Risk Management

SE423: Software Project Management

Outline

- Risk Management Process
- Risk Identification
- Risk Analysis
- Risk Planning
- Risk Monitoring
- Strategies and Techniques

Risk Management Process

What is a Risk?

- According to the PMBOK Guide (7th edition):
  - “Project **risk** is an uncertain event or condition that, if it occurs, has a positive or negative effect on one or more project objectives. Negative risks are called **threats** and positive risks are called **opportunities**”
  - “A risk may have one or more causes, and, if it occurs, one or more impacts”

- Project Risks
  - What can happen?
  - What is the likelihood?
  - What will the damage/benefit be?
  - What can we do about it?
- Usually, engineers focus on analyzing worst-case scenarios only.

What is a Risk?

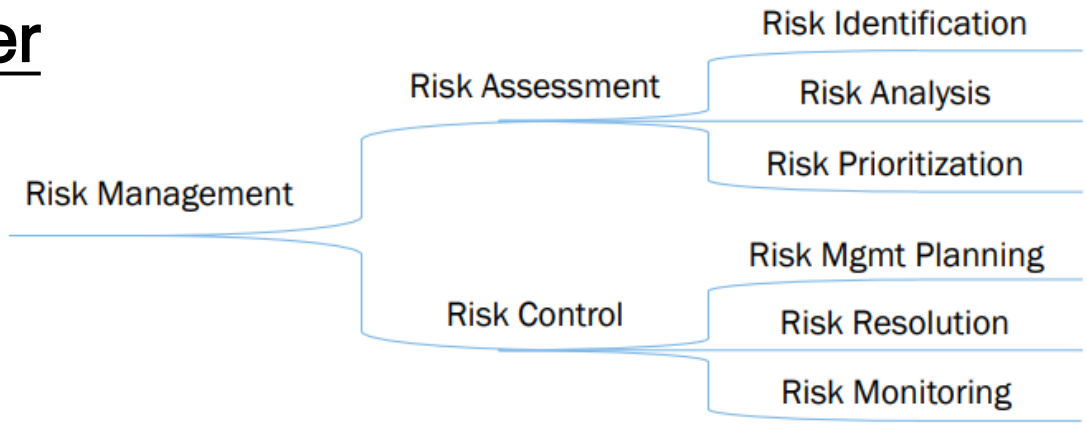
- Events that haven't happened yet
- Characterized by:
  - Uncertainty (0 < probability < 1)
  - An associated loss/gain (financial, human safety, reputation, etc)
  - Manageable: may be controlled/used in different ways
- Needs to be actively identified and managed
  - Some choose to ignore negative risks: fearing they will be seen as too negative people
- Is a key element in project decision making – especially important for the tough decisions
- Proactive vs. Reactive: being proactive reduces problems effects (maximizes benefits)
- Active Risk Management is a sign of a well-run project and a mature organization

