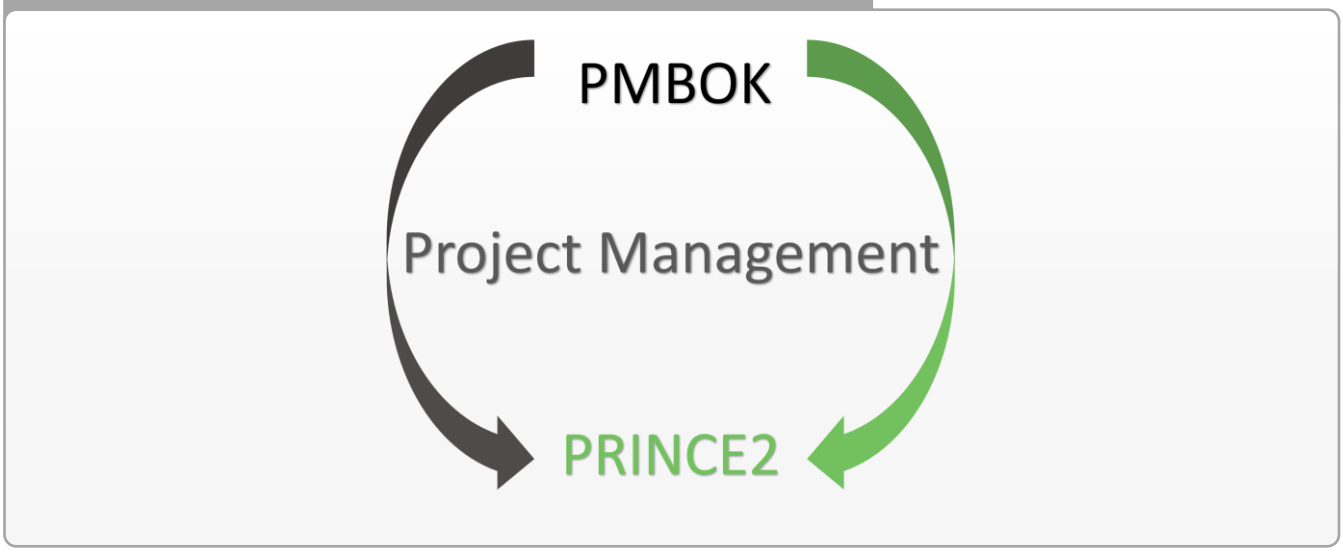
SPECIFIC OUTCOME 1 - 4

- Demonstrate an understanding of potential risks to a unit
- Identify potential risks and assess the impact thereof in a unit
- Develop contingency plans for managing risk
- Test and revise contingency plans

PROJECT MANAGEMENT FUNDAMENTALS

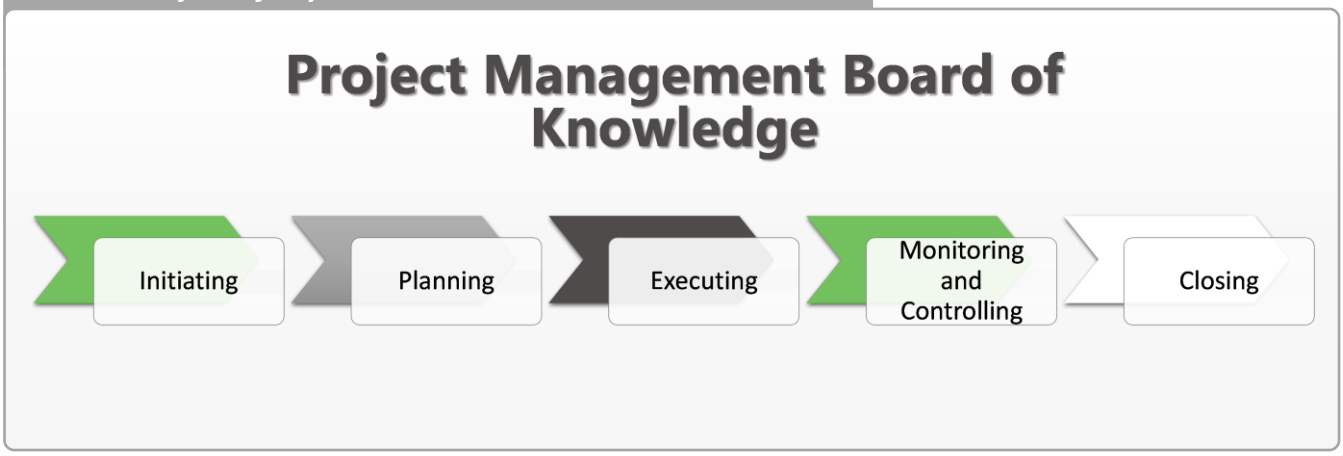
Developing project plan is a process involving the life cycle of project management, PMBOK Project Management Board of Knowledge and Prince 2 are 2 worldwide methods used that define the techniques and processes in project planning.

Project Management Methods



The example below shows the PMBOK standard using the 3p's principle in project planning – project management integration, project processes and Project life cycle.

PMBOK Project Life Cycle



It further defines the following table of activities that are executed during each phase, around 10 knowledge areas.

‘

PMBOK Project Life Cycle

Knowledge Areas

Management Process	Initiation	Planning	Executing	Monitoring & Controlling	Closing
Project Integration Management	Develop Project Charter	Develop Project Management Plan	Direct & Manage Work	Monitor & Control Project Word Perform Change Control	Close Project or phase
Project Scope Management		Plan Scope Management Collect requirements Define Scope Create WBS		Validate Scope Control Scope	
Project Time Management		Plan Schedule Define Activities Sequence Activities Estimate Resources Estimate Duration Develop Schedule		Control Schedule	
Project Cost Management		Plan Cost Management Estimate Costs Determine Budget		Control Costs	
Project Quality Management		Plan Quality Assurance	Control Quality		
Project HR Management		Plan Human Resources	Acquire Project Team Develop Project Team Manage Project Team		
Project Communication Management		Plan Communication Management	Manage Communications	Control Communications	
Project Risk Management		Plan Risk Management Identify Risks Perform Quantitative/Qualitative Risk Plan Risk Responses		Control Risks	
Project Procurement Management		Plan Procurement	Conduct Procurement	Control Procurements	Close Procurement
Project Stakeholder Management	Identify Stakeholders	Plan Stakeholder Management	Manage Stakeholder Engagement	Manage Stakeholder Engagement	

As you can see each phase becomes a process once the project is initiated, each process is then planned in accordance with the knowledge area assigned to the processes and the activity that is required to achieve the output.

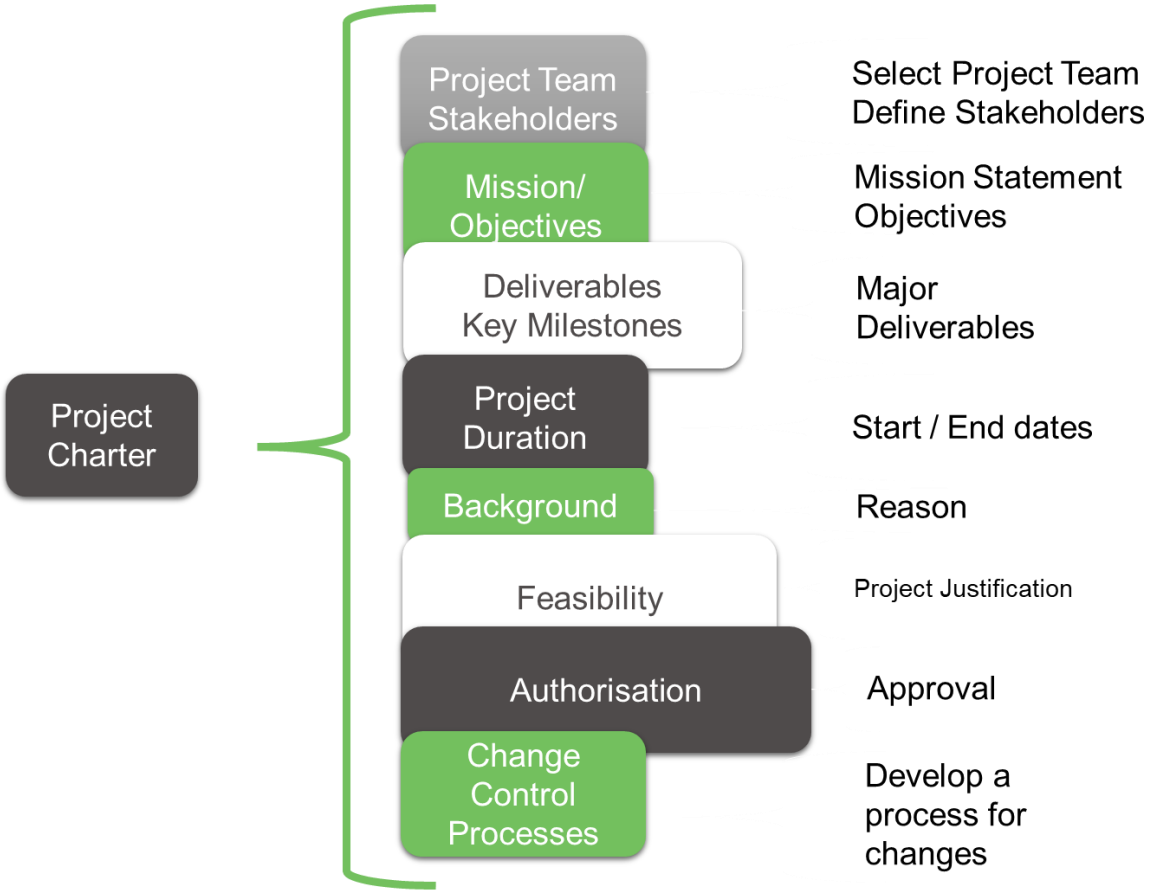
For instance, we can see that project management integration involves the initiation of the Project charter which sets the highest level of standards to be achieved for the project as well as the identification of stake holders.

PROJECT CHARTER

The project charter is a formal document that recognises the projects existence, it is created by the Project manager and issued by the sponsor in the initiation phase of a project. The document defines all the high-level requirements for the project and links it to ongoing work. It authorises the project and the project manager and justifies the project in terms of its value to the company.

Depending on the project management standards being used to manage projects in some cases the scope management plan is used as the charter.

This includes but is not limited to the following elements:



The project team is selected and organised in terms of authority, this is done using and organisational structure formation and is known as an OBS – Organisational Breakdown Structure.

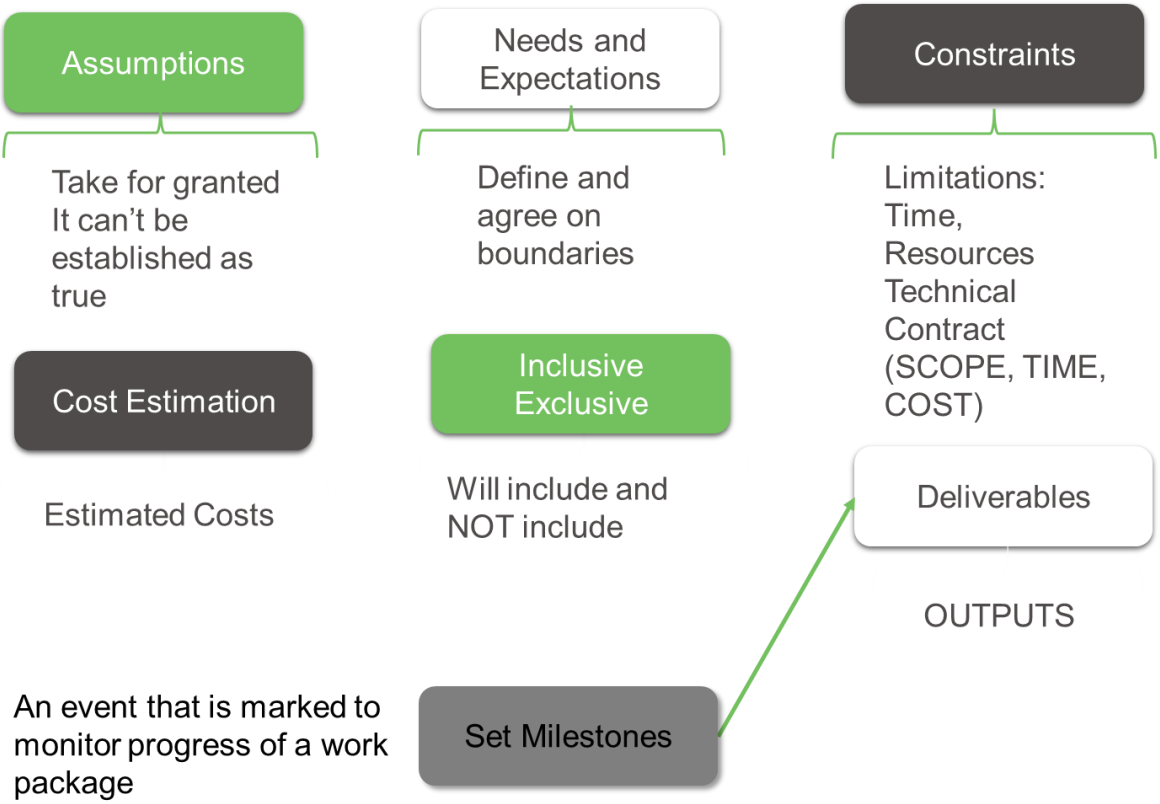
The stakeholders identified, defined, and analysed to ensure needs and expectations can be met.

A mission statement and objectives of the project established, the major deliverables identified and documented with duration as well as the project duration.

Furthermore, a background of the reason why the project is being undertaken with a project justification to justify the projects existence and execution in terms of value either monetary or overall benefit to community. This must then be authorised and approved by the project manager.

Lastly a change control process developed to establish the process that should be followed in the event of a change occurring.

In addition, during planning the following areas should be considered and documented in the plan, which could be in the Project Charter.

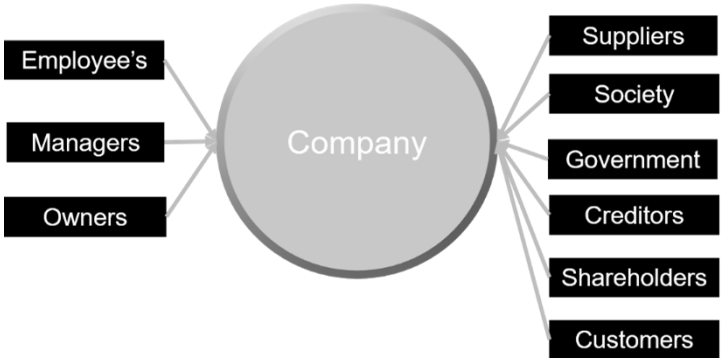


Assumptions of the project, things that will be taken for granted and can't be established as true. The needs and expectations – this set the agreed of upon boundaries of what will be accepted and unacceptable standards, behaviour, outputs, etc.

