Risk Management

Motivations

- When we looked at **project selection** we just took into account financial data
- In the **scope management** document we emphasized the importance of making our goals achievable, i.e. the A in SMART ... however between achievable and achieved there is a big difference.
- In the **planning phase** we had to deal with various uncertainties (estimation) and tried to deal with them generically (e.g. time buffers)
- We stuck to one plan (the nominal plan), but the world is non-nominal: changes, both negative and positive, will occur!

Risk Management

Risk management collects techniques, know-how and processes to help identify, assess, manage, and monitor risks

The objectives of Project Risk Management are to increase the probability and the impact of positive events and decrease the probability and impact of events adverse to the project.

Risk Management: Some Goals

- Understanding whether a project is worth taking
- Help refining the budget for the project
- Increase chances of ending the project successfully
- Increase chances of terminating the project as planned:
  - Within scope
  - Within quality
  - Within budget
  - On time

Risk Management: Two Definitions

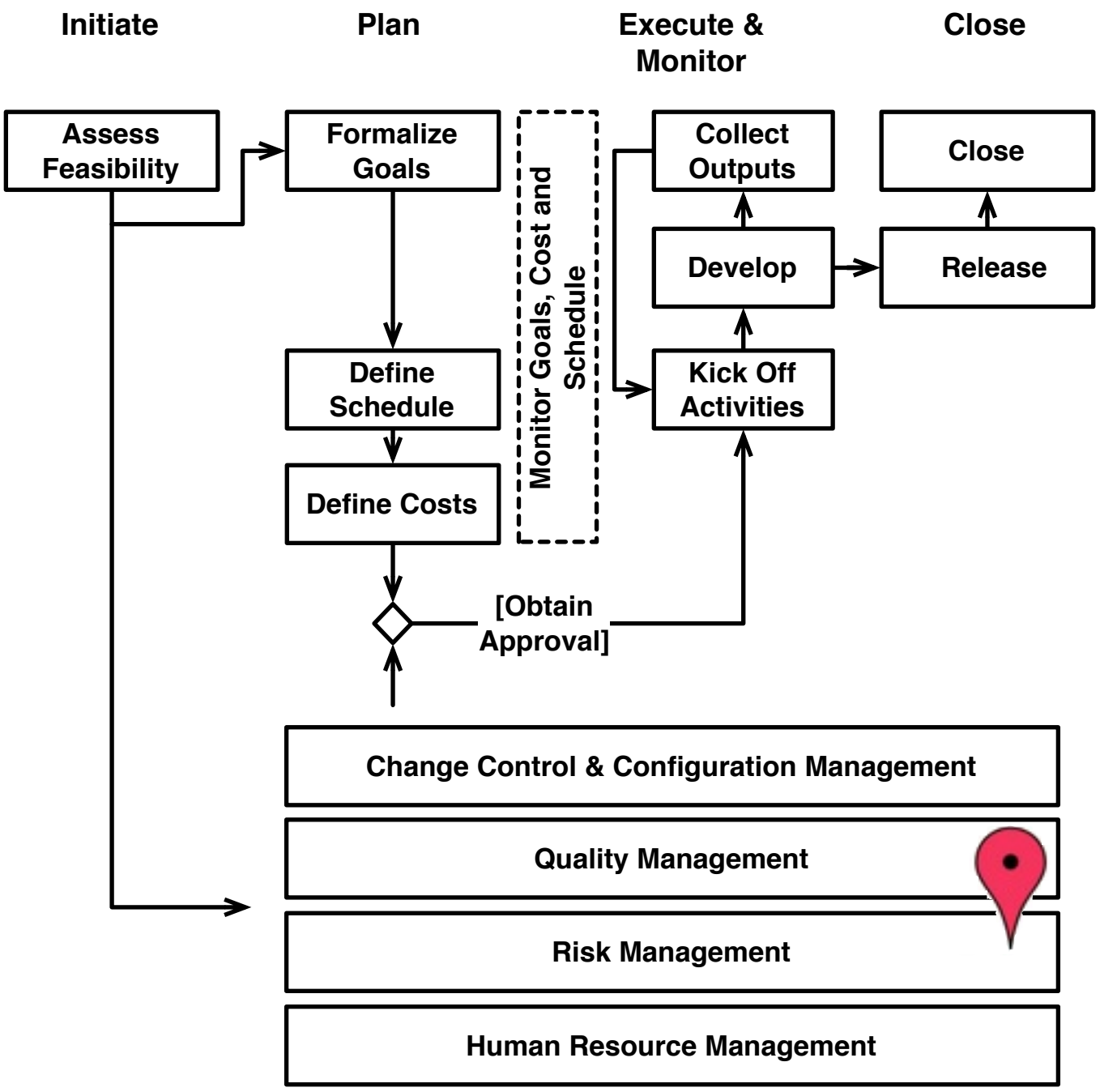
- "Traditionally":
  - **Risk** is the possibility of suffering loss
- In project management:
  - **(Project) Risk** is an event or condition that, if it occurs has positive or negative influence on an objective
    * Negative outcome: menace
    * Positive outcome: opportunity