Negative Risks (Threats) Classification

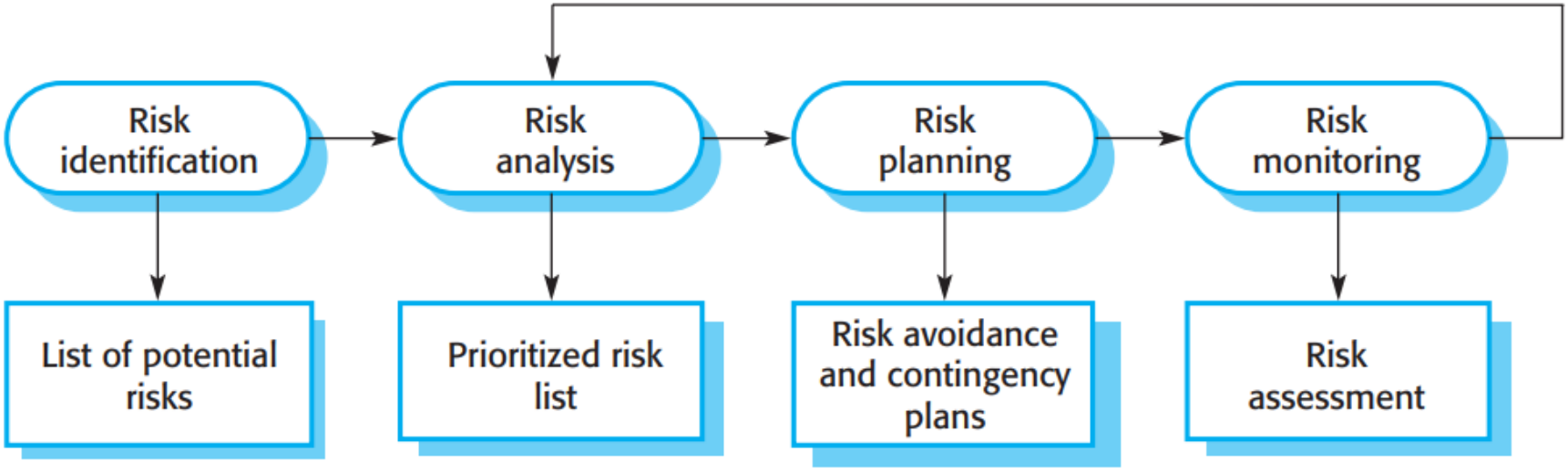
- Requirements Risks
  - Incorrect: Requirements don't reflect actual user needs.
  - Incomplete: Missing functionality or edge cases.
  - Unclear or inconsistent: Ambiguities or contradictions across stakeholders.
  - Volatile: Frequent changes that disrupt planning and development.
- Cost Risks
  - Unreasonable budgets: Underestimating the true cost of delivery (time, talent, or tools)
- Schedule Risks
  - Schedule compression (customer pressure, marketing launches, etc.)
- Quality Risks
- Life Cycle / Operational Risks: poor handoffs (transfer of responsibility: team to team, phase to phase, internal to external, turnover induced), lack of documentation, ignoring maintenance

Risk Management Process

- Risk management is a systematic approach to reducing the harm due to threats and maximizing the benefits due to opportunities, making a project less vulnerable to challenge or failure and its resulting product more robust, and preparing it to make better use of opportunities.
- Understanding the hierarchy of Risk Management = Understanding risks and how to deal with them.
- **We will focus in this chapter on threats management.**



Risk (threats only) management process



Reality check for your project plan

- Testing the plan before you begin
- Assessing the project using risk management (ensures the plan is resilient), not optimistic)
- Involving the team in planning (plans made in isolation often miss operational realities)
- Building confidence for your plan
- Selling the plan to relevant stakeholders: it is not only about approval, but also about advocacy (مناصرة)

Risk (Threat) Identification

What can Possibly Go Wrong?

Consider the “average” project:

- Testing takes longer than planned – cannot resolve bugs
- Vendor cannot deliver a product on schedule
- Critical engineer
  - Has accident
  - Becomes a parent (many family emergencies)
  - Has major surgery
- Critical engineer leaves project/company
- Change of ownership. Project on hold
- Major downsizing
- Dysfunctional staff
- Natural disasters, internet and power failures

Risk Identification: Introduction

- *Risk identification* is concerned with determining what risks might have an impact on the project
- In addition, risk identification seeks to profile risks so that effective mitigation and response planning might be possible
- Risk identification is an iterative and incremental process that continually adds new risks, deletes non-risks, and refines existing risk profiles as the project progresses