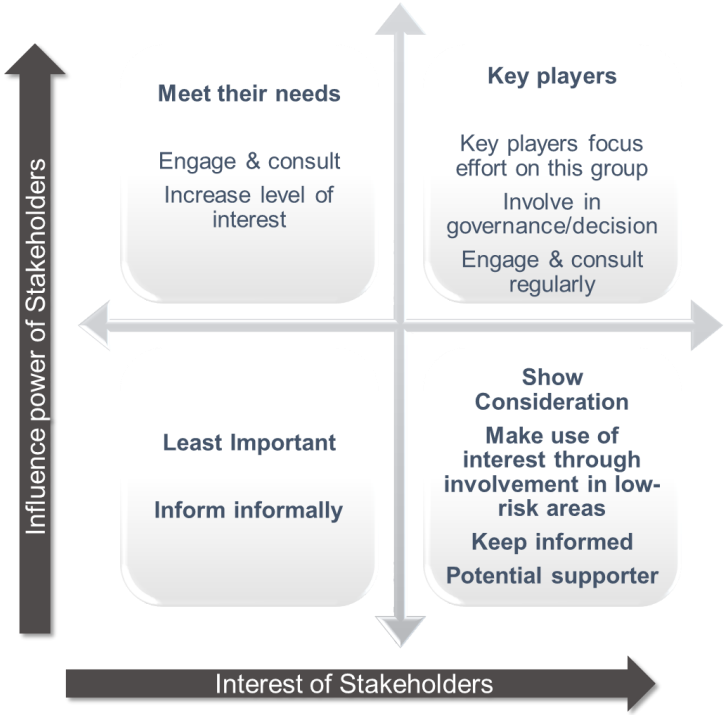
Overall constraints of the project any limitations that have been set for the project. Estimated costs, what will be included and excluded in the scope as well as the highest level of deliverables, the project phases with set milestones to be achieved during the project.

PROJECT STAKEHOLDERS

Any person, group and or organisation that has an interest or concern in a project.



Stakeholders can be analysed using the matrix of influence power over the interest they may have in the project.



Where the top left quadrant symbolises stakeholders that have high power but low levels of interest in the project and what needs to be done to meet their needs.

Key players are placed in the top quadrant to the right indicating stakeholder that have both high power and high interest in the project, the bottom left quadrant stakeholders with low interest low power and the last quadrant low power high interest.

By doing this analyse will help in ensuring all stakeholders are categoried and informed sufficiently during execution.

PROJECT CHANGE CONTROL

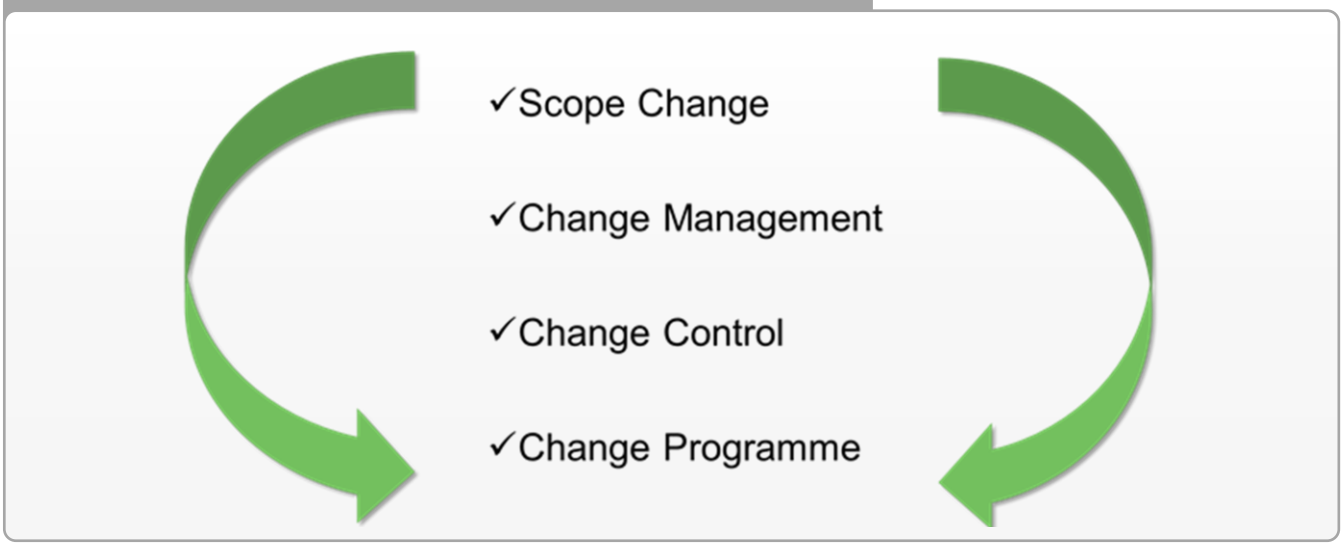
Plan for change during the project execution as change is inevitable. Different types of changes that may occur are scope change, change management where management process for changes to project deliverables, then change control this for any technical changes that may occur and change programs which are multi-faceted business solutions.

Change can be driven by a number of factors:

- Business needs may change
- Legislation and regulations,
- Other projects
- Stakeholder needs

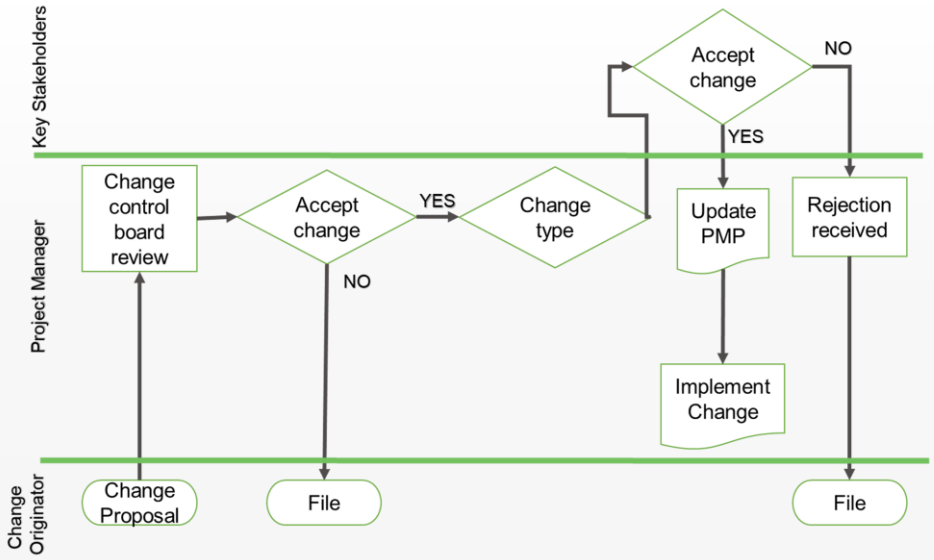
However, a process is necessary to evaluate the triple constraints of the project to identify what it will affect in the project, the scope is evaluated, the cost that the change will bring and how the current time of the project will be affected by the change.

Types of Change



As mentioned, changes can't just simply be implemented as the change may affect various parts of the ongoing project, this needs to be evaluated be the change is implemented. The process example shows and typical example of a change control procedure.

Example Change Control Process



PROJECT SCOPING

Project scope is a part of project planning that requires determining and documenting specific goals, deliverables, and tasks that need to be completed to achieve the overall objective of the project. It is therefore the extent of the area or subject matter that something deals with or to which it is relevant as the word scope is defined in the dictionary.

Defining scope is perhaps the most important part of the upfront definition and planning process. If you don't know for sure what you are delivering and what the boundaries of the project are, you have no chance for success.

Project Scope Management includes the processes required to ensure that the project includes **all the work required, and only the work required**, to complete the project successfully. Project scope management is primarily concerned with defining and controlling what is and is not included in the project. A project scope management plan is contained in, or is a subsidiary of, the project management plan.

The components of a project scope management plan include:

- A process to prepare a detailed project scope statement based upon the preliminary project scope statement.
- A process that enables the creation of the WBS from the detailed project scope statement and establishes how the WBS will be maintained and approved.
- A process that specifies how formal verification and acceptance of the completed project deliverables will be obtained.
- A process to control how requests for changes to the detailed project scope statement will be processed.

The purpose of defining scope is to clearly describe and gain agreement on the logical boundaries of your project.

Defining and managing the project scope influences the project's overall success. Each project requires a careful balance of tools, data sources, methodologies, processes and procedures, and other factors to ensure that the effort expended on scoping activities is commensurate with the project's size, complexity, and importance.

Project Scope is the part of a project planning that involves determining and documenting a list of specific project goals, deliverables, tasks, and deadlines.

Activities under Project Scope Management

Management Process	Initiation	Planning	Executing	Monitoring & Controlling	Closing
Project Integration Management	Develop Project Charter	Develop Project Management Plan	Direct & Manage Work	Monitor & Control Project Word Perform Change Control	Close Project or phase
Project Scope Management		Plan Scope Management Collect requirements Define Scope Create WBS		Validate Scope Control Scope	
Project Time Management		Plan Schedule Define Activities Sequence Activities		Control Schedule	

Scope statements are used to define what is within the boundaries of the project and what is outside those boundaries. The more aspects of scope you can identify, the better off your project will be.

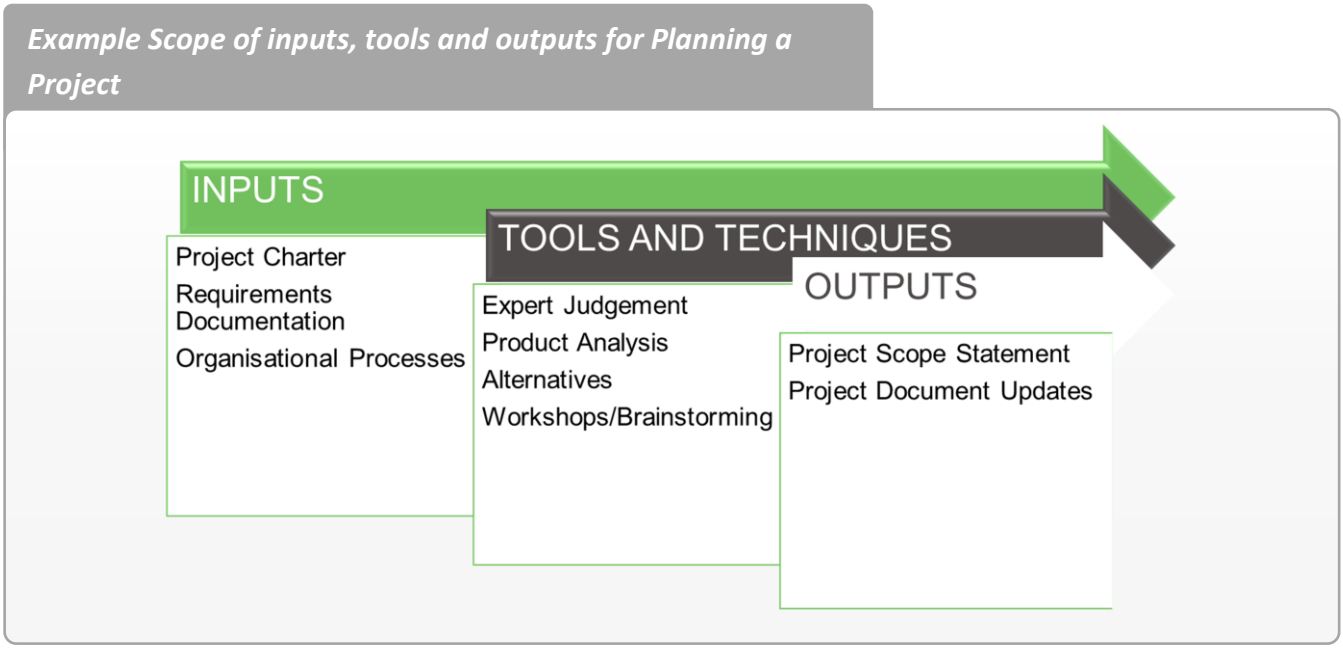
Project scoping refers to product and project scopes, product scope is the features and functions that characterize a product, service or result and project scope to the work that needs to be accomplished to deliver the product.

The preparation of a detailed project scope statement is critical to project success and builds upon the major deliverables, assumptions, and constraints that are documented during **project initiation** in the preliminary project scope statement.

- Forces creative thinking through elements of the project
- Interprets Outputs
- Verifies project objectives of planned works
- Validates interpretation of planned work

Project Scope is the part of a project planning that involves determining and documenting a list of specific project goals, deliverables, tasks, and deadlines.

Example Scope of inputs, tools and outputs for Planning a Project



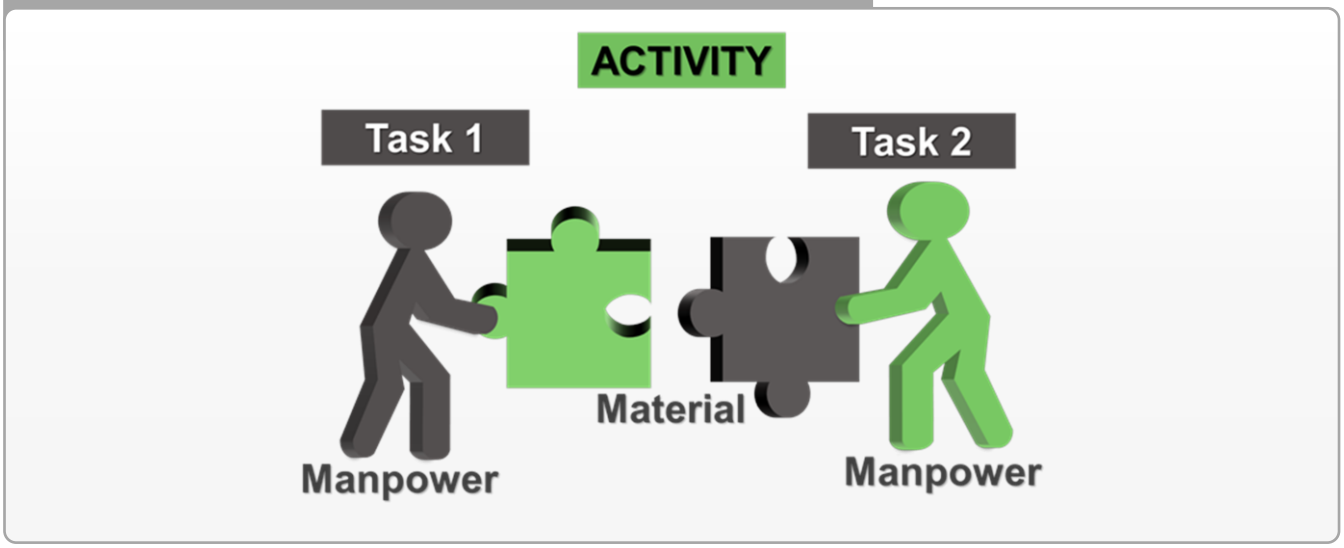
Make sure that the goals and objectives in planning are effectively set to ensure that smaller component goals can be aligned and logically ordered to meet with individual goals to get to the overall objective of the project.

Determine the Principal Work Activities

An **activity** is any subdivision of project tasks. The set of activities defined for a project should be **comprehensive** or completely **exhaustive** so that all necessary work tasks are included in one or more activities.

Typically, each design element in the planned project will have one or more associated project activities. Execution of an activity requires time and resources, including manpower and equipment.