Risk Management

- Used in several fields, such as:
  - Finance
  - Insurance
  - Engineering (safety critical, security, …)
- Various standards recognize the importance of risk in software development:
  - **ISO/IEC 12207** (Information Technology - Software life cycle processes)
  - **UNI EN 29000-3** (Guidelines for the application of ISO 9001 to software development and maintenance)
  - **UNI ISO 10006** (Guidelines for managing projects)
- Various techniques (FMEA, FTA, simulation, …) have been defined and adopted to assess it.

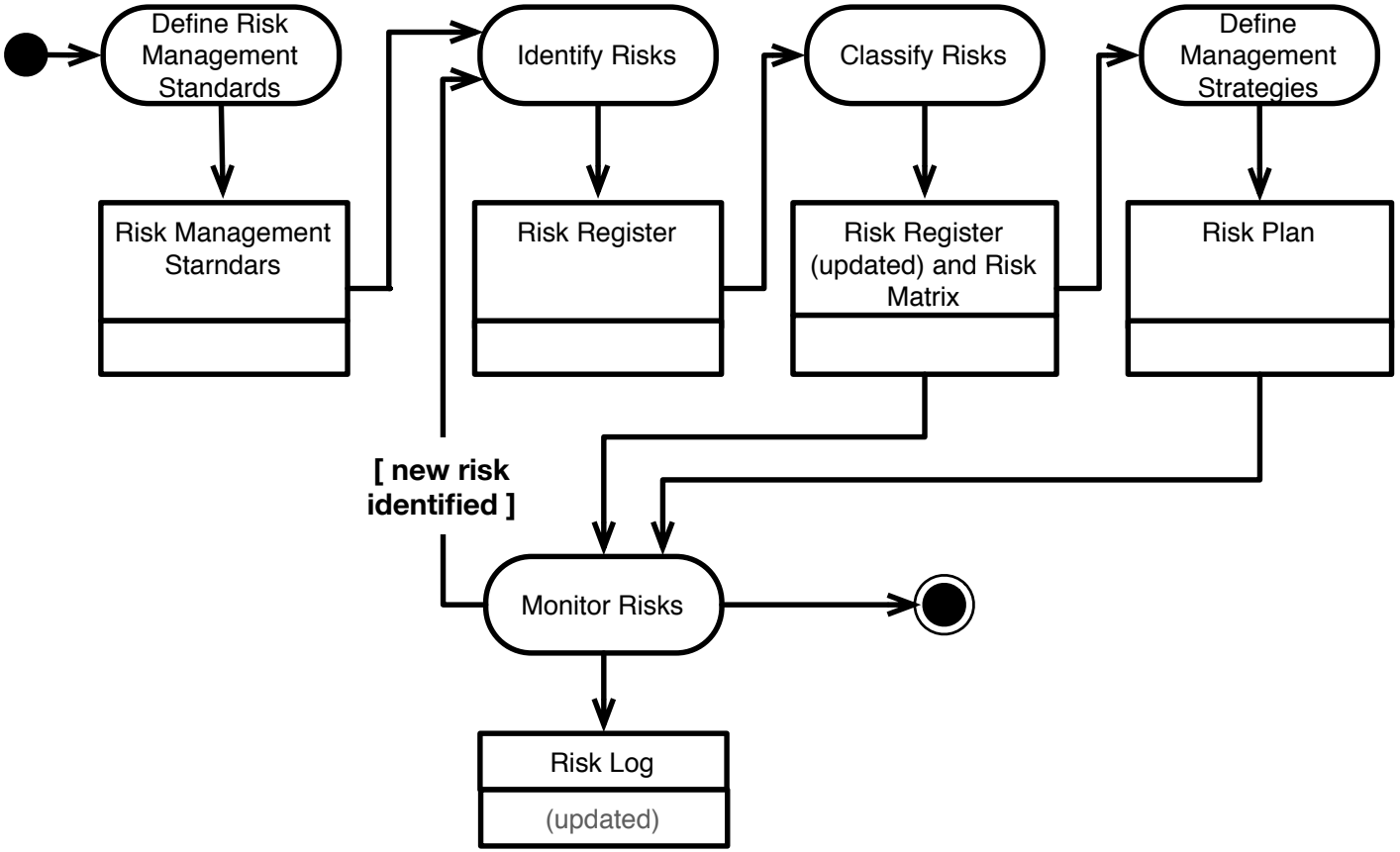
Goals of the Unit

- Learning the techniques to identify, assess, prioritize, manage and control project risks
- Learning what are the most common risks in software development projects
- Learning how to budget for project risks


Initiate
Plan
Execute & Monitor
Close
Assess Feasibility
Formalize Goals
Monitor Goals, Cost and Schedule
Collect Outputs
Close
Develop
Release
Define Schedule
Kick Off Activities
Define Costs
[Obtain Approval]
Change Control & Configuration Management
Quality Management
Risk Management
Human Resource Management

Risk Management and Project Management

The Risk Management Process



- It runs in parallel to the other PM activities throughout the project

Defining Risk Management Standards

Goal: describing how risk management will be structured and performed on the project.

- Output: a document (or set of documents and templates)
- Part of the project management plan