How to Categorize Risk

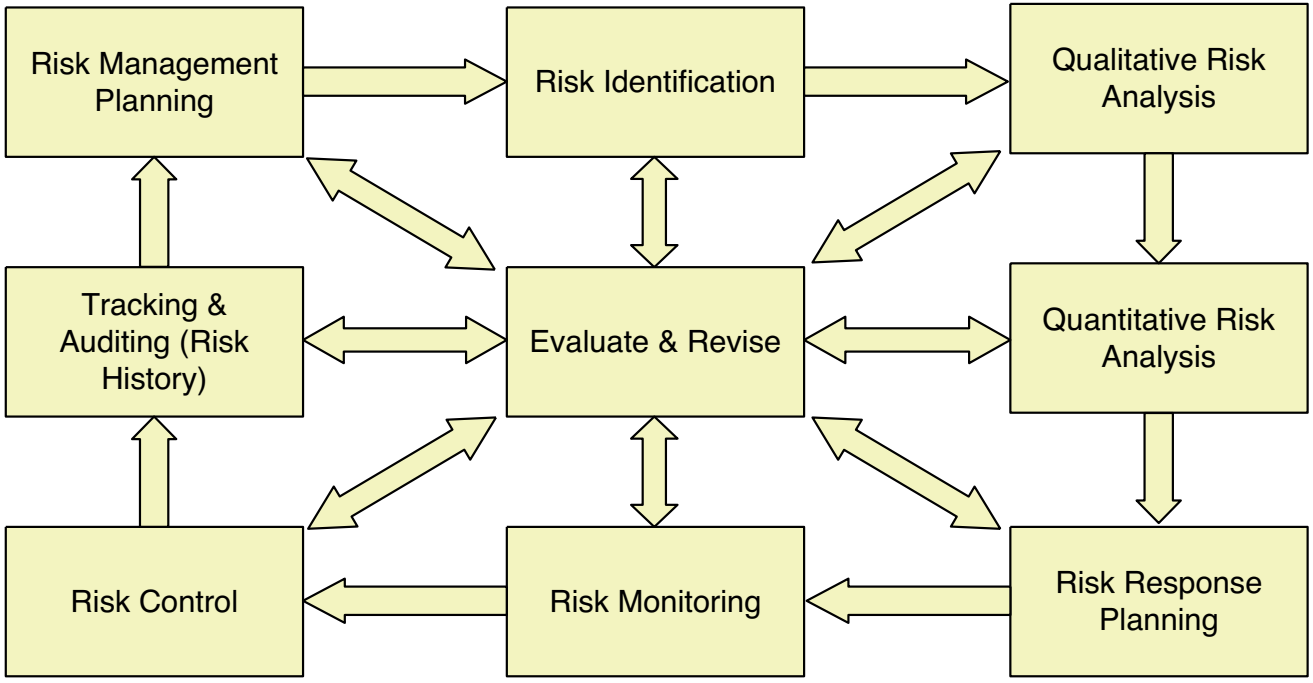
Risks: known, unknown (predictable/unpredictable), unknowable

- **Known Risks:** Risks that can be uncovered after careful evaluation of the project plan, business and technical environment, and other reliable sources of information (I.e. unrealistic delivery dates, lack of user input, expert possibly joining the team, etc.)
  - Refer to those risks that can be estimated from historical information
  - Can be mitigated by management techniques and through response plans, should they occur
  - *Example:* Potential delay in delivery from third-party vendor
  - *Example:* Key personnel leave project (or join project)
  - *Example:* Development systems down

How to Categorize Risk

- **Predictable Risks** [but unknown risks]**:** Risks that can be extrapolated from past projects. (Staff turnover, poor communication with the customer)
  - Refer to those risks that we know have a probability of occurring, but do not know the precise impact
  - Cannot be managed directly but can be mitigated by the use of contingency
  - *Example:* Loss of key personnel due to turnover
- **Unpredictable Risks**
  "Joker" risks that are hard to predict.
- **Unknowable risks**
  - Refer to those risks that are outside the scope of historical or probabilistic models for the project
  - Are beyond the scope of risk management and usually are addressed by *crisis* or *disaster management*
  - *Examples:* Corporate failures, natural disasters, acts of terrorism or war, major snowstorm and power loss

Risk management model (after Taylor)



Risk Identification

- Get the team involved in this process: Don't do it alone
- Produces a list of risks with potential to disrupt your project's cost or schedule
- Use a checklist or similar source to brainstorm possible risks
- Use a SWOT analysis process

Risk Categories

- By predictability:

Known	Unknown predictable	Unknown unpredictable	Unknowable

- By Type: Project, Technical, Business

- By Category: strategic, financial, legal/compliance, quality, schedule, customer/stakeholder

- By Source: Internal, external, technical, project environment

Three Types of Risk (Threats)

Project Threats

Threaten the project plan. i.e. if the risks materialize, then it is likely that the project schedule will slip and costs will increase.

- Budgetary/funding
- Schedule
- Personnel issues
- Resources
- Project plan
- Project management processes
- Customers
- Requirements problems: Scope or requirements changes
- Project complexity and size.
- Hardware
- Environmental risk

Three Types of Risk (Threats)

Technical Risks

Threaten the quality and timeliness of the software to be produced.