Example Scope of inputs, tools and outputs for Planning a Project

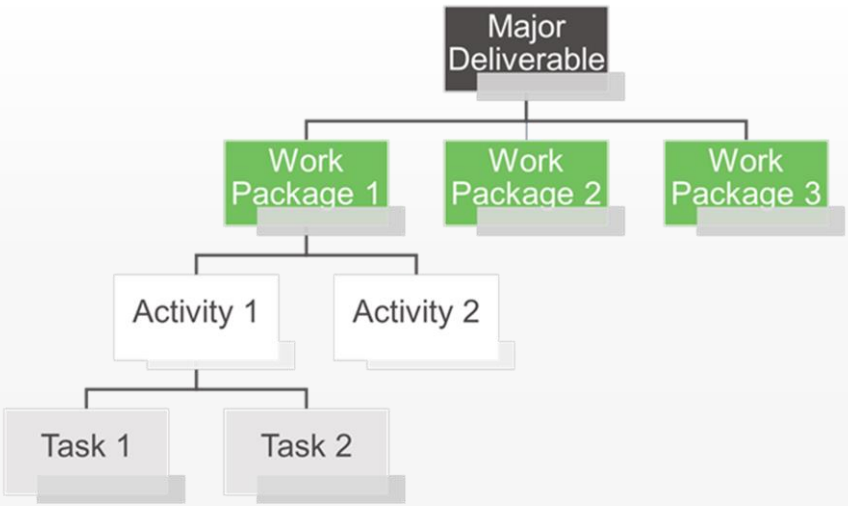


Each phase of a project is composed of a number of major activities that will lead to achieving one or more deliverables. Activities are composed of a series of tasks that are the lowest level of detail that can comfortably be managed. Team members who will be performing the tasks should be involved in the activity/task planning process.

WORK BREAKDOWN STRUCTURES

Work breakdown structure or WBS is a tool used to structure activities and tasks. It is an oriented hierarchical structure that assists in breaking work down into manageable portions. It organizes and defines the scope of the project. The planned work contained within the lowest-level WBS components, which are called **work packages**, can be scheduled, cost estimated, monitored, and controlled.

Example hierarchal WBS



Work breakdown structures can be structured in two ways namely hierarchal graphical or using numbered levelling to show decomposed levels of work that needs to be performed. The example shows a work break structure in hierarchal form, while a numbered 1, 1.1, 1.2, 1.3 further levelling 1.1 down to 1.1.1, etc. It also represents the major deliverables and sets levelling for work package levels and then activity to task levels.

Example Number format WBS

1. Major Deliverable

1.1 Work Package 1

1.1.1 Activity 1

1.1.2 Activity 2

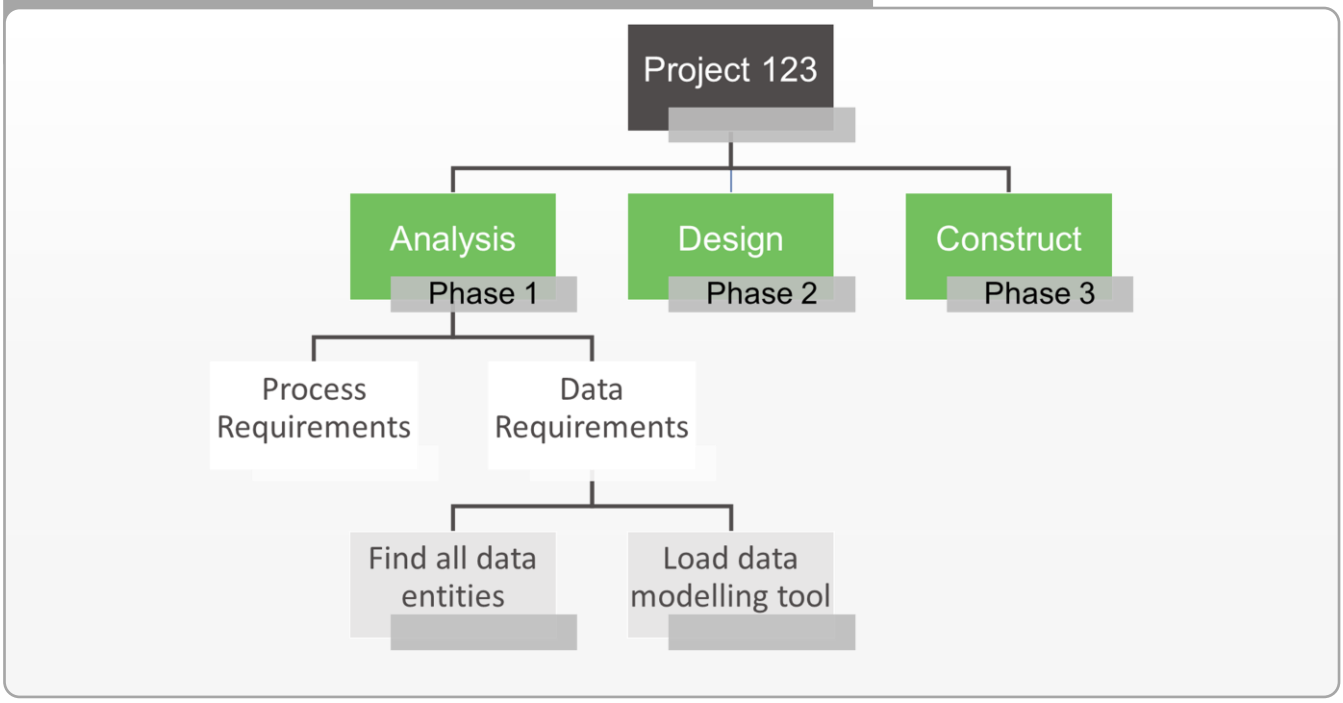
1.2 Work Package 2

1.3 Work Package 3

The sequence of activities are aligned to a variety of techniques that can be used for instance by time, availability of resources, logical sequence of events, etc. for instance in the example we can see that

activities that have been planned in Phase 1 are most likely in logical sequencing from process requirements – data requirements then conceptual design which are the main level of activity for the major deliverable Analysis.

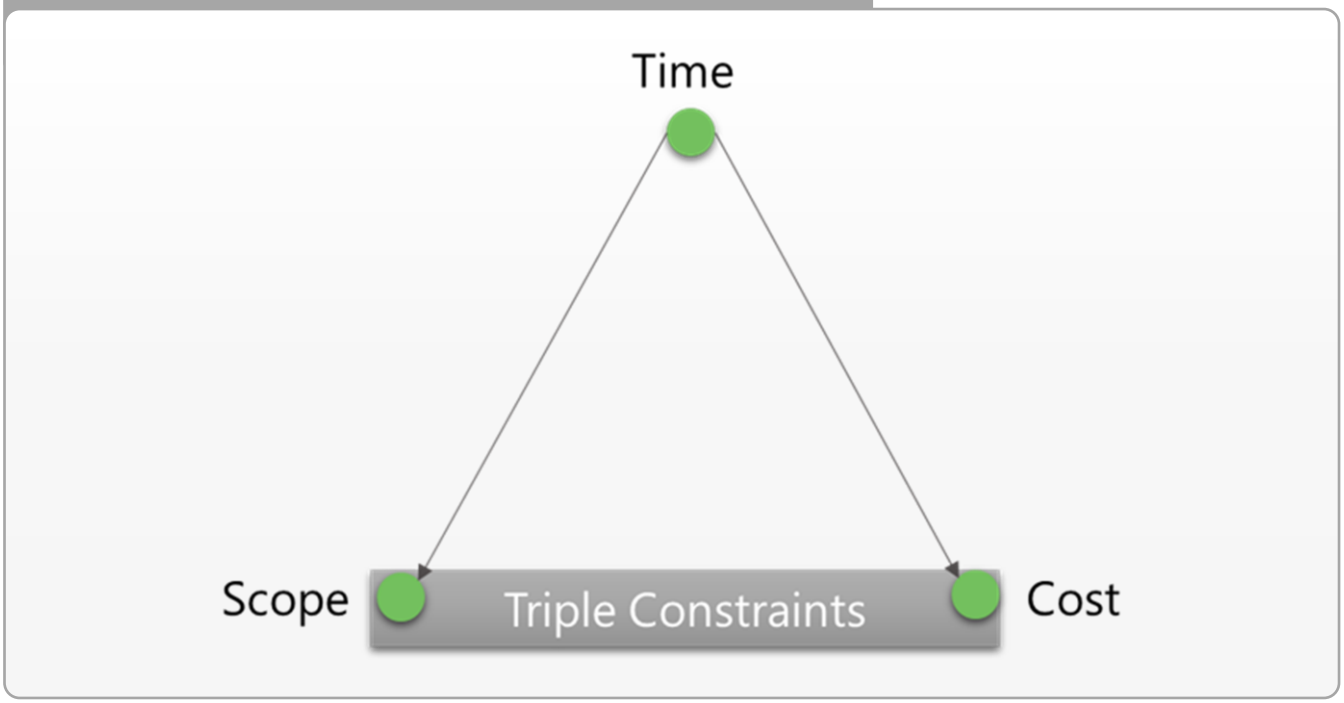
Example outputs of a project



PROJECT SCHEDULING

Project scheduling is that part of project management that schedules planned activities from the WBS by allocating time and resources to each activity. A schedule is a program of events or appointments expected in each time, where the events are broken down into major and minor phases, milestones allocated, activity and resources are allocated to each task. It ensures that the planned work is governed within the triple constraints of a project.

Triple Constraint



The purpose of scheduling is to:

- Match resources,
- Eliminate bottlenecks during execution,
- Allow for timely procurement,
- Important in project success within time,
- Budget, cost, changes and risks can be managed efficiently.

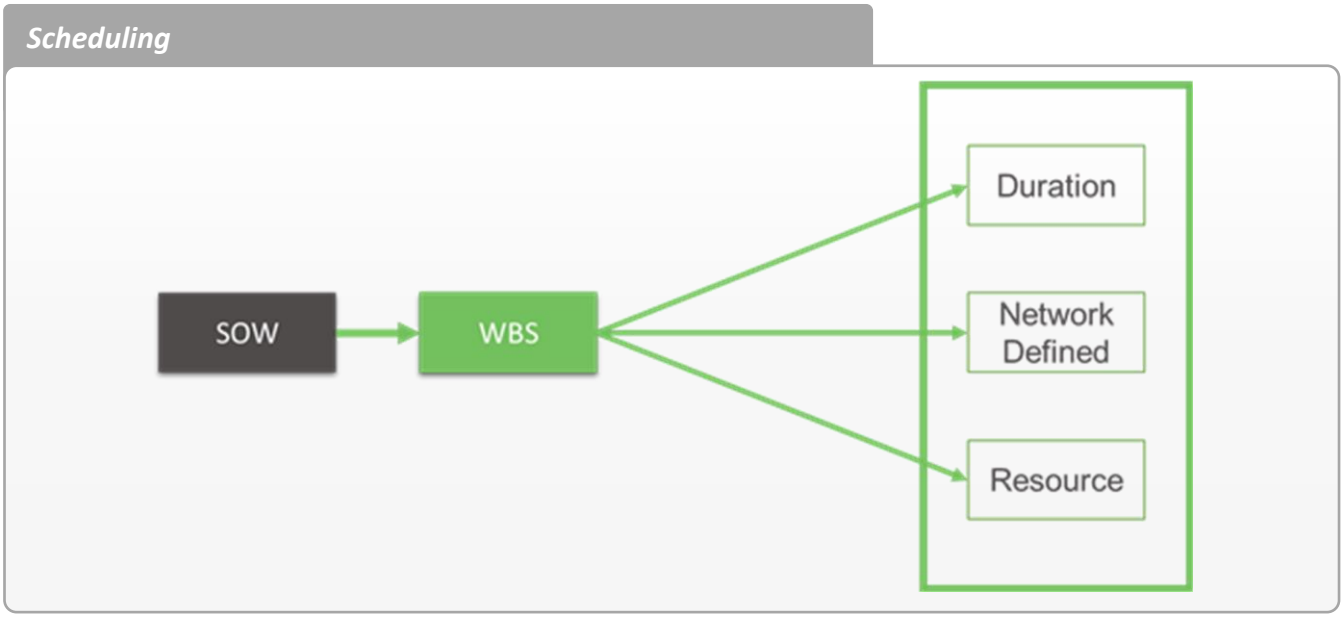
Scheduling principles include the rule of morally correct behaviour, and or execution of activities.

The principles during project scheduling are based on:

- Baseline – things that have happened before meaning that they consistent with experience – for instance if you had an activity that has been performed before you would analyse that activity and the sequence of events that were executed then base your current estimate on the timeline of that activity in that project.
- Expert interviews – by interviewing experts we can get a better gauge on what can be expected and what time frames to allocate.
- Experience in subject matter areas
- Industry standards.

- When creating a schedule don't be to optimistic in estimation – schedule only 80% of the time,
- Know your schedule – Good communication – meetings, emails
- Stick to the schedule – Monitor planning
- Control Changes efficiently – Fully analysis
- Base delivery time on market related – find out best practice/time/method

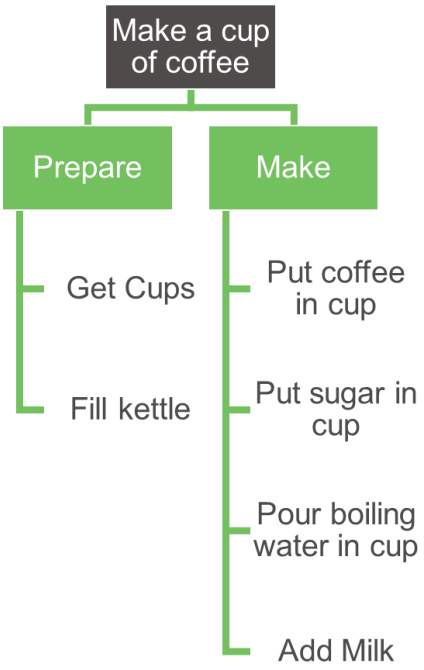
To create a schedule, you will need the scope or statement of work and the work breakdown structure, durations are then allocated to each activity/task, resources required for the specific activity or task, and the network between activities defined.



For instance: If we wanted to create a schedule to make a cup of coffee, it may look something like this:

Activity	Duration	Start	End	Resource
Prepare	1 minutes	Date	Date	Me
Get Cups	30 seconds	Date	Date	Me
Fill kettle with water	30 seconds	Date	Date	Me
Make	1 minute	Date	Date	Me
Put coffee in cup	20 seconds	Date	date	Me
Put sugar in cup	20 seconds	Date	Date	Me
Pour boiling water in cup	10 seconds	Date	Date	Me
Add milk	10 seconds	Date	Date	Me

The work breakdown structure to make this coffee will mostly like look as follows:



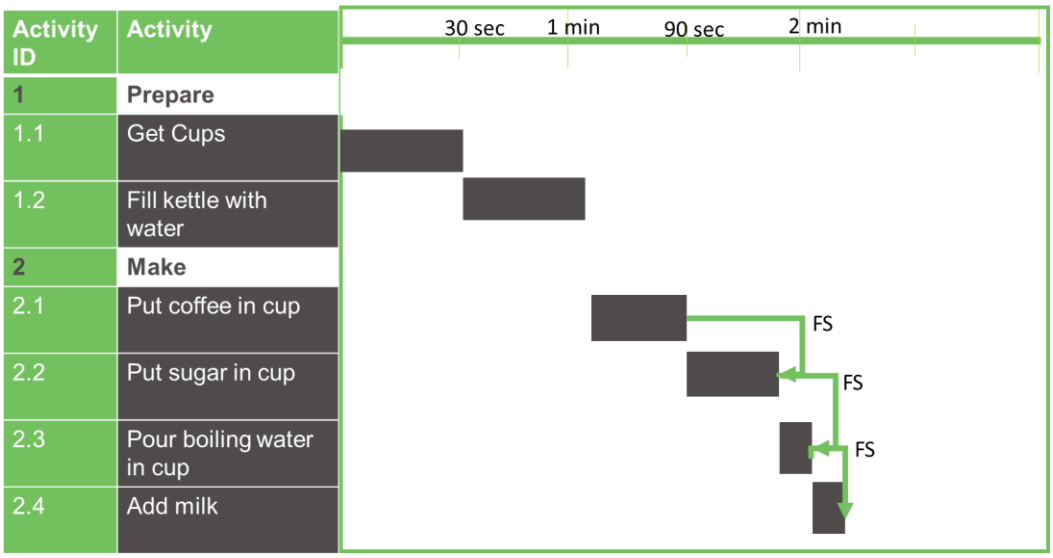
Notice how the network of activities has been divided into 2 main programs the preparation and then the making of the coffee. The work packages then follow of the work effort that needs to be performed while making this coffee. From the schedule notice how, the main programs calculate to the total of the work package. Then we need to create a relationship between the various activities and their related tasks.