- Helps define project standards and best practices

Define Risk Management Standards

- The document includes, at a minimum:
  - The procedures to monitor and update risks
  - The procedures to apply contingency plans
  - Who is in charge of what
- Added value:
  - Definition of risk probabilities and impacts
  - Risk Categories or other sources to identify risks
  - Reporting formats
- A risk management plan could be standardized and adopted organization-wide
- Different projects require different levels of formality in risk management

Risk Identification

Goal: understanding what are the risk that could potentially influence the project and document their characteristics

- Risk identification is an iterative process (new risks may be identified as the project progresses; old risks may become “obsolete”)
- Output: Risk Register, basis for qualitative/quantitative risk analysis

Risk Identification and Classification

- Process (iterative):
  - Collect:
    * identify specific project risks
    * describe the risk
  - Analyze:
    * Identify the root causes (do not misinterpret effects as causes)
    * Define the risk category (impact) and probability
    * Identify other useful characteristics:
      - When it can occur or frequency of occurrence
      - How it manifests
- Output:
  - Risk Register

Risk Identification Techniques

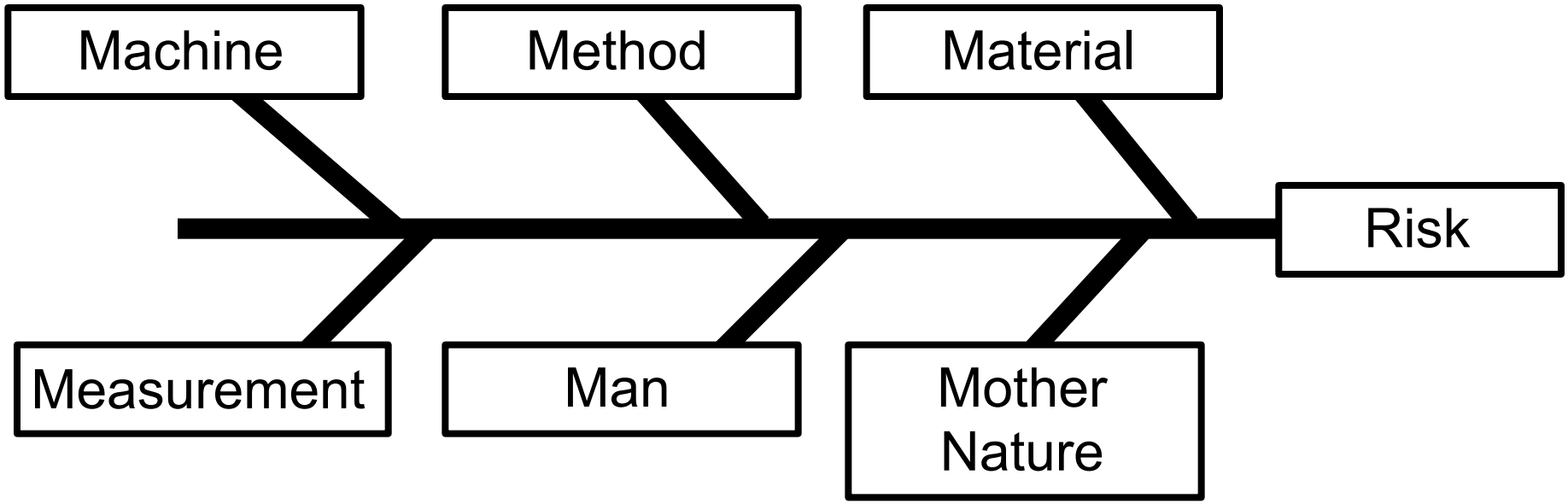
- Meetings
- Document Analysis
- Risk Breakdown Structures, Checklists, Templates
- Analogy