- Design
- Implementation
- Interfacing
- Verification
- Cutover
- Maintenance
- Security

Three Types of Risk (Threats)

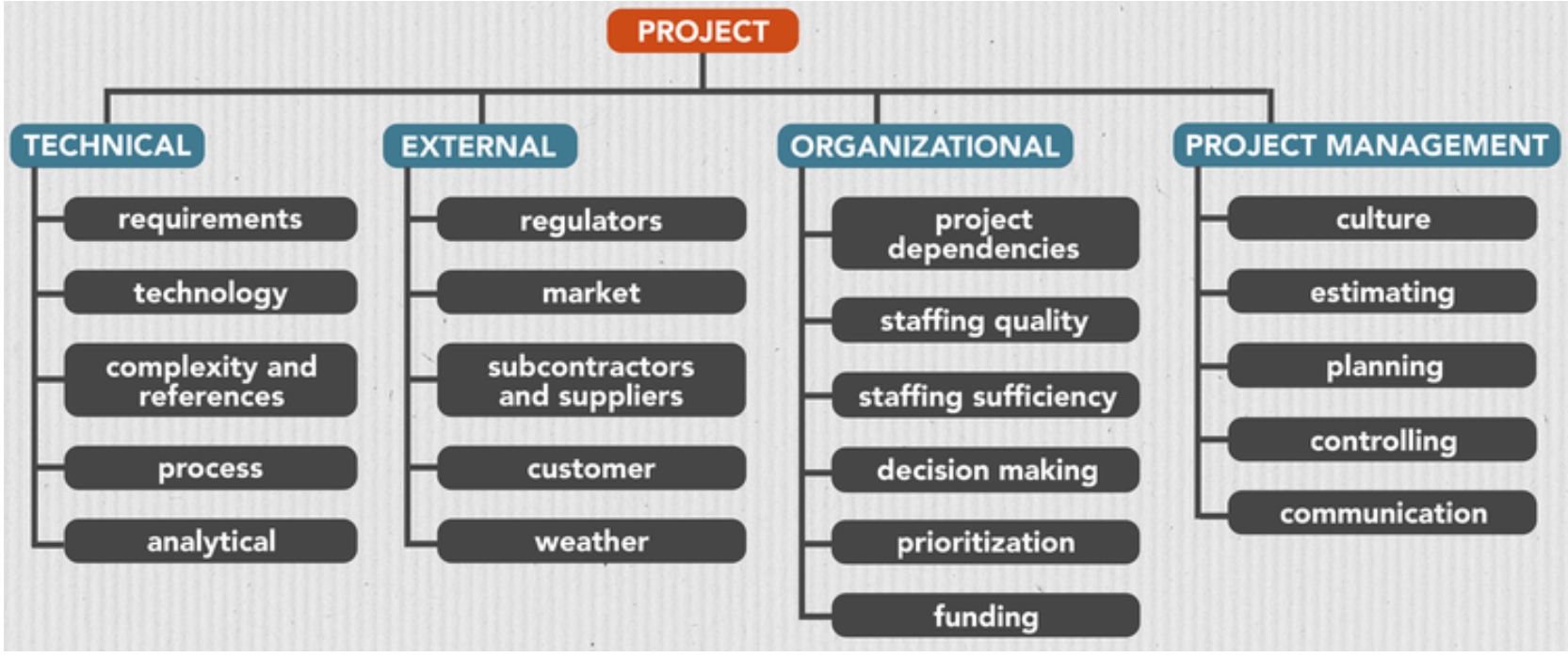
Business Risks

Threaten the viability of the product to be built.

- Building a great product that no-one wants anymore. (Market risk)
- Building a product that no longer fits into the overall business strategy for the company (Strategic risk).
- Building a product that the sales force do not find a way how to sell.
- Losing the support of senior management due to a change in focus or a change in people. (Management risk).
- Losing budgetary or personnel commitment (Budget risk)
- Contracts
- Political concerns
- Legal risk

Risk Breakdown Structure (RBS)

- Risk categories can be represented visually in a Risk Breakdown Structure (RBS) diagram
- Provides hierarchical decomposition of risk categories
- Analogous to WBS



Risk identification: tools and techniques

- **Documentation reviews**
  - To identify risks, start by reviewing all the inputs (Reviewing project charters, contracts, plans, lessons learned, and technical documentation.)
- **Information-gathering techniques**
  - Brainstorming
    - With diverse participants. Brainstorming is a self-regenerating process (Regenerating: one idea often sparks another, creating a cascade of insights)
  - Delphi technique
    - Employs a facilitator who distributes a questionnaire to participants and who compiles and synthesizes results (Experts respond independently, reducing groupthink or dominant voices)
    - Participants do not interact directly as they do in brainstorming, best for Complex or politically sensitive projects where direct discussion might bias input
- **Interviews**
  - Uses standard question and answer techniques with various stakeholders or anyone with project-relevant knowledge: One-on-one or small group conversations using structured or semi-structured questions.