The Activity ID allows us a means of connecting and linking activities to each other. The predecessor column determines the link. In the example we can see that the preparation tasks are not dependent on any tasks in the schedule, however in this case making the coffee is dependent on the preparation tasks.

Activity ID	Activity	Duration	Start	End	Resource	Predecessor
1	**Prepare**	1 minutes	Date	Date	Me	
1.1	Get Cups	30 seconds	Date	Date	Me	
1.2	Fill kettle with water	30 seconds	Date	Date	Me	
2	**Make**	1 minute	Date	Date	Me	
2.1	Put coffee in cup	20 seconds	Date	date	Me	1.1
2.2	Put sugar in cup	20 seconds	Date	Date	Me	1.1
2.3	Pour boiling water in cup	10 seconds	Date	Date	Me	2.2,2.1
2.4	Add milk	10 seconds	Date	Date	Me	2.3

A gantt chart, helps us display the scheduled information graphically, this chart was discovered by Henry Gantt in the 1700's as means of graphical display for the information.

Because "me" is the only assigned resource, you would need to do one of the 2 tasks in the preparation one after the other, so they will not be linked to each other but can't be done simultaneously unless another resource is assigned.



The next package, we know that the activities are linked in parallel as we can't do the one without the other. So, they will have a linking relationship from finish to start. This means that each task must finish before the next can start. Other relations include:

A start-to-start relationship is rarely used but worth knowing about, it is simply when 2 tasks can start simultaneously. Then a start to finish meaning simply that one task must start before another can be finished.

Other duration techniques including adding leads and lags. Leads are simply the time need for an activity to start before another can start, a lag on the other hand is the time that needs to elapse before another can start, for instance in our case of making coffee we may have a waiting time while waiting for the kettle to boil.

Categorising tasks and their dependencies take a lot of time and thought into ensure that activities/tasks are categorised according to their order of execution. Logical would be an example of

what we have just done with our coffee project, resource would be scheduling tasks according to the available resources, then according to priority what must be done first which could also translate to logical, and tasks in series the same, then by overlapping tasks/activities to get the most benefit in ensure execution on time within scope and budget.

PROJECT COMMUNICATION

Communicating regularly and effectively is a key to successful projects. This entails sharing the **right** information with the **right** people in a **timely** manner.

Informative communication supports the following:

- Continued buy-in and support from key audiences and team members
- Prompt problem identification and decision-making
- A clear project focusses
- Ongoing recognition of project achievements
- Productive working relationships among team members

Design a communication plan by asking the following questions:

- Who needs to receive information?
- What kind of information is required?
- When is the information needed?
- How should the information be presented?
- How is the team going to work together?
- How are status meetings going to run?

A typical example of a communication plan will look as follows – we can see what is to be communicated, the type of communication it is, who the audience is, the vehicle that will be used to deliver the communication the frequency of delivery and who will be responsible for the drafting and delivery of the communication.

Formal combinations are pre-planned, conducted in a standard format in accordance with an established schedule. Examples include weekly team meeting and monthly

progress reports.

Informal meetings occur as people think of information that needs to be shared. These forms of communication occur during the normal course of business and include brief conversations in the corridor, emails, and chats over lunch.

PROJECT COSTING/BUDGETING

You would need to ideally make a budget at the beginning of the planning session regarding the project at hand. Here we have an example of a budget, let's look at the difference between budgeting and costing.

What does budgeting mean?

Costing in often confused with budgeting, in that we are given a budget and want to spend all the money, however budgeting refers to a list of planned expenses and or revenues. Budgets have the following advantages:

- To provide a measure against actual expenditure enabling a financial operation of a business
- Allows evaluation of performance based on baselines
- Allows control of working environment
- Allocates resources based on prior corporate planning

Costing on the other hand is the allocation of estimate cost to each activity on the schedule.

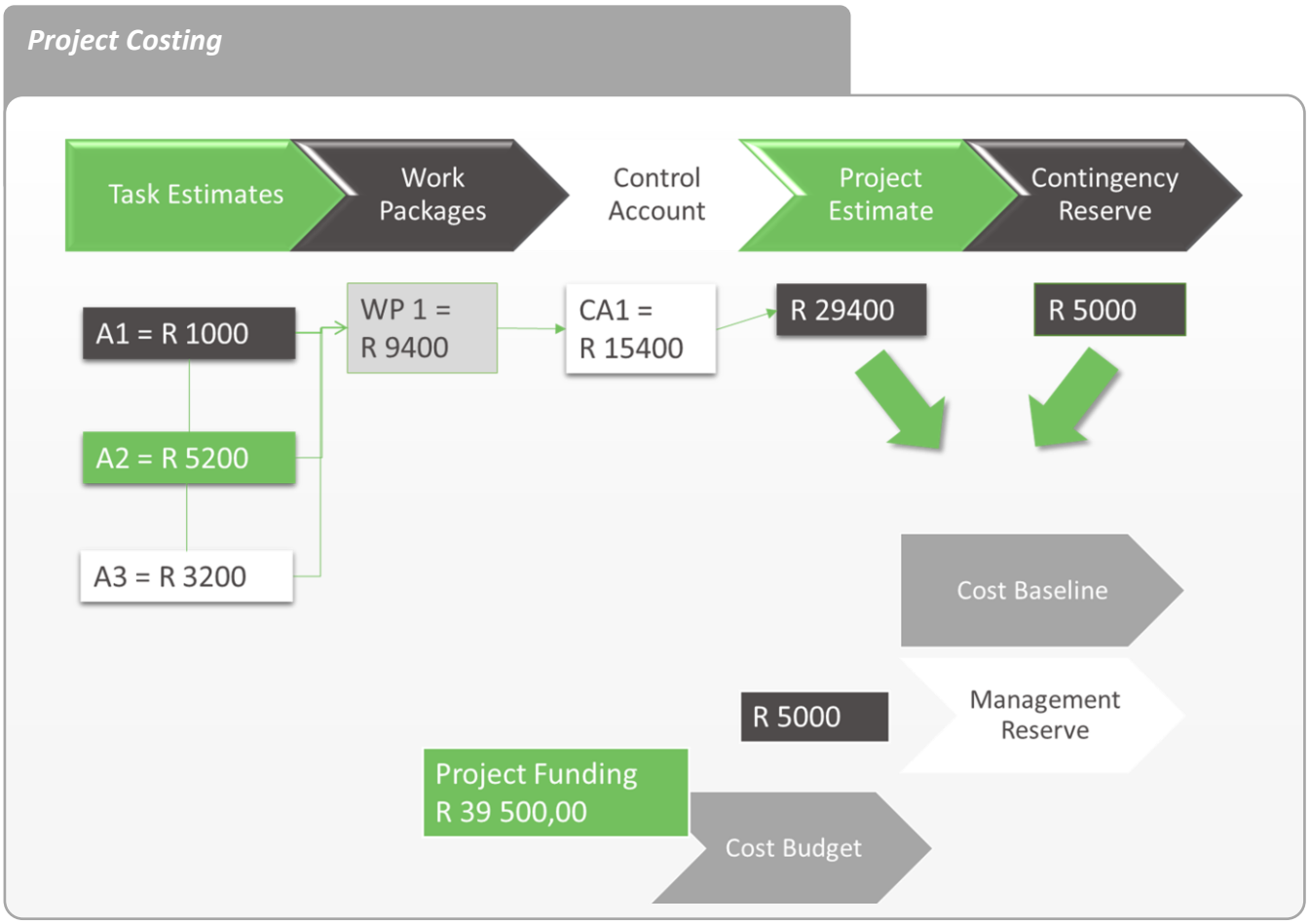
Just a recap of our 10 knowledge areas according to PMBOK we have dealt with the project management scope, the schedule, risks, communication and now moving on to costing. From the table we can get a good idea of the activities that we need to perform through the life cycle of project and the processes that need to be followed to create project documentation.

Management Process	Initiation	Planning	Executing	Monitoring & Controlling	Closing
Project Cost Management		Plan Cost Management Estimate Costs Determine Budget		Control Costs	

The Costing process can be simplified as follows:

Each tasks cost is estimated, each total of the work package calculated to result in a total per work package these are then allocated to a control account, work packages should be categories per control account, then all control accounts calculated to gather a project total.

Then a contingency reserve estimated based on costs of contingencies planned for during risk planning, this value then provides a cost baseline, management then adds a reserve estimate based on unforeseen forecasts, then values are then added to provide a cost budget which is then aligned to the budget allocated for the project.



Project Cost Terminology you may be dealing with

- **Cost:** is a resource sacrificed or foregone to achieve a specific objective – usually measured in monetary value.
- **Project Cost Management:** a process required to ensure that projects are completed within approved budget.
- **Cost Estimating:** Estimating an approximate value through calculation.
- **Cost Budgeting:** Overall cost estimation from individual work items.
- **Cost Control:** Control changes to project budget.

Just as with any budget we need to be able to identify the different types of cost that will be encountering during this process during project planning.

- Fixed costs are related to once of values allocated to a number of activities,
- Variables are costs that may change.
- Direct costs are costs that are directly related to a project.
- Indirect costs are costs that are not directly related to the project for instance: work effort from an employee of an organisation, for the time spent on the project during normal working hours.

So how do we know what and or how to estimate these costs. The following techniques help to know how to estimate costs:

- **Analogous or top-down estimates**: Use the actual cost of a previous, similar project as the basis for estimating the cost of the current project.
- **Bottom-up estimates**: Involve estimating individual work items or activities and summing them to get a project total.
- **Parametric modelling**: Uses project characteristics (parameters) in a mathematical model to estimate project costs.
- **Computerised tools**: Tools, such as spreadsheets and project management software, that can make working with different

Here are some ideas of when to use which technique – the analogous method we use when we are checking for feasibility and generally past project data is used. The parametric method is used when estimating individual activities/tasks, with this method historical data can be used, quotations can be used. Vendor bid analysis, is used when cost estimation and control is done for tendering for projects.

Costing Methods

Method	When to use	What to use
Analogous	When checking on feasibility	Past project data
Parametric	When calculating an estimate for activity parameters	Historical data and other variables
Vendor Bid Analysis	Cost estimation and control purposes	Published details of competitor pricing structures

Keeping track of all actual costs is also equally important as any other technique. Here, it is best to prepare a budget that is time-based as learnt in the budgeting process, by allocating costs accordingly, it will make it easy to track costs as they happen, this will help by keeping project costs in check.

Then we can calculate the variance between the planned costs vs the actual cost and graphically represent it using a graph to quickly determine whether we are on budget or not.

Example Schedule with costing

Activity ID	Activity	Duration	Actual Start	Start End	Resource	Predecessor	Cost	Actual Cost
1	**Prepare**	1 minutes	Date	Date	Me		R20.00	R18.50
1.1	Get Cups	30 seconds	Date	Date	Me		R10.00	R9.00
1.2	Fill kettle with water	30 seconds	Date	Date	Me		R10.00	R9.50
2	**Make**	1 minute	Date	Date	Me		R15.00	
2.1	Put coffee in cup	20 seconds	Date	date	Me	1.1	R2.50	
2.2	Put sugar in cup	20 seconds	Date	Date	Me	1.1	R2.50	
2.3	Pour boiling water in cup	10 seconds	Date	Date	Me	2.2,2.1	R5.00	
2.4	Add milk	10 seconds	Date	Date	Me	2.3	R5.00	

PROJECT QUALITY

Quality is a dynamic state associated with products, services, people, processes, and environments that meets or exceeds expectations.

Quality is the overall measure of our project in terms of cost, scope and time, once these 3 constraints have been met quality should be achieved. During planning the quality element of each constraint, task activity and work effort must be standardised to ensure an effective measure during execution.

Quality is governed by the following elements:

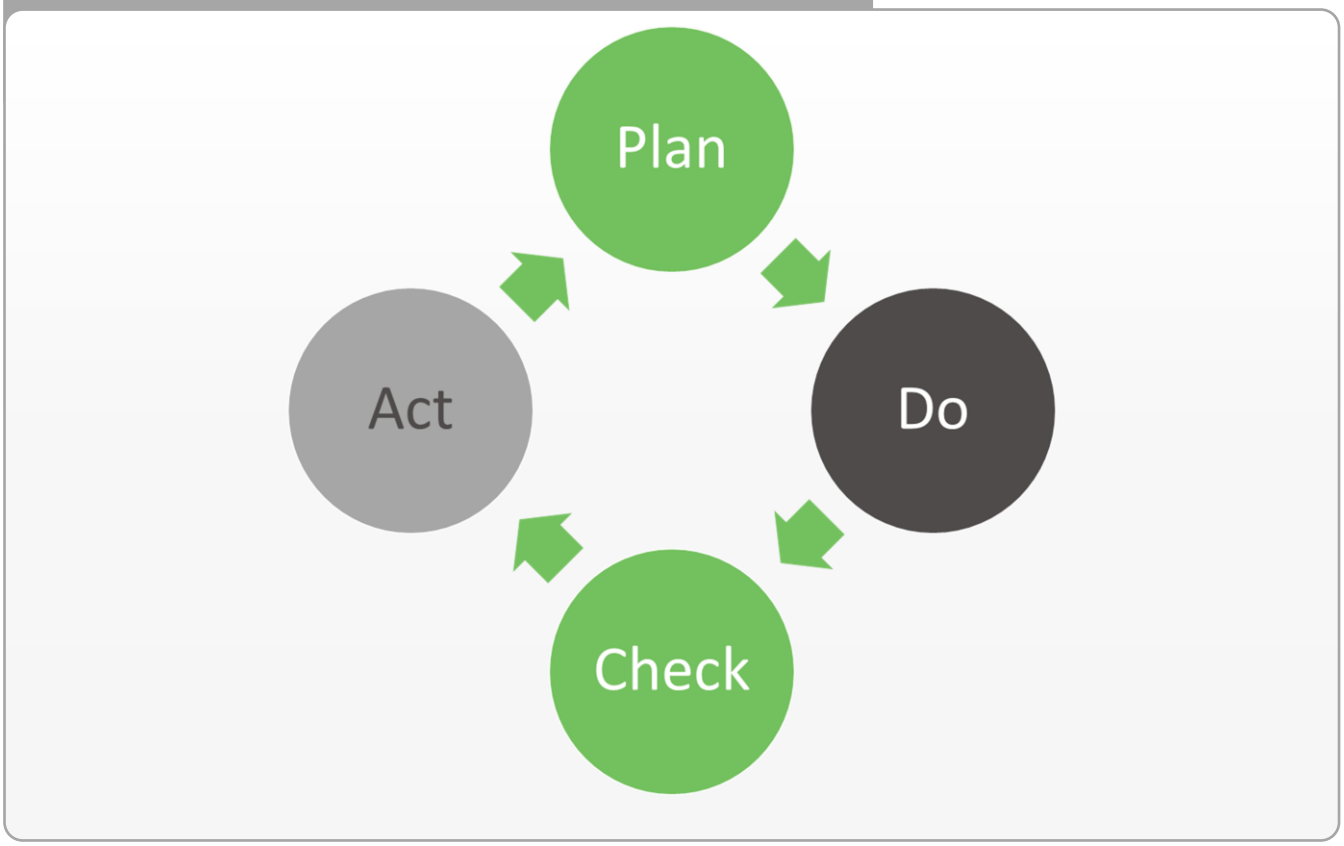
- Management Responsibility
- Documented Quality Management Systems
- Design Control
- Document Control
- Purchasing
- Inspection Testing
- Non-conformance
- Corrective Actions
- Quality Records
- Quality Audits
- Training

This quality standard can be represented as follows the acceptance of planned deliverables against the met quality requirement specified for each deliverable.