Boehm's Top Ten Causes for Project Failures

- Boehm developed a list of the ten most common causes for projects to fail
- Some of the causes mentioned in the list can be used as starting point to identify the risks applicable to a project at hand
- Risks include:
  - Personnel or subcontractors Shortfall
  - Unrealistic schedule and budget
  - Developing the wrong software functions/user interface
  - Gold plating (getting priorities wrong)
  - Ineffective change control
  - Technical risks

Root Cause Analysis Techniques

- Cause-Effect Diagram (Ishikawa)
- Fault Trees/Failure Modes and Effect Analysis



Fishbone Diagrams: Some starting points

- **The 6 M's:**
  - Machine, Method, Materials, Measurement, Man and Mother Nature (Environment)
    (recommended for manufacturing industry).
- **The 8 P's:**
  - Price, Promotion, People, Processes, Place / Plant, Policies, Procedures & Product (or Service)
    (recommended for administration and service industry).
- **The 4 S's:**
  - Surroundings, Suppliers, Systems, Skills
    (recommended for service industry).

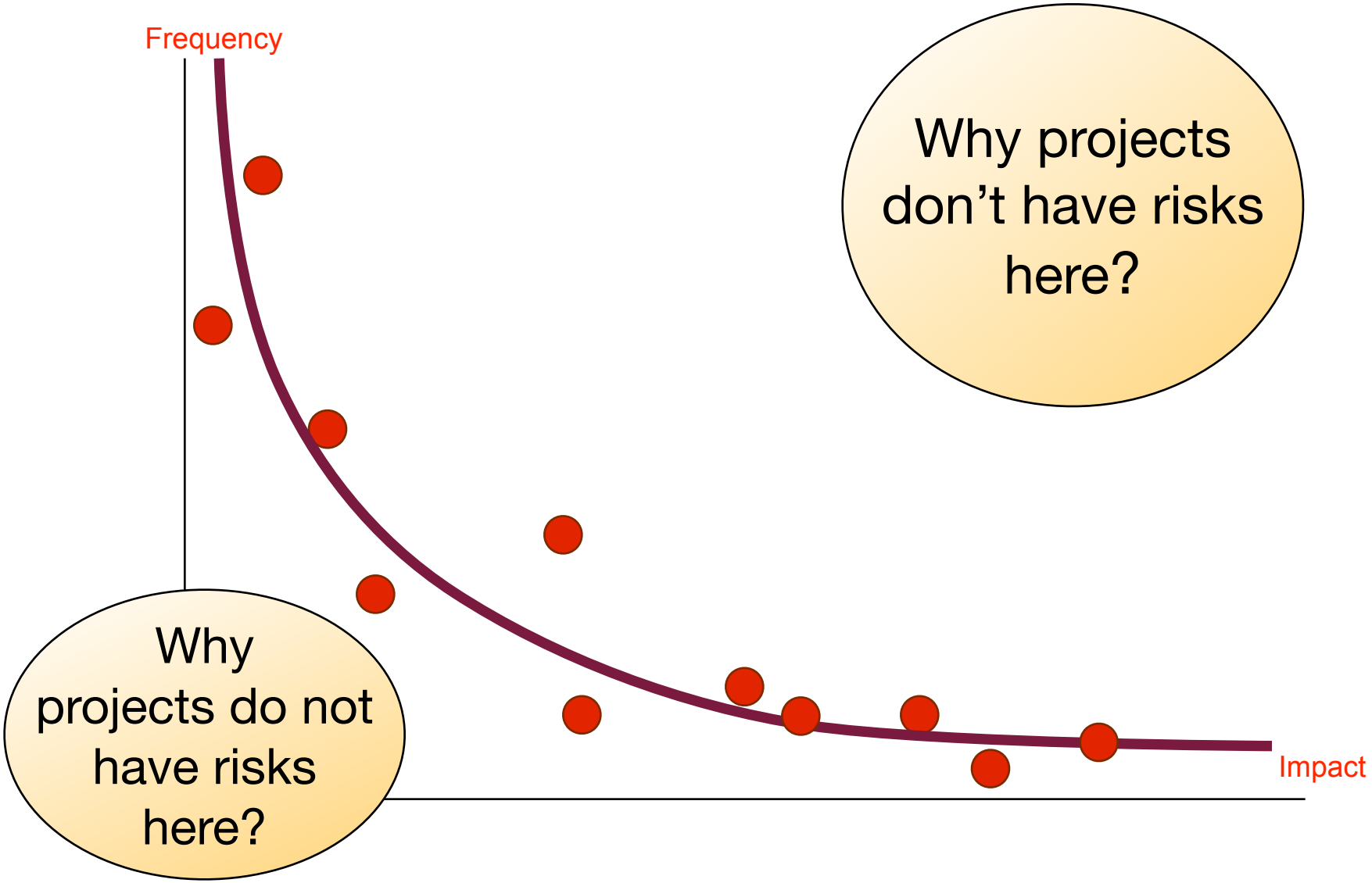
Risk Assessment and Risk Management Strategies

Risk Assessment

Goal: prioritize risks according to their impact and likeness on the project

- Output: a prioritized list of risks (priority defined according to probability and impact)
- Information on whether a project is worth taking
- Information about what risks must be monitored

Probability/Impact



Techniques

- **Qualitative risk analysis**
  - Simpler
  - Can be used when no precise information about probabilities of risk is available
- **Quantitative risk analysis**
  - More systematic
  - Suitable for mathematical analysis
  - Provide figures on the (economical) impact of risks

Qualitative Risk Analysis

Qualitative Risk Analysis

- **Start from**
  - Risks Management Standard which define the scales to be adopted for probability and impact
  - The outputs of the risk identification phase (during which we assigned a probability to each risk)
- **Highlight most significant risks:**
  - By organizing risks into a risk matrix
  - By scoring risks
- **Output:**
  - Assess whether the project is worthwhile.
  - Decide what risks must be monitored