Risk identification: tools and techniques

- *Root cause analysis RCA:* Technique helps determine the source of risk
  - The source of risk may seem superficial and directly visible: simply, the most immediate source. Often the true source of risk, its root cause, is less obvious and not easily detectable
  - Hall method suggests using the 'Five Whys?' approach: Ask the question 'Why?' five (more or less) times for each risk, Each successive question moves closer to the root cause. Not a highly robust method, but simple and effective.
    - Example: problem -> The team is repeatedly failing to complete planned user stories within the sprint.
    - Why 1: Why are we missing sprint deadlines? Because developers often discover unexpected technical issues late in the sprint.
    - Why 2: Why are technical issues discovered late? Because requirements are not fully understood before development begins.
    - Why 3: Why are requirements not fully understood? Because the product owner and stakeholders provide high-level descriptions without detailed acceptance criteria.
    - Why 4: Why are stakeholders providing only high-level descriptions? Because they are busy and believe the team can "figure out the details" during development.
    - Why 5: Why do stakeholders believe the team can fill in the details? Because there is no formal

Risk identification: tools and techniques

- **Checklist analysis**
  - Based on historical information and previous project team experience. Requires one or more similar projects
  - Risks can be compiled into a checklist
  - Lowest level of the RBS can be used as a starting point for a checklist
  - Checklists for projects cannot ever be exhaustive (remember, projects are *unique*)

Risk identification: tools and techniques

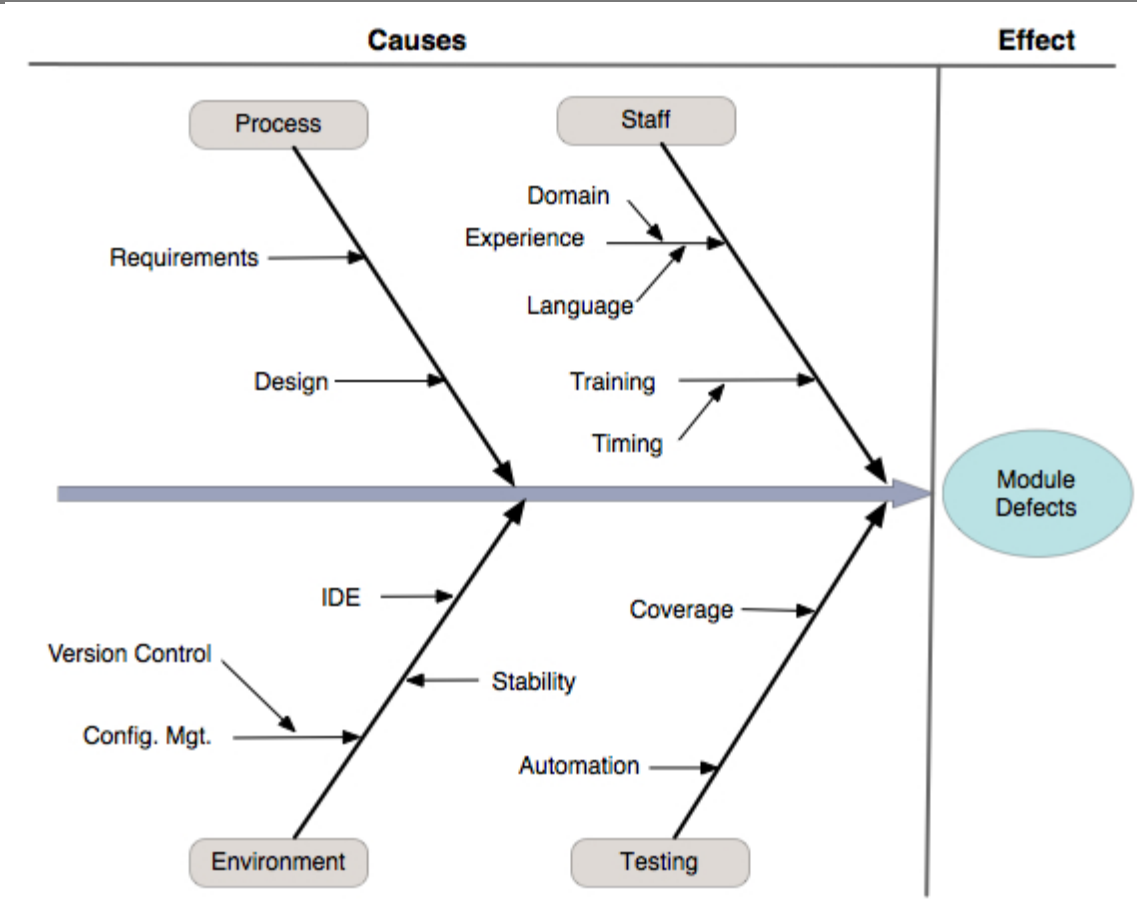
- **Assumptions analysis**
  - Validates the assumptions identified and documented throughout the project planning processes
  - Assumptions should be accurate, complete, and consistent
  - Assumptions are tested against two factors:
    - Strength or validity of the assumption
    - Consequences to the project if assumption turns out to be false
  - False assumptions should be reclassified as risks
- **Diagramming techniques**
  - Cause-and-effect (fishbone or Ishikawa) diagrams
  - System or process flowcharts
  - Influence diagrams