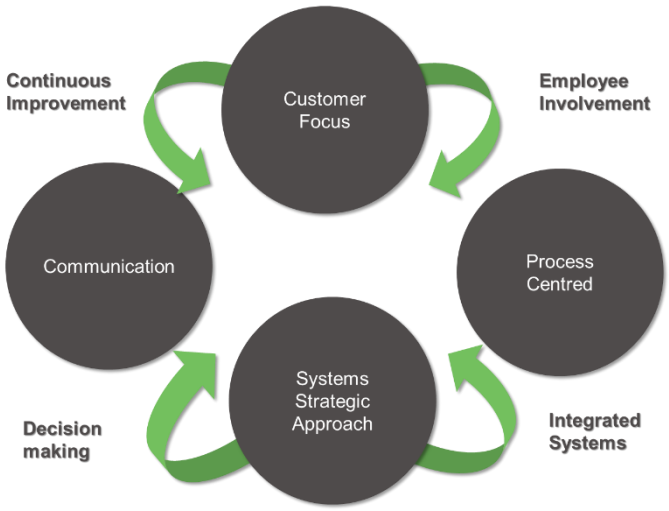
Quality should constantly be improved, during execution the current level of quality must be measured against the expected level of quality.

Quality control can be conducted using a Shewhart cycle, where the process involves the planning of quality standards, execute, check the result, act on the results and then repeat the entire cycle periodically.

Shewhart Cycle



This Total Quality Management as learnt in Topic 7 of Cluster 7 is applied during project quality management.



Remember if you can't measure it, you can't improve it.

PROJECT RISK MANAGEMENT

What is a risk – the possibility of meeting danger or suffering harm. Project risk however can be defined as the potential impact to an asset or some characteristic value that may arise from some present process or form some future event.

It therefore combines the probability of event occurring with the impact that event would have.
Tools and techniques to identify risks:

- To identify risks the following tools and techniques can be used to determine risks. Some of which you will learn about in the next topic. High level deliverables of a project, WBS and Project Schedule
- Scope change requests
- Project Assumptions
- Project team inputs
- Stakeholder and sponsor input
- Formal risk identification
- Previous lessons learned
- Audits and reviews
- Performance and status reports
- Diagramming techniques cause and effect/process flows

Once we have identified the potential risks, the risks can be classified according to the following types of risks. Potential risk which is a risk that has a less than 100% probability of happening, Actual risk if it will happen and a perceived risk when a subjective judgement is made about the characteristics and severity of a risk.

Term	Explain	Example	Trigger
Potential Risk	It may happen – probability of less than 100%	Project delayed due to lack of resources	Unreliable supplier
Actual Risk	If it has a probability of 100%	Strike action	Union strike
Perceived Risk	Subjective judgement that is made about the characteristics and severity of a risk	Underestimate likelihood of workers going on strike	Incorrect judgement

Then we need to determine the probability of a risk happening, to determine this value a scoring technique can be used based on the probability factor for instance on a scale of 0 – 5 where 0 is highly unlikely and 5 highly likely.

So, let's say we are for seeing that our deliveries may not arrive on time because the supplier has communicated that it may be delayed, but not sure for how long, we can apply a rating of 3 to the probability of the risk happening.

Example Probability Calculation

Risk Probability

Unlikely				Highly likely	
0	1	2	3	4	5

Project delayed due to lack of resources

$$= \frac{The\ number\ of\ ways\ an\ event\ occurs}{The\ total\ number\ of\ possible\ outcomes}$$

A more concise evaluation is done by doing qualitative analysis on how often a delay in supplies happens with the current supplier meaning you would gather data over an agreed period of time from the supplier on how often delays occur, then a statistical analysis done to more accurately determine the probability factor by using a probability calculation. By dividing the number of ways an event occurs by the total number of possible outcomes.

Then we determine the impact that this delay would have on the project by evaluating the plan and determining whether the delay would cause a delay in the project ending on time. If it won't impact the project, then the impact will be low maybe a 1 or 0. Remember that it isn't to say that if a probability is high that the impact will also be high and vice versa.

Example Impact Calculation

Risk Impact

Project delayed due to lack of resources

Low 0	1	2	3	4	High 5

Then we multiply the probability by the impact to determine a threat value. In this case the threat value is 4, the threat value can then be quantified by the using the following matrix to determine the level of the risk according to the matrix.

Example Threat Value Calculation

Threat Value

Risk	Probability	X Impact	Threat Value`
Project delayed due to lack of resources	3	1	3

The colours in the risk matrix represent from green to red, where the green values represent low risks, yellow moderate, orange moderate to high and the red areas or threats values very high

meaning that you will want to monitor your plan closely to be able to mitigate those risk if they occur because the likelihood of then occur is high and the impact they will have will jeopardise your project success. So how do we mitigate risks, by planning contingencies.

Risk Quantification

		Impact of the risk/damage/injury				
		1	2	3	4	5
Likelihood of the risk/damage/ injury occurring	5	5	10	15	20	25
	4	4	8	12	16	20
	3	3	6	9	12	15
	2	2	4	6	8	10
	1	1	2	3	4	5

Mitigation is planned for through contingency where a contingency is a plan of action that is planned for in case of the risk occurring then the contingency will be executed.

Risk can further be categorised into the following categories:

- Financial/Economic, so if a risk will result in the loss of money and or running out of money, economical markets changing etc.

- Operational risks are related to risks that occur as a result of operations.

- Reputational when an organisations name and or brand will be at risk if it occurs, program risk is like operational risks but only apply to sub-program activities with the project and then finally health and safety risk.

A variety of measures can be taken to reduce and or stop a risk threat cause, avoidance where a measure is introduced during planning to ensure the risk doesn't occur, then we could:

Modify an existing program, activity or task to reduce the risk, take safety precautions, retain or accept that certain risks may occur then lastly share and transfer the risk.

Steps to develop the Contingency Plan:

Step 1: Risk Management Planning - The manager and the team decide who is going to develop the risk management plan
Step 2: Risk Identification - The assigned team identify the various risks and make a list of the risks through brainstorming, interviewing and sample risk lists.
Step 3: Risk Probability - The risk management plan team, determine the probability of the risks occurring through Impact Scales.
Step 4: Risk Response Plan - The risk management plan team decides for each identified risk whether to accept the risk, avoid the risk or accept the risk.
Step 5: Risk Monitoring and Control - Risk monitoring and control is a process that lasts the entirety of the project. The team monitors the risks as the project matures, new risks develop and anticipated risks disappear.

The contingency plan should specify the responses to each of the different types of loss situations, setting out the steps to be followed under various circumstances and assigning responsibilities for various tasks.

RISK MANAGEMENT LEGISLATION

In terms of the South African Compensation for Occupational Injuries and Disease Act, applicable to most classes of employees, automatic compensation is paid from a state administered fund. This relieves employees from having to prove negligence by the employer, but also means that they cannot sue the employer.

This does not free the employer of the need to take suitable precautions.

Requirements have been laid down, some of the principal statutes being:

- The Occupational Health and Safety Act No 85 of 1993 (as amended)

- The Mines and Works Act No 27 of 1956 (as amended)
- The Electricity Act No 40 of 1958 (as amended)

all as read in conjunction with the Criminal Procedure Act No 51 of 1977 (as amended).

Failure to meet these requirements will result in criminal action against the person responsible. Special audit sheets are needed to check that the requirements are met.

Note: These are also regulations relating to specific trades and types of hazard.

ROLE OF ORGANISATIONAL POLICIES AND PROCEDURES

Quality standards are defined in terms of company, legislation, or industry standards. Company policies and procedures are developed as a result of interpreting industry standards and/or legislation. The company policies and procedures form part of the risk management process in that they provide guidelines to ensure that the company adheres to industry standards and legislative requirements:

- Statutory Requirements, e.g., Acts, Bills
- Regulatory Requirements, e.g., Regulations, Rules
- Supervisory Requirements, e.g., Directives, Codes, Standards, Procedures, Rulings
- Company codes, policies and procedures

RISK MANAGEMENT POLICY

An organisation's risk management policy should set out its approach to and appetite for risk and its approach to risk management. The policy should also set out responsibilities for risk management throughout the organisation.

Furthermore, it should refer to any legal requirements for policy statements e.g., for Health and Safety.

Attached to the risk management process is an integrated set of tools and techniques for use in the various stages of the business process. To work effectively, the risk management process requires:

- Commitment from the chief executive and executive management of the organisation
- Assignment of responsibilities within the organisation

- Allocation of appropriate resources for training and the development of an enhanced risk awareness by all stakeholders.

QUALITY STANDARDS

Quality standards are the measurable quality requirements for each work responsibility or duty, often referred to as the output of your work.

Outputs are the products and services that individuals in an organisation provide to one another or to the customer, such as:

- An answered telephone
- A clean floor
- A serviced car
- A completed report
- An issued policy documents
- A teamwork plan

Listing responsibilities as outputs is useful, because there are many ways to produce an output even though the standards that need to be maintained are the same. By listing outputs, you encourage a process of continuous improvement, because you create a certain amount of freedom, to the person producing the outputs, to experiment with different ways of doing the work in an attempt to improve the way the outputs are produced.

Example: The receptionist is required to answer the telephone within 3 rings in a polite professional manner.

- As the standard has been set, the receptionist can now be measured accordingly.
- The receptionist would have been informed why this is important (image of the company) and would now understand why she has to comply with the standard.

Quality standards provide guidelines in terms of requirements that need to be met to make sure that the outputs are produced according to set standards. Quality standards are often defined in terms of regulatory compliance, cost, time, quantity and quality.

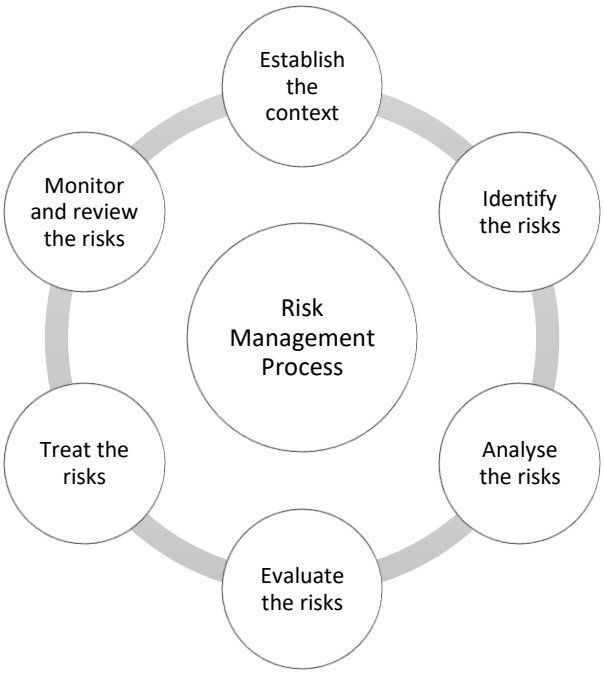
RISK MANAGEMENT PROCESS

The risk management process is the series of steps that enable initial and continual review of risk and help to ensure that the business is on-track for meeting its objectives.

The risk management process helps to put in place and review the risk management plan (see notes later in this module).

The elements of the risk management process are:

- Establish the context
- Identify the risks
- Analyse the risks
- Evaluate the risks
- Treat the risks
- Monitor and review



Establish the context

When considering risk management within a small business, it is important to establish boundaries for the risk management process. For example, a business owner may be only interested in identifying financial risks so information collected will only cover that area of risk.

In establishing the context, consider:

- the objectives of the business
- key stakeholders and impacts
- risk categories.

It is generally more productive to break down the risks into categories, rather than identify risks for the company as a whole.

Identify the risks

Risk cannot be managed unless it is identified. Once the context of the business has been defined, the next step is to use this information to identify as many risks as possible.

The aim is to identify the risks that may affect, either negatively or positively, the objectives of the business and all its activity.

Identify the range of hazards, threats, or perils that impact or might impact:

- Your organisation.
- Your infrastructure.
- The surrounding area.

You will need to:

- **Identify retrospective risks** - Retrospective risks are seen in incidents or accidents that have occurred in the past. Retrospective risk identification is the most common way to identify risk and the easiest. A risk is easier to understand if its impact has already been experienced. It is also easier to quantify its impact and to evaluate the damage. There are many sources of information about retrospective risk including:

- hazard or incident logs or audit reports
- customer complaints
- accreditation documents and reports
- staff or client surveys
- newspapers or professional media, such as journals and websites.

- **Identify prospective risk** - Prospective risks are harder to identify. These are things that have not yet happened but might happen in the future. Identification should cover all risks, whether or not they are currently managed. The plan will be to record all significant risks and monitor the effectiveness of their treatment. Methods for identifying prospective risks include:

  - brainstorming with staff and external stakeholders
  - researching the economic, political, legislative and operating environment
  - interviewing staff and clients to identify potential problems
  - flow charting a process
  - reviewing system design or preparing system analysis.

Risk categories will help break down the process for prospective risk identification. It is important to remember that risk identification will be limited by the experience and perspective of those conducting the risk analysis. Problem areas and risks can be best identified by the use of reliable sources.

In addition, understanding categories assists business owners to select the best tools and techniques for risk identification and analysis. For example, if a particular risk category is technical in nature, the risk identification methodology used will involve significant research and collection of existing information about risk exposure.

Analyse the risks

During risk identification, a business owner may have identified many risks but it is often not possible to address all of them.

Determine the potential impact of each hazard, threat, or peril by estimating the:

- relative severity of each hazard, threat, or peril (danger).
- relative frequency of each hazard, threat, or peril.

- vulnerability to each hazard, threat, or peril of your people, your operations, your property, and your environment.

Risk analysis will determine which risks have a greater consequence. This will provide better understanding of the possible impact of a risk, and the likelihood of it occurring. That leads to decisions about resources required to control the risks.

Risk analysis involves combining the possible consequences, or impacts, of an event, with the likelihood of that event occurring. The result is called a 'level of risk'. ***Risk = consequence x likelihood.***

The risk analysis should be documented in the risk management plan.

Evaluate the risks

It is important to determine how serious the risks facing a business are. The business owner must determine the level of risk that a business is willing to accept. Risk evaluation involves comparing the level of risk found in the analysis process with previously established risk criteria. From there it must be decided if these risks require treatment.

Categorize each hazard, threat, or peril according to how severe it is, how frequently it occurs, and how vulnerable you are.

The result of a risk evaluation is a prioritised list of risks that require further action. This step is about deciding whether risks are acceptable or need treatment.

Low or tolerable risks may be accepted. 'Accepted' means the business chooses to accept that the risk exists, either because the risk is low and the cost of treating it would be uneconomic, or there is no reasonable treatment that can be implemented.