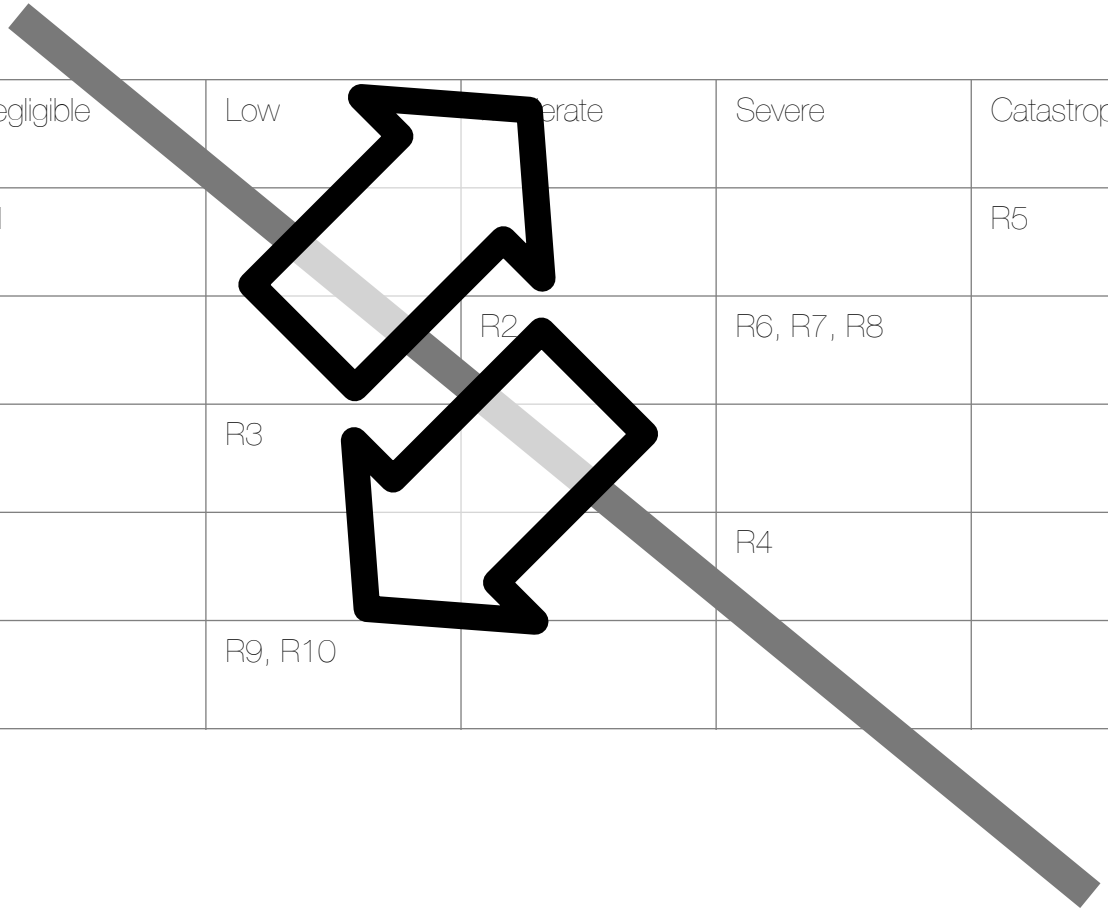
Risk Matrix

	Negligible	Low	Moderate	Severe	Catastrophic
Very High	R1				R5
High			R2	R6, R7, R8	
Moderate		R3			
Low				R4	
Very Low		R9, R10			

Risk Matrix

- Decide where to set the “bar”...

	Negligible	Low	erate	Severe	Catastrophic
Very High	R1				R5
High			R2	R6, R7, R8	
Moderate		R3			
Low				R4	
Very Low		R9, R10			



Risk Matrix

- RED: Require special treatment (or drop the project)
- ORANGE: Need close monitoring
- GREEN: LOW: Standard in a project... nuisances

	Negligible	Low	Moderate	Severe	Catastrophic
Very High	R1				R5
High			R2	R6, R7, R8	
Moderate		R3			
Low				R4	
Very Low		R9, R10			

Risk Scoring

- Define classes of probabilities and classes of qualitative or numeric classes of impact
- Example
  - Probability: very low, low, moderate, high, very high
  - Impact: negligible, low, moderate, severe, catastrophic
  - Risk Score: **low, medium, high** (see previous slide) or numeric: **SCORE = P x I**

Very Low	0.1	1	Negligible	0.1	1
Low	0.3	2	Low	0.3	2
Moderate	0.5	3	Moderate	0.5	3
High	0.7	4	Severe	0.7	4
Very High	0.9	5	Catastrophic	0.9	5

Socially constructed risk

- Two problems with qualitative risk
  - **Modelers:** we are “risk illiterate”
    (we believe some things are riskier than others, sometimes even when statistics tell us otherwise)
  - **Models:** who says what the probabilities are? How do we calculate the risk exposures objectively?
    (projects are one-offs)

Examples of risks: Causes of Death

- Heart disease: 597,689
- Cancer: 574,743
- Chronic lower respiratory diseases: 138,080
- Stroke (cerebrovascular diseases): 129,476
- Accidents (unintentional injuries): 120,859
- Alzheimer's disease: 83,494
- Diabetes: 69,071
- Nephritis, nephrotic syndrome, and nephrosis: 50,476
- Influenza and Pneumonia: 50,097
- Intentional self-harm (suicide): 38,364

Source: http://www.cdc.gov/nchs/fastats/lcod.htm
(2011 data)