Cause and Effect Diagram

Also known as the *Ishikawa* (or fishbone) diagram

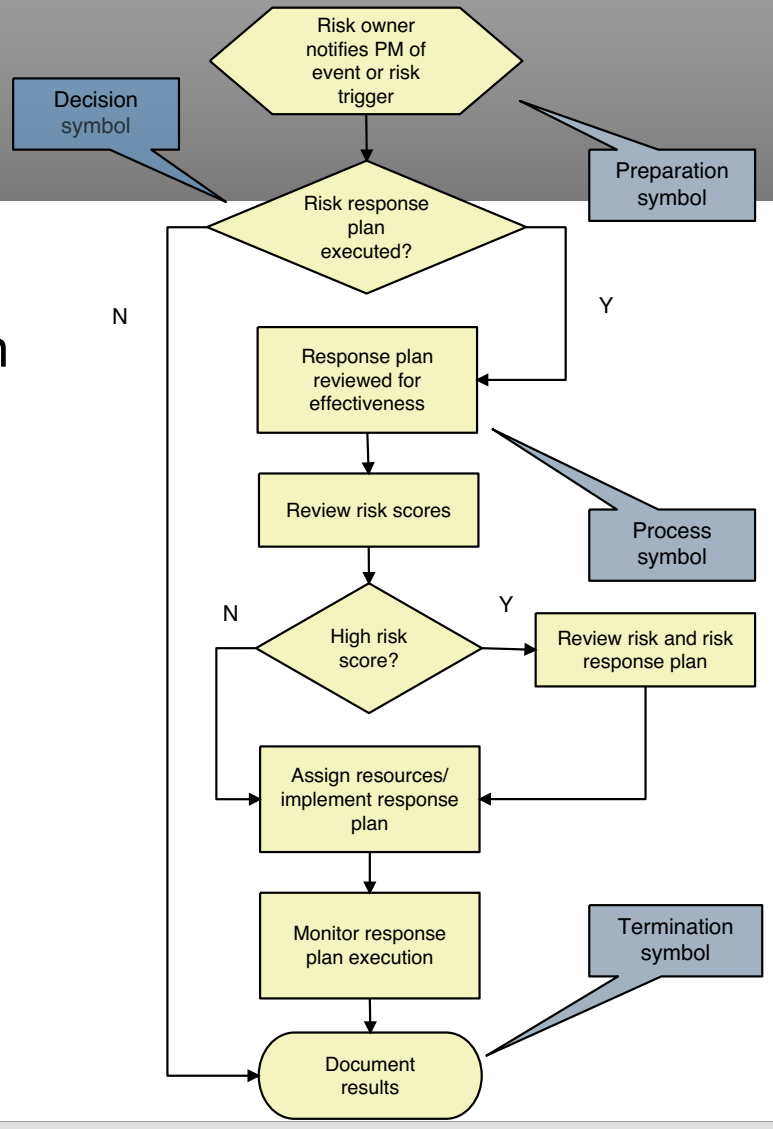
- Show the relationship between the effects of problems and their causes
- Depicts every potential cause and sub-cause of a problem and the effect that each proposed solution will have on the problem
- Useful as a tool for visually representing and capturing cause-and-effect relationships