A risk may be accepted if:

- the cost of treatment exceeds the benefit, so that acceptance is the only option (applies particularly to low risks)
- the level of the risk is so low that specific treatment is not called for
- the opportunities presented outweigh the threat to such a degree that taking the risk is justified

- there is no treatment for the risk – for example, the risk that the business may suffer storm damage.

If the risk is medium or high and therefore not acceptable, the risk must be mitigated or treated. Specific actions to treat the risk should be outlined in the risk management plan.

Treat the risks

Risk treatment is about options for dealing with risks that are *not* acceptable. Risk treatment involves identifying controls for risk. The aim is to either reduce or eliminate negative consequences, or to reduce the likelihood of an adverse occurrence. Risk treatment should also enhance positive outcomes.

It is often not possible, nor cost-effective to implement all treatment strategies. A business owner should choose, prioritise and implement the best combination of risk treatments.

Develop strategies to deal with the most significant hazards, threats, or perils. Develop strategies (risk treatments) to:

- prevent,
- mitigate,
- prepare for,
- respond to, and
- recover from hazards, threats, or perils that impact or might impact your organisation and its people, operations, property.
- The steps to this are:
- identify – develop and design treatment options
- evaluate – do the options satisfy treatment objectives and are they cost effective?
- develop and implement a risk treatments and controls.
- For businesses, many of the treatments are often part of establishing everyday business practices and procedures such as:

- staff training and development
- financial reporting systems
- good customer management
- ensuring compliance.

Therefore, ensuring good management practices are already in place will help you control risks from the outset.

A quality assurance program can also help to control risk. Quality assurance is the process that continues from risk treatment through monitoring and review to a cycle of continuous improvement.

All risk treatments should be documented in your risk management plan.

Monitor and review the risks

Monitoring is an essential step in the risk management process. A business owner/manager must monitor risks and review the effectiveness of treatments and strategies that have been set up to manage risk.

Risks need to be monitored regularly to ensure changing circumstances do not alter risk priorities. Very few risks are static, therefore the risk management process needs to be repeated often, so that new risks are captured into the process and can be effectively managed

A risk management plan should be reviewed at least annually. The best way to make sure this occurs is to combine the review with annual business planning.

TYPES OF RISK

Upside risk

An upside risk is something that might happen that's better than some benchmark level. The benchmark is something we choose, but typically it is our planned or expected outcome, or the outcome we think 'ought' to happen.

In some areas of risk management, the upside is more important than in others. In safety, for example, the natural benchmark is 'total safety' (one does not want to speculate about how many people one 'expected' or 'planned' to kill or injure.) Consequently, there is no upside to speak of.

By contrast, in financial risk management it is natural to talk about expected returns and there's nearly always an important upside to consider.

Positive risk

Refers to risk that we initiate ourselves because we see a potential opportunity, along with a potential for failure. We must be intelligent risk takers. For example, we have a project that is scheduled to take 90 days to complete.

The client would rather the project be delivered earlier and would get more value if it were delivered earlier but understands that 90 days is how long the project will take. One of your team members has an idea: If you utilise a new machine, it's possible that you can deliver the project in 60 days instead of 90. If this were a guaranteed solution, you would jump on it. However, there is risk, since it will be the first time you've used the machine.

You must deal with a lack of expertise and a learning curve. It's possible that if the machine doesn't work out, the project could end up taking 110 days to deliver. What would you do?

Downside risk

The risk that an asset will decline in value including the implications of risk, e.g., a "worst case" scenario of the gradation of risk in which an investor will lose money in a business venture if the venture fails.

Negative risk

is represented by potential events that could harm a project. In general, these risks are to be avoided, e.g., you have a supplier that you're counting on to provide raw materials to build a prototype. The supplier has a union contract that expires in the next 60 days. There is a risk that the supplier will have a strike that will disrupt shipments. You need to identify this as a risk, estimate the probability of occurrence (perhaps this will increase or decrease over time), determine the impact to the build if it occurs, and then put together a plan to minimise the impact on the project if it occurs

Example:

The implications of meeting and exceeding or not meeting quality requirements are also referred to as upside and downside risk.

- Upside risk is the potential gain for both the individual and the company if standards are met and exceeded.

- Downside risk is the potential loss both the individual and the organisation may suffer if quality standards are not met.

The following examples will help you gain a better understanding of the upside and downside risks of the outputs of a job:

Scenario	Effects for Judy	Effects for the company
Judy is able to answer 10 calls a day more than her colleagues due to her efficiency and because she knows her products well	**Upside risk:** Judy could get better performance reviews than her peers, resulting in increased responsibilities and possible benefits, pay and perhaps promotion (if this is available for the company) **Downside risk:** Judy's supervisor may begin giving Judy more work because she knows Judy will do it better than other staff that don't perform so well – Judy may become overloaded. This is known as performance punishment i.e. good performers get more work and the poor performers don't. A supervisor can manage the situation by exploring reasons for non-performance and taking steps to correct the gaps.	**Upside Risk:** Increased productivity – good reputation for efficient service **Downside Risk:** Judy may feel that she is being taken advantage of and may leave the company or become demotivated – this will affect her productivity
A client asks Judy for a refund that is owing to her. The client needs the refund by close of	**Upside Risk:** The client is impressed with Judy's service and advises her supervisor – Judy is recognised for her customer service. Judy feels good because the client is very thankful and desperately needed the money.	**Upside Risk:** The client tells other people about the service & this leads to increased business.

business today. To assist the client Judy decides to drop the cheque off at the client's home on the way home from work as she sees it is on route.	**Downside Risk:** Judy does not know the client and could put herself at risk by going to a stranger's house. If anything happened to Judy on the way to the client and at the client, after working hours, the company may not compensate her because it is not part of her job to personally drop off cheques at clients' houses.	**Downside Risk:** If anything happened to Judy – the company may be liable to compensate because Judy was acting in the best interest of the client

When outputs are produced according to quality requirements the employee, company and customers benefit. The business stays profitable and attracts more customers.

When outputs are not produced according to quality requirements a lot of time is wasted fixing up errors, re-doing work which ultimately costs money and could even result in the business having to close down, customers being dissatisfied, employees being dismissed for poor ratings, etc. There is always a price to pay for not doing the job correctly.

CATEGORIES OF RISK

There are many examples of risk in business. To identify your specific business risks, consider them in categories.

The link between RISK and LOSS is obvious - and it has produced during the past 50 years a group of specialised activities all devoted to reducing loss. Ironically - though each "**petal of the RISK flower**" attempts to minimise corporate loss. Further, they are unaccountable for the resources management invests in them. Not one of them can provide "*dollars saved per dollar invested*."

Categories of Risk

Risk categories should be considered one by one, providing a structured approach to risk identification. This enables greater focus on a particular category, stimulating thought, and increasing the opportunity of identifying a broader range of risks.

Common risk categories are:

- **Financial –** includes cash flow, budgetary requirements, tax obligations, creditor and debtor management, remuneration and other general account management concerns.
- **Equipment –** extends to equipment used to conduct the business and includes everyday use, maintenance, depreciation, theft, safety and upgrades.
- **Organisational –** relates to the internal requirements of a business, extending to the cultural, structural and human resources of the business.
- **Security –** includes the business premises, assets and people. Also extends to security of company information, intellectual property, and technology.
- **Legal and regulatory compliance –** includes legislation, regulations, standards, codes of practice and contractual requirements. Also extends to compliance with additional 'rules' such as policies, procedures or expectations, which may be set by contracts, customers or the social environment.

- **Reputation –** entails the threat to the reputation of the business due to the conduct of the entity, the viability of products/services, or the conduct of employees or others associated with the business.

- **Operational –** covers the planning, daily operational activities, resources (including people) and support required within a business that results in the successful development and delivery of products/services.

- **Contractual –** meeting obligations required in a contract including delivery, product/service quality, guarantees/warranties, insurance and other statutory requirements, non-performance.

- **Service delivery –** relates to the delivery of services, including the quality of service provided, or the way a product is delivered. Includes customer interaction and after-sales service.

- **Commercial –** includes risks associated with market placement, business growth, product development, diversification and commercial success. Also, to the commercial viability of products/services, extending through establishment, retention, growth of a customer base and return.

- **Project –** includes the management of equipment, finances, resources, technology, timeframes and people involved in the management of projects. Extends to internal operational projects, business development and external projects such as those undertaken for clients.

- **Safety –** including everyone associated with the business: individual, workplace and public safety. Also applies to the safety of products/services delivered by the business.

- **Workplace safety -** Every business has a duty of care underpinned by State and Federal legislation. This means that all reasonable steps must be taken to protect the health and safety of everyone at the workplace. Occupational health and safety is integrated with the overall risk management strategy to ensure that risks and hazards are always identified and reported. Measures must also be taken to reduce exposure to the risks as far as possible.

- **Stakeholder management –** includes identifying, establishing and maintaining the right relationships with both internal and external stakeholders.

- **Client-customer relationship –** potential loss of clients due to internal and external factors.

- **Strategic –** includes the planning, scoping, resourcing and growth of the business.
- **Technology –** includes the implementation, management, maintenance and upgrades associated with technology. Extends to recognising critical IT infrastructure and loss of a particular service/function for an extended period of time. It further takes into account the need and cost benefit associated with technology as part of a business development strategy.

Knowing your risk categories can assist you in risk planning and communicating risk information. They provide a structure for identifying risk and are often initially identified through a brainstorming exercise.

Factors that could Constitute Risks to a Unit

The risks facing an organisation and its operations can result from factors both external and internal to the organisation. The risks can be categorised into types of risk such as strategic, financial, operational, hazard, etc.

EXAMPLE

Financial risks are typically well controlled and are part of the routine focus of management risk discussions, with strong impetus coming from the increased regulatory, accounting, and financial audit focus. As financial information is a key element of stakeholder communications, performance measurement and strategic delivery, management risk discussions will devote considerable time to these risks.

Financial risk is often defined as the unexpected variability or volatility of returns and includes both potential worse than expected as well as better than expected returns. We know that organisations require a steady stream of reliable income in order to operate and grow

Operational risks are typically managed from within the business and often focus on health and safety issues where industry regulations and standards require. These internally driven risks may affect your organisation's ability to deliver on its strategic objectives.

Hazard risks often stem from major exogenous factors, which affect the environment in which the organisation operates. A focus on the use of insurance and appropriate contingency planning will help address some of these. However, there is often a danger that as many of these risks cannot be controlled, boards and senior management will not reflect these in their strategic thinking. Confining strategic management to controllable factors will leave your business at risk of failing to address these factors.

Strategic risks are typically external or affect the most senior management decisions. As such, they are often missed from many risk registers. Your senior management has a responsibility to make sure all these types of risks are included in their key strategic discussions.

Asset Risk

Some organisations prefer to look at factors related to asset when identifying factors that could constitute risks to a unit.

We can categorise asset risk according to four major categories of assets:

- **Property risk** – Property includes:
    - Buildings
    - Office furniture and fixtures
    - Computers (hardware and software)
    - Intellectual property (trademark, logo, copyright, patent, etc.)
    - Motor vehicles
    - Other equipment (lawn maintenance equipment, contractors' equipment, audio-visual equipment, laptops, exhibits, etc.)

Property also includes cash and securities, financial assets and even borrowed property. Property risks come in various forms, including those caused by nature (flood, earthquake, hurricane, forest fires, wind/tornadoes, extreme heat or cold) and others resulting from human intervention (fire, theft, vandalism, collision, carelessness). The risks of loss associated with property and income assets could devastate an organisation. Imagine what would happen if your organisation's computers and accounting records were lost in a fire, or if a significant sum of money were embezzled.

- **Income risk** – Depending on the type of organisation, common sources of income include:
    - Donations
    - Grants
    - Government contracts
    - Fees for services
    - Investment income
    - Merchandise sales
    - Loans
    - Proceeds from special events
    - Sponsorship fees
    - Registration/ participation fees
    - Membership dues

Most managers have come face to face with an income risk, such as the loss of budget, sales falling shy of projections, contract cancellations and more. A disaster such as a fire or flood can also curtail operations, resulting in an interruption of the income stream. Consequences of a loss can range from inconvenience to devastation. While income ups and downs are arguably part and parcel of the business world, it's possible to use risk management techniques to reduce the likelihood that a loss of income will destroy an organisation.

- Goodwill risk - Goodwill is an asset that is difficult, if not impossible, to quantify. A more descriptive word might be "reputation." Every organisation understands that its reputation is key to recruitment of staff and customers, retention of those staff and customers, and overall good organisational health. Damage to reputation can be devastating, and many organisations would

have a hard time recovering from a blow to their reputation. In many cases, damage to reputation occurs in the wake of a crisis, such as a scandal involving maladministration or widely publicised client injury. In some cases, there may be guilt by association if a corporate partner comes under fire. Even an incident of tax evasion by a major shareholder could have repercussions for an organisation

Some techniques for reducing income risk include:

1. Business interruption insurance
2. Establishing a reserve fund
3. Implementing sound financial controls
4. Diversifying income sources

- Operational risk - Operational risk is defined as the risk of loss resulting from inadequate or failed internal processes, people, and systems, or from external events.

Examples of operational risk include:

- Technology failure
- Business premises becoming unavailable
- Inadequate document retention or record-keeping
- Poor management
- Lack of supervision
- Lack of accountability
- Poor control
- Errors in financial models and reports
- Attempts to conceal losses
- Attempts to make personal gains

- Third party fraud

A delict is an act (or omission) which in a wrongful and culpable way causes loss to another - responsibility toward society at large. This is where potential losses are most difficult to estimate. You may have heard of the Thalidomide disaster. In the 1960's a drug meant to relieve morning-sickness in pregnancy resulted in babies being born deformed. It is thought that a similar disaster under today's conditions could result in awards as high as R5bn. (This is an example of Products Liability).

A boiler explosion might cause tremendous physical damage, and interrupt production, but the liability claims for physical injury and damage to third party property can be even bigger.

An organisation can suffer loss even without legal liability being established:

- The cost of investigation and documenting their defence.
- Legal fees.
- Out of court settlements, where it is considered more cost effective to settle with the claimant, than risk everything on the outcome of an expensive court action.
- Where disputes go to court, legal costs are much greater, as are the actual awards handed down.

People risk - People are the heart and soul of an organisation. They represent the talent, commitment, and community your organisation serves. The people assets in your organisation include staff, clients, and shareholders.

Examples of people risk include:

Risk of Staff Loss: Each person is a unique individual with a unique set of skills. In a very real sense, each is irreplaceable. So, the first risk in terms of employees is the risk of loss of talent/ expertise when a trained and skilled employee leaves the organisation.

Health and safety: Another risk is that of loss due to injury or death. Unlike damage to property or loss of income, injuries sustained by employees may never be fully repaired and could lead to expensive litigation. In the workplace, an organisation's priority must be the health and safety of all. The goal is the prevention of occupational health risks, accidents, and injury.

This means that all must work to legal health and safety standards and improve on these wherever possible. All employees must constantly be on the alert against possible hazards and hazardous behaviour. The organisation must minimise such hazards with well-designed procedures, processes, equipment and safety training programmes. The organisation must ensure that all employees are aware that irresponsible or careless activities place themselves and others at risk.

Employee turnover: In terms of **employee decision-making**, Andrew Wong says it is natural for an employee to **aspire** to earn a better salary. **Financial gain** not only helps to meet the financial needs and improve the lifestyle of the person and his/her family, but it may also reflect greater capability of the employee to take up greater scope of work or responsibilities.