Risk Management Strategies

a.k.a. Risk Response Planning: how do we take care and exploit risks

Risk Management Strategy

Goal: find a treatment for the unacceptable risks and decide the strategies to apply for the remaining risks, should they occur during the project

- Output: a plan with only acceptable risks
- A contingency plan for each remaining significant risk

The Scenario

- RED: Require special treatment (or drop the project)
- ORANGE: Need close monitoring
- GREEN: LOW: Standard in a project... nuisances

	Negligible	Low	Moderate	Severe	Catastrophic
Very High	R1				R5
High			R2	R6, R7, R8	
Moderate		R3			
Low				R4	
Very Low		R9, R10			

Strategies: Menaces

- **Avoid**
  - Change the plan to eliminate the threat (increase time, relax objectives, take corrective actions - increase time to do requirements)
- **Transfer**
  - Shift the negative outcome to a third party. It transfers responsibility, it does not eliminate the risk (insurance, contracts to transfer liability… they require to pay you a price)
- **Mitigate**
  - Reduce probability or impact (often better than trying and repair the damage; prototyping)

Strategies: Opportunities

- **Exploit**
  - Eliminate uncertainty relate to the occurrence of the opportunity (e.g. assign more talented people, provide better quality)
- **Share**
  - Allocate responsibility of exploitation to a third party (joint-ventures, partnerships, …)
- **Enhance**
  - Modify the size of an opportunity by increasing probability and/or positive impact

Strategy: common

- ***Accept***
  - **Passive:** just let the team deal with the risks
  - **Active:** provide some buffer (time, money, …)

Why?

... Low impact or probability

... Simpler to deal with the risk, if it occurs than planning a response in advance

Risk Response Planning: Outputs

- **Risk Response Plan:**
  - **Strategy (strategies) for dealing with the risks: must be concrete!**
  - **Triggers** (elements used to monitor and understand whether a risk has occurred)
  - **People** responsible of monitoring the risk
  - **People** responsible of applying contingency plans

The Risk Register

- The most common tool to list and manage risks is a spreadsheet
- One row per risk
- Each risk characterized by:
  - ID, Title, Description
  - Risk Category (if you are inclined to classifications)
  - Probability, Impact and, possibly, Score (PxI)
  - Root cause
  - Time-frame
  - Monitoring modalities (periodicity, person, reporting)
  - Status (active, occurred, inactive)

Risk Monitoring and Control

a.k.a. Risk Response Planning: how do we take care and exploit risks

Risk Monitoring and Control

- Input:
  - The risk register
- Process
  - Analyze deviations from the nominal plan
  - Identify causes
  - Evaluate corrective actions
  - Modify current plan
- Mind:
  - Planned risks must be dealt with as above (use contingency plans)
  - Unplanned risks require the full process!

Conclusions
and
The main risks of …
Risk Management!

Some Common Errors

- **During the Planning Phase:**
  - **Not identifying a maximum risk value**
    - Give up a project if too risky
  - **Not writing a balanced risk management plan**
    - Size and complexity have to be at the right level for the project
  - **Misinterpreting effects as causes**
    - You end up caring for the wrong event and not looking at the actual problem
    - Example 1: We might be late with the project
    - Example 2: We may be charged 100.000 euros as a penalty

Some Common Errors

- **During Risk Monitoring:**
  - **Risk homeostasis:** we tend to increase our risk-taking
  - **Anchors and frames:** we tend to stick to anchor and frames overlooking opportunities or the need to change course.
    An example is **sticking to past decisions** (as an anchoring mechanism)
  - **Sunk costs**: an incorrect economical assumption
    ("I have spent so much… it is more convenient to keep going!")
  - **Cognitive dissonance**: we do not like inconsistencies; our brain creates consistent theories, sometimes altering (or not considering) all facts.
    ("I know smoking is bad … but (another) cig won't hurt me")

Some Common Errors

- **During Risk Monitoring:**
  - **Do not apply contingency plans**
    * Dealing with risk when they occur is more error-prone than think about the strategies before they occur
  - **Do not involve actors**
    * Make sure stakeholders understand consequences of the risk (share the risk)
    * involve stakeholders in dealing with them
  - **Do not update the plan**
    * Helps keeping the contingency plans really applicable