An opportunity may arise whereby there is a significant financial gain (e.g., higher salary, or allowances or both), but with higher occupational hazards, or perhaps s/he has an opportunity to work in a foreign country which has security risks or entails harsh living conditions for the employee and the family.

Of course, each person has his or her own tolerance level with respect to the above-mentioned risks. Rationally and emotionally, he or she will make decisions based on certain criteria, making the necessary evaluation and assessment.

The general rationale is “suffer a few years for that extra significant financial gain” and this then becomes the governing principle or reason to make the decision to take up a new job or transferred position. However, in the scenario described by Wong, there is also a significant risk to the organisation: if the employee perceives the payoff to be “not worth it” after a while and cannot handle the increased workload or strain, s/he can become demotivated and unproductive, even though it was his/her own choice.

That is why organisations have **Wellness or Employee Assistance Programmes (EAP)** in order identify, interact with, and refer troubled employees before they affect productivity and team morale.

At Risk Behaviour: As a manager, you will be held accountable for your subordinates’ behaviour – good or bad. You can take a proactive approach to eliminating at risk behaviour by recognising its causes in the workplace. The possible sources of at-risk behaviour are endless and will vary on its degree of severity and the impact it will have on the performance of your team. Some sources of at risk behaviour could relate to the following:

Ignorance - Ignorance could create at risk behaviour when your subordinates don't know all they should about a situation. As a result, they might not be able to recognise, diagnose, or fix a dilemma. You should make sure that your subordinates are educated about your company and its current activities, goals, vision, values policies, and procedures. By training your employees on these issues you could pro-actively avoid future high-risk situations.

Lack of recognition by management - Recognition by management is an important form of reward for an employee. If a manager does not recognise an employee who needs recognition, the employee can become frustrated and might change his/her behaviour patterns to gain the manager's attention.

Although this attention could be negative, the employee would rather be recognised this way than not at all, e.g., an employee might start coming in late regularly or fail to submit reports or start to verbally abuse others, simply to get attention. This could in the long-term impact negatively on conduct, productivity, performance, and capacity.

Personal financial burdens - When an employee does not earn enough money to cover personal expenses, he might become a high risk, especially if he/she works with money. In this instance at risk behaviour can have two objectives: to take revenge on the organisation, or to obtain enough money to cover their personal expenses.

As a manager, you might have the authority to determine salary levels for your subordinates. It is unrealistic for managers to grant subordinates all the salary they might want. Yet it is realistic to pay employees a salary based on industry standards. If your organisation's salary levels fall below such standards, you can expect to encounter at risk behaviour.

Substance Abuse - This includes drugs and alcohol and has, in recent years become a serious social and business problem. The substance abuser poses a major threat to an organisation in terms of productivity, performance, and conduct. The condition is often not apparent but manifests itself with poor performance issues, absenteeism, and financial burdens.

Environmental and Corporate Social Responsibility: Outside of the workplace, an organisation's priority must be to act responsibly by protecting the environment and the communities around it. In addition, organisations must ensure that they act responsibly at all times in the disposal of waste and in pollution control.

RISK CONTINGENCIES

There are many cases of relatively small property losses resulting in prolonged stoppages of production. That is why contingency planning is so important.

Contingency planning is a kind of back-up, or safety net, to the risk management process.

DECIDING ON PREVENTIVE ACTION

Having evaluated the risks, the next step is to put in place preventive and protective measures. Among the things to be considered at this stage are:

1. Whether risks are preventable or avoidable. Is it possible to get rid of the risk? This can be done, for instance, by:
   - Considering whether the task or job is necessary,
   - Removing the hazard,
   - Using different substances or work processes.

2. If risks are not avoidable or preventable, how risks could be reduced to a level at which the health and safety of those exposed is not compromised. When determining a strategy to reduce and control risks, employers should be made aware of the following additional general principles of prevention:

   - Combating the risk at source
   - Adapting the work to the individual, especially as regards the design of work places, the choice of work equipment and the choice of working and production methods, with a view, in particular, to alleviating monotonous work and work at a predetermined work-rate and to reducing their effect on health
   - Adapting to technical progress
   - Substituting the dangerous by the non-dangerous or the less dangerous (replacing the machine or material or other feature that introduces the hazard by an alternative)
   - Developing a coherent overall prevention policy which covers technology, organisation of work, working conditions, social relationships and the influence of factors related to the working environment

- Giving collective protective measures priority over individual protective measures (e.g., Controlling exposure to fumes through local exhaust ventilation rather than personal respirators)
- Giving appropriate instruction to workers.

For guidance on the control of risk through these measures employers should be referred to specifications, in national legislation, national standards, published guidance and other such criteria, published by national authorities.

A further important general principle of which employers need to be aware is that they should not transfer risks. That is to say that in providing a solution to one problem, another problem should not be created. For instance, it would be of doubtful benefit to provide double-glazing to office windows to reduce noise from outside, unless provision was made for adequate ventilation.

CONTINGENCY STRATEGIES FOR MANAGING RISK

Once risks have been identified and assessed, all techniques to manage the risk fall into one or more of these four major categories:

- **Avoidance**
- **Reduction / Mitigation / Modification**
- **Acceptance / Retention**
- **Sharing / Transfer**

Ideal use of these strategies may not be possible. Some of them may involve trade-offs that are not acceptable to the organisation or person making the risk management decisions.

- **Avoidance**

  Avoidance includes not performing an activity that could carry risk. An example would be not buying a property or business in order to not take on the liability that comes with it. Another would be not flying in order to not take the risk that the aeroplane could be hijacked.

  Avoidance may seem the answer to all risks, but avoiding risks also means losing out on the potential gain that accepting (retaining) the risk may have allowed. Not entering a business to avoid the risk of loss also avoids the possibility of earning the profits.

Whenever an organisation cannot offer a service while simultaneously ensuring a high degree of safety, it should choose avoidance as a risk management technique.

Do not offer programs/ services/ products that pose too great a risk. In some cases, avoidance is the most appropriate technique if an organisation simply doesn't have the financial resources required to fund adequate training, supervision, equipment, or other safety measures. Always ask, "Is there something we could do to deliver this program/conduct this activity safely?" If you answer "yes," risk modification may be the more practical technique.

- **Reduction/ Mitigation/ Modification**

  Modification involves methods that reduce the severity of the loss. Examples include sprinklers designed to put out a fire to reduce the risk of loss by fire. This method may cause a greater loss by water damage and therefore may not be suitable. Alternative fire suppression systems may mitigate that risk, but the cost may be prohibitive as a strategy.

  Modification is simply changing an activity to make it safer for all involved.

  Policies and procedures are examples of risk modification. An organisation concerned about the risk of using unsafe drivers may add licence checks to its screening process, or an annual road test for all drivers.

- **Acceptance / Retention**

  Retention involves accepting the loss when it occurs. True self-insurance falls in this category. Risk retention is a viable strategy for small risks where the cost of insuring against the risk would be greater over time than the total losses sustained.

  All risks that are not avoided or transferred are retained by default. This includes risks that are so large or catastrophic that they either cannot be insured against, or the premiums would be prohibitive. War is an example since most property and risks are not insured against war, so the loss attributed by war is retained by the insured.

  Also, any amounts of potential loss (risk) **over** the amount insured is retained risk. This may also be acceptable if the chance of a very large loss is small or if the cost to insure for greater coverage is so great it would hinder the goals of the organisation too much.

There are two ways to retain risk. The first is by design. Organisations make conscious decisions to retain risk every day. For example, when an organisation purchases liability insurance and elects a certain excess amount, it's retaining risk. This can be a rational and appropriate approach to managing risk.

Where organisations get into trouble is when risk is retained unintentionally. The unintentional retention of risk can be the result of failing to understand the exclusions of an insurance policy, insufficient understanding of the scope of risk the organisation faces, or simply because no one has taken the time to consider the risk and how it can be addressed.

- **Sharing / Transfer**

  Sharing or risk transfer means causing another party to accept the risk, typically by contract or by hedging.

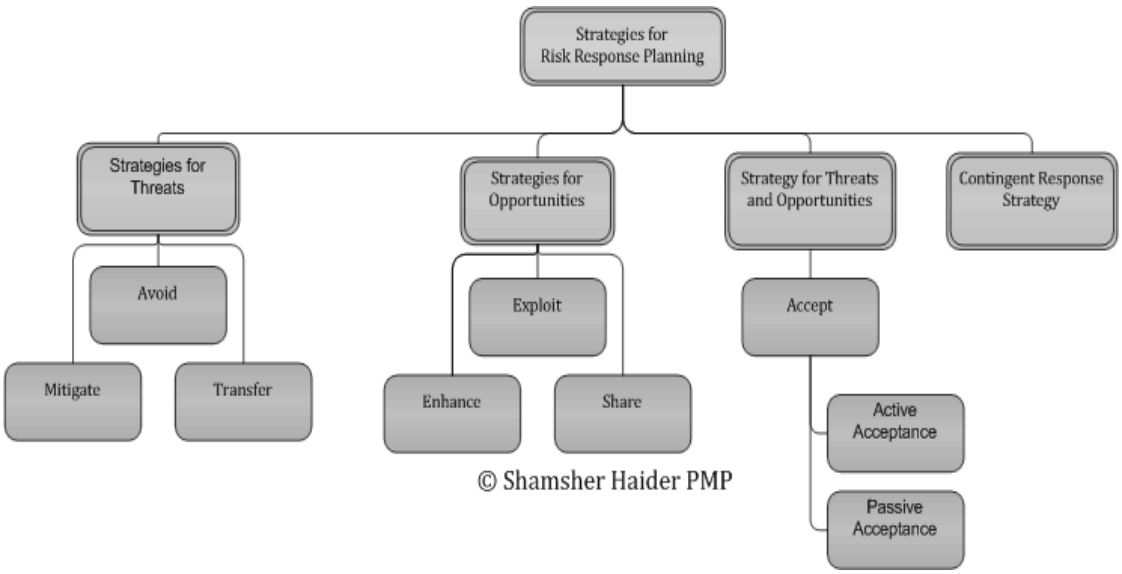
  Risk sharing can therefore involve sharing risk with another organisation through a contract.

  Two common examples are insurance contracts that require an insurer to pay for claims expenses and losses under certain circumstances, and service contracts whereby a provider (such as a transportation service or caterer) agrees to perform a service and assume liability for potential harm occurring in the delivery of the service.

  Risk retention pools are another way of retaining risk for a group. Unlike traditional insurance no premium is exchanged between members of the group up front, but instead losses are assessed to all members of the group.

APPLYING CONTINGENCIES

Shamsher Haider, a PMI certified project management professional (PMP) suggests the following on the ERPM BlogSpot:



STRATEGIES FOR THREATS

Avoid: This means staying clear of the risk altogether. While avoidance obviously is the best possible course, it might not be feasible in all circumstances, e.g. the impact of the cost of avoidance might dominate the benefits of avoiding the risk. Avoidance can be accomplished by changing the process or the resources to attain an objective or sometimes modifying the objective itself to avoid the risks involved. An example of avoiding risk could be avoiding use of untested third-party components in the software design or avoiding inclusion of an inexperienced resource in the project team.

Mitigate: This means trying to reduce the probability and/or impact of the risk. Reduction in probability of occurrence would reduce the likelihood of its occurrence and reduction in impact would imply a lesser loss if the risk event occurred. 100% mitigation would be equivalent to avoidance. An example of mitigation would be an early verification of the requirements by prototyping before moving on to full-fledged development.

Transfer: This implies transferring the liability of risk to a third party. While this strategy does not eliminate or mitigate the risk or its consequences itself, it transfers the responsibility of its management to someone else. Insurance is a classic example of this strategy. By buying insurance you transfer your risk to the insurance company by paying the risk premium. Fixed Cost contract is yet another example of risk transfer strategy. In a fixed cost contract, the risk is transferred to the seller.

STRATEGIES FOR OPPORTUNITIES

Exploit: This strategy involves removing all uncertainties pertaining to a positive risk and making sure that the risk event occurs.

An example could be a situation where the seller will pay an incentive fee if work is completed a week ahead of the completion deadline. Ordinarily there is a probability that the work might get completed earlier, but if we plan to exploit this situation, we will plan to complete the work a week ahead to turn this uncertainty into a certain event.

Enhance: This strategy involves planning for increasing the size of the opportunity by increasing its impact and /or the probability of its occurrence. Identification of the root cause of the presence of an opportunity can help focus on the root cause and enhance its impact and / or probability.

Share: This strategy involves sharing the fruits of an opportunity with a third party because you do not have the capability to exploit it alone.

Suppose your competitor is set to launch a new product six months from now, and you identify the opportunity that by launching a product with similar features a month before your competitor's launch you can wrest the market away.

In this scenario the situation becomes complicated because you have all the resources to launch your product in five months except a portion requiring device driver and hardware level programming. You can launch a joint venture with another company specializing in device driver programming to share the opportunity.

STRATEGY FOR THREATS AND OPPORTUNITIES

Accept: Sometimes we identify a risk but realize that time and / or resources required to formulate and enact response strategies overweigh the results of the effort. In such a case we just accept the risk. If we plan to face the occurrence as it is, it is called passive acceptance. On the other hand if we develop a contingency reserve to handle the situation if the risk occurs, we call it active acceptance.

CONTINGENT RESPONSE STRATEGY

Also known as ***contingency planning***, this strategy involves development of alternatives to deal with the situation after the risk has occurred.

Active acceptance of risks leads to contingency planning, whereby we anticipate a risk to occur and instead of trying to mitigate or eliminate its occurrence we plan what to do when the event occurs.

Contingency reserves are a commonly used tool to handle the occurrence of a risk event. Contingency reserve can imply allocation of cash, time, or resources to cope with the situation when the risk event has occurred.

Fallback plans can be developed for high impact risks. A fallback plan as the name suggests, is the backup plan, in case the original contingency plan doesn't work out as planned.

An example could be identification of risk that a certain .Net programmer will resign in middle of the project. Since under the current circumstances you can do nothing to mitigate or eliminate the risk you accept it but develop a contingency plan to hire a certain programmer on hourly wages.

To cope with the situation if no programmer is available on hourly wages at the time of resignation of your programmer, you develop a fall-back plan of temporarily moving a software engineer from a certain low priority project to work on the assignment till an alternative can be hired.

DEVELOP CONTINGENCY PLANS

After the most appropriate preventive and protective measures have been identified, the next step is to put them in place effectively.

Effective implementation involves the development of a plan specifying:

- The measures to be implemented
- The means allocated (time, expenses etc.)
- Who does what and when?
- When actions are to be completed?
- A date for reviewing the control measures.

It is important to involve workers and their representatives in the process:

- To inform them about the measures implemented, about how they will be implemented, and who will the person in charge of implementing them
- To train or instruct them about the measures or procedures that will be implemented.

In preparing a contingency plan to deal with the interruptions to the organisation's business, the first steps should be to identify:

- All potential sources of loss-producing events which may disrupt operations.
- Interdependences between different parts of the organisation itself; for example, would damage to one process or storage area disrupt all production of one or more of a firm's products?
- Dependencies upon individual suppliers or customers.
- Alternative sources of supply or outlets where any of the above dependencies exist.
- All seasonal factors.

Steps to develop the Contingency Plan

Step 1: Risk Management Planning - The manager and the team decide who is going to develop the risk management plan

Step 2: Risk Identification - The assigned team identify the various risks and make a list of the risks through brainstorming, interviewing and sample risk lists.

Step 3: Risk Probability - The risk management plan team, determine the probability of the risks occurring through Impact Scales.

Step 4: Risk Response Plan - The risk management plan team decides for each identified risk whether to accept the risk, avoid the risk or accept the risk.

Step 5: Risk Monitoring and Control - Risk monitoring and control is a process that lasts the entirety of the project. The team monitors the risks as the project matures, new risks develop, and anticipated risks disappear.

The contingency plan should specify the responses to each of the different types of loss situations, setting out the steps to be followed under various circumstances and assigning responsibilities for various tasks:

1. List every business process in the department. (Example: Payroll might be listed in the Human Resource's plan.)
2. List the tasks for every business process and the steps it takes to complete these tasks.
3. For every step, list every dependency (computer hardware, software, external and internal suppliers.)
4. Rate the likelihood for each dependency to fail (Prioritise! Usually a 1-High, 2-Medium or 3-Low works well. Alphabetising with H, M or L usually doesn't work as well, because these three letters - alphabetically - don't follow your priority. Remember this when you design your database!)
5. Assume that every dependency will fail, beginning with 1-High dependencies. Write a contingency action that accomplishes the task without relying upon the dependency.

Once you have analysed business functions this way, you will be able to create contingencies at the appropriate places. In many areas, the contingency will be at the task level; in other areas at the process level; still others may be at the department level.

In some cases, no viable contingency is possible. If power goes down, and you have no generator, you aren't doing any business. If this is the situation with any specific process, make a note of it and describe what you'll do if the dependency fails.

Structure your contingency plan positively - involve the appropriate people and the right amount of people - it's a big task, after all. It will require input from many.

Ongoing Training

Any disaster and crisis management plans must be tested regularly and updated where shortcomings are found so that the plans are not only kept as up to date as possible, but also so that the personnel involved have been trained.

Crisis Situations

It must be realised that having a plan, even if it is kept up-to-date and even if people have been fully trained in what to do, will not necessarily result in your being able to cope with the crisis when it occurs. It is essential for those who are drafting or amending the plan to bear in mind that:

- The more severe the crisis is, the greater the loss of or lack of resources.
- The plan will not work without people to make it come alive.
- The effects of stress on both people and the plan will be unpredictable. The plan as a consequence will work in unpredictable ways.

Communicate Contingency Plans to Relevant Stakeholders

Key to the success of the risk management process is communication and consultation with key staff. Staff members will assist in the identification process, as well as treating and monitoring the risks. They will have a part in putting together the risk management plan and can be assigned to oversee certain risks that may impact on their area of the business.

Wide consultation will help ensure that most risks are identified, helping to lessen the potential of things going wrong.

The human factor is rarely absent from risk situations. Frequently carelessness, incompetence or lack of technical knowledge is either the primary or at least a contributory cause of a loss-producing event. Furthermore, the failure of an individual or group to respond in the correct way to a loss situation may contribute to the size of the ensuing loss.

Consequently, training and effective communication have a major role to play in loss reduction programmes and should cover everyone employed by, or associated with the work of an organisation.

Management

The aim should be to create in management an awareness of the risks to which the organisation is exposed and of the ways in which they may be controlled.

The lead in risk control, and therefore loss control, must come from top management, and, although only a few members of the top management team will need to have a detailed technical knowledge of the various risks and hazards, all should understand and have a commitment to the principle of total risk control.

Risk control is essential at every stage of an organisation's activities such as:

- At the planning stage.
- At the production stage.
- After sales usage and service.

Staff

There are several fundamental points to bear in mind when communicating the contingency plans to employees:

- They need to be aware of the hazards to which they may be exposed in the course of their work and what steps they can take to minimise the risk of injury to themselves and fellow employees.

- Training may be required regarding the use of special clothing and equipment provided for their safety.
- Instructions for all employees as to what to do in emergencies, for example, upon the outbreak of fire, breakdown of plant, and especially the breakdown of safety devices.
- Training of some employees to deal with emergencies until expert help arrives, for example the training of first aid and firefighting teams;
- Installing a sense of safety-consciousness in all employees, both in relation to the way they carry out their work and in the avoidance of defects in the firm's products. Each employee should feel a sense of responsibility towards fellow-employees, customers, and the general public.

Contractors, Suppliers and Servicing Agents

Sometimes the organisation can be jeopardised by people other than its own employees:

- Contractors and sub-contractors who undertake work on its behalf.
- Suppliers of components and raw materials.

All these people should be made aware of the risks that affect the organisation, and their cooperation sought. For example, is it fair to blame a welder who accidentally starts a fire, if the area where he is working was not first cleared of flammable materials?

Expensive mechanical failures and products recall have resulted from minor impurities in lubricants and raw materials.

Risk Reporting and Communication

Internal Reporting

Different levels within an organisation need different information from the risk management process. The Board of Directors should:

- Know about the most significant risks facing the organisation.
- Know the possible effects on shareholder value of deviations to expected performance ranges.
- Ensure appropriate levels of awareness throughout the organisation.
- Know how the organisation will manage a crisis.

- Know the importance of stakeholder confidence in the organisation.
- Know how to manage communications with the investment community where applicable.
- Be assured that the risk management process is working effectively.
- Publish a clear risk management policy covering risk management philosophy and responsibilities.

Business Units should:

- Be aware of risks which fall into their area of responsibility, the possible impacts these may have on other areas and the consequences other areas may have on them.
- Have performance indicators which allow them to monitor the key business and financial activities, progress towards objectives and identify developments which require intervention (e.g. Forecasts and budgets).
- Have systems which communicate variances in budgets and forecasts at appropriate frequency to allow action to be taken.
- Report systematically and promptly to senior management any perceived new risks or failures of existing control measures.

Individuals should:

- Understand their accountability for individual risks.
- Understand how they can enable continuous improvement of risk management response.
- Understand that risk management and risk awareness are a key part of the organisation's culture.
- Report systematically and promptly to senior management any perceived new risks or failures of existing control measures.

External Reporting

A company needs to report to its stakeholders on a regular basis setting out its risk management policies and the effectiveness in achieving its objectives.

Increasingly stakeholders look to organisations to provide evidence of effective management of the organisation's non-financial performance in such areas as community affairs, human rights, employment practices, health and safety and the environment.

Good corporate governance requires that companies adopt a methodical approach to risk management which:

- Protects the interests of their stakeholders.
- Ensures that the board of directors discharges its duties to direct strategy, build value and monitor performance of the organisation.
- Ensures that management controls are in place and are performing adequately.

The arrangements for the formal reporting of risk management should be clearly stated and be available to the stakeholders.

The formal reporting should address:

- The control methods – particularly management responsibilities for risk management.
- The processes used to identify risks and how they are addressed by the risk management systems.
- The primary control systems in place to manage significant risks.
- The monitoring and review system in place.

Any significant deficiencies uncovered by the system, or in the system itself, should be reported together with the steps taken to deal with them.

Distribute and Store Contingency Plans

Your contingency plans must be distributed and stored in accordance with the organisation's risk management procedures.

Some recommendations are:

- Formally review and update the plan at least quarterly.
- Review contingencies within the plan, such as storage of a specific set of records, and update the contingencies on a regular schedule. The frequency of updating will vary with the degree the material changes over time and the degree of risk the firm accepts if the data is outdated.

- Store disks or tapes of critical information such as accounts receivable, client information, vendor and personnel records or outstanding billings in a safe, secure place such as a bank vault.
- Duplicate prepared information and place in a three-ring binder to facilitate adding and deleting materials over time.
- Maintain duplicate records at a different site
- Individuals with key responsibilities should keep copies of the emergency plan at their homes

TEST AND REVISE CONTINGENCY PLANS

After you have prepared the contingency plan, you need to do several things to keep it practical and relevant - don't just create a document and file it away. As your business and its environment change, you'll need to review and update these plans accordingly.

Here are some key steps in the contingency plan maintenance process:

- Communicate the plan to everyone in the organisation.
- Inform people of their roles and responsibilities related to the plan.
- Provide necessary training for people to fulfil these roles and responsibilities.
- Conduct disaster drills where practical.
- Assess the results of training and drills and make any necessary changes.
- Review the plan on a regular basis, especially if there are relevant technological, operational, and personnel changes.
- Distribute revised plans throughout the company, and make sure the old plan is discarded.
- Audit the plan periodically:
    - Reassess the risks to the business.
    - Analyse efforts to control risk by comparing actual performance to the performance level described in the contingency plan.
    - Recommend and make changes, if necessary.

Test Contingency Plans

Testing *every* contingency in your plan is time- and cost-prohibitive. To make testing manageable, test in four stages. Each stage should build on the results of the previous stage. If an area proves to be unsound, or if it conflicts with other contingency plans, you can re-write and re-test the plan.

Stage 1 - Senior Staff Review

The senior staff select an internally publicised date and time to review all contingency plans. Aside from ensuring overall business soundness, this review also serves to recognise people who have thoughtfully completed their assignment. Knowledge of a firm date for a senior staff review will increase quality, accuracy, and timeliness.

Stage 2 - Interdepartmental Reviews

Each department should review another department's plans. The goal of this stage is to find bottlenecks, identify conflicts and allocate resources. If possible, departments that are "downstream" in the business process can review the plans of "upstream" departments.

Stage 3 - Failures in Critical Systems

This testing can be localised within departments. It involves simulating system or vendor failures. You don't actually have to shut down critical equipment or processes - you can role-play a "what if" scenario. You can either run a "surprise" drill or plan a role-playing event for a specific time.

Stage 4 - The Real Deal

This testing involves short-term shutdowns in key areas. If possible, these tests should be conducted in a real-time environment. The goal, of course, is to fully test the contingency plan. Concentrate this last phase of testing only on areas that have a high business priority and a high risk for failure.

By implementing testing in four stages, you can optimise your time and accomplish the goal of proving that the contingency plan is valid.

Monitoring and reviewing

Arrangements for monitoring and reviewing the protective and preventive measures should be introduced following the risk assessment to ensure that the effectiveness of these measures is maintained, and the risks controlled.

The information generated by monitoring activities should be used to inform the review and revision of the risk assessment.

Risk assessment should not be a once-and-for-all activity. The assessment needs to be reviewed and revised, as necessary, for a number of reasons, including:

- The degree of change likely in the work activity
- Changes which might alter the perception of risk in the workplace, such as a new process, new equipment, or materials, change of work organisation, and new work situations including new workshops or other premises
- Once the new measures have been introduced following the assessment, the new working conditions should be assessed to review the consequences of the change. It is essential that the risk is not transferred, that in providing a solution to one problem, another problem should not be created
- The assessment no longer being applicable because the data or information on which it is based is no longer valid
- The preventive and protective measures currently in place being insufficient or no longer adequate, e.g. Because new information is available regarding control measures
- As a result of the findings of an accident or "near miss" (a near miss is an unplanned event that did not result in injury, illness, or damage - but had the potential to do so).

Document Recommendations on Improvements to Contingency Plans

Copies of the contingency plan and all revisions need to be submitted to those staff members that are expected to respond to the different situations identified in the plan.

The contingency plan should be reviewed at least annually and updated whenever changes occur that will significantly affect the ability of your unit to respond to an emergency.

This includes when the regulations are revised, if your unit's contingency plan fails in an emergency, if your unit changes in a way that materially increases the potential for an emergency or there are changes in the response necessary in an emergency, if the list of emergency coordinators changes or if the list of emergency equipment changes.

These revisions should be made to the plan immediately (within 24 hours).

It is recommended that a revision record be kept that includes amendment dates, revision numbers and a brief summary of the nature of the revision(s). It is also acceptable to make contingency plan changes in supporting documentation as long as this documentation is referenced in the original plan.

Capture lessons learned on the effectiveness of risk reduction measures.

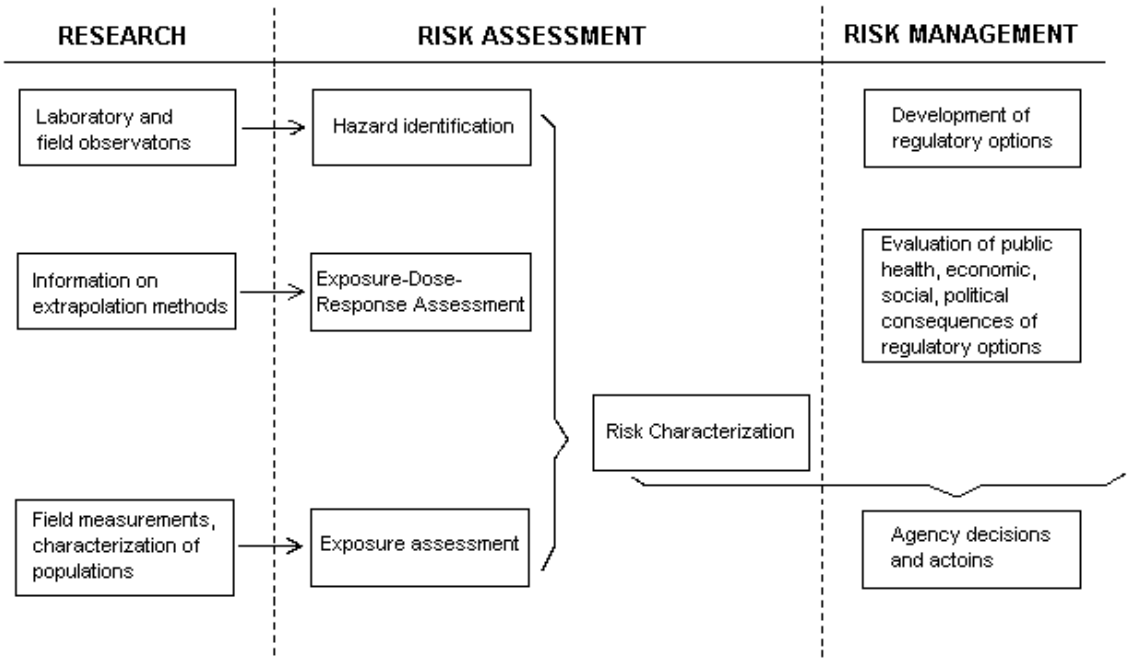
As plans are executed, they must be monitored to ensure that their objectives are achieved as intended. It should be recognised that, in a high-risk environment, the one thing that can be expected is that not everything will happen according to plan. What is important is that an understanding of what needs to be done develops during the planning and monitoring processes.

Check that the risk indicators are not being exceeded, and that reduction efforts are effective. At regular periods, the progress should be checked against the plan to ensure that:

- Risks identified earlier are still valid, and the risk indicators have not changed.
- Any changes of risk significance are understood and communicated to those who need to know.
- Implemented responses have been effective and lessons learned are captured.
- The risk reduction measures can be considered a success (or if they are failing then identify new measures that need to be put into place).
- Residual risks are acceptable or are subject to continuing action on the plan; in this event the monitoring must continue.
- No other risks have materialised over time.

Discover the reason(s) for change in the risk status. It is, of course, possible that the risk reduction measures are not working as well as had been expected, and thus corrective action is required. If the corrective action required is significant in terms of cost and time, especially if it involves several risks (a highly likely situation), a new risk analysis may be required.

Risk management is not a complex task. If you follow the steps in this Learner Guide, you can put together a risk management plan for your unit in a short space of time.



From: National Academy of Sciences / national Research council Paradigm for Research / Risk Assessment / Risk Management (NAS/NRC, 1983)

"Although we cannot foretell the future, we need to plan for it. Plan for things that could go wrong, and for things that could go exceptionally right."

Brock Henderson