Cause-and-effect diagram



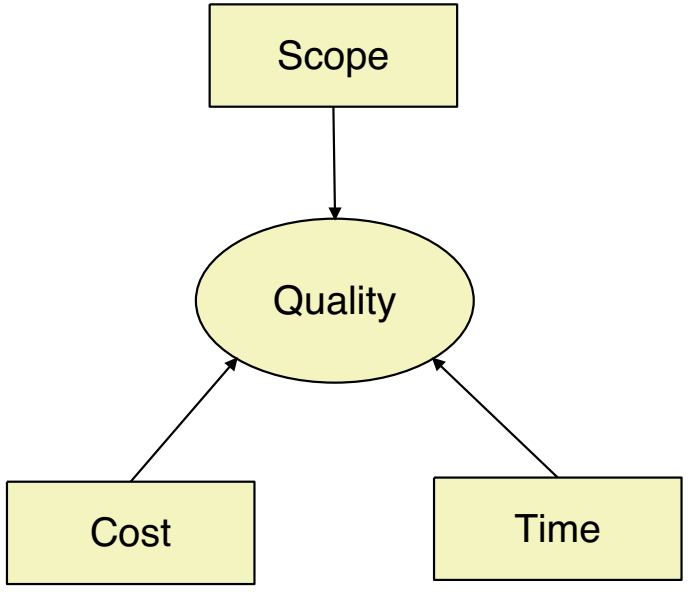
System or process flowcharts

- Familiar diagram to most stakeholders
- Shows logical steps needed to accomplish an objective
- Shows how elements of a process or system relate to each other
- Depicts cause/response relationships



Influence diagrams

- Primarily used to show the causal influences among project variables
- May also show the sequencing of events
- Used to visually depict risks (or decisions), uncertainties or impacts, and how they influence each other



Risk Identification Techniques

g2

- Identification based on past experience (Leverage the team's or organization's prior project experiences to anticipate risks).
- Identification based on historical data, perhaps through the use of a project database (Use documented evidence from past projects).
- Decision Driver Analysis, where the key decisions are examined for risk. The factors influencing decisions offer possible sources of risk (Examine key project decisions e.g., technology choices, vendor selection, staffing plans, and assess what risks they introduce).
- Threat identification in security risks (Specifically focus on identifying risks related to cybersecurity, data protection, and system vulnerabilities).

Risk Item Checklist Categories

A checklist is useful for supporting risk identification of known and predictable risks in the following subcategories:

- **Product size** – risks associated with the overall size of the software to be built or modified.
- **Business impact** – risks associated with constraints imposed by management or the marketplace.
- **Customer characteristics** – risks associated with the sophistication of the customer and the developer's ability to communicate with the customer in a timely manner.
- **Process definition** – risks associated with the degree to which the software process has been defined and is followed by the development organization.
- **Development environment** – risks associated with the availability and quality of the tools to be used to build the product.
- **Technology to be built** – risks associated with the complexity of the system to be built and the "newness" of the technology that is packaged by the system.
- **Staff size and experience** – risks associated with the overall technical and project experience of the software engineers who will do the work.

Product Size Risks

- Project risk is directly proportional to product size.
- Measure the following sizes against previous projects. If those projects were successful & results are similar, then risk is probably low. If a large negative deviation is observed then risk is HIGH.
  - Estimated size of the product in LOC (lines of code) or FP (function points)?
  - Degree of confidence in estimated size estimate?
  - Estimated size of product in number of programs, files, transactions?
  - Percentage deviation in size of product from average for previous products?
  - Number of users of the product?
    - Impact on system (loading)
  - Anticipated volatility of the requirements?
  - Amount of reused software?

Business Impact Risks

- The following items help identify generic risks associated with business impact:
  - Effect of product on company revenue.
  - Visibility to senior management.
  - Reasonableness of delivery deadline
  - Number of customers who will use the product & consistency of their needs.
  - Number of other products that it will interact with.
  - Sophistication of end users.
  - Governmental constraints.
  - Costs associated with late delivery or a defective product?

Customer Related Risks

- The following items help identify generic risks associated with the customer:
  - Have you worked with the customer in the past?
  - Does the customer have a solid idea of what is required?
  - Is the customer willing to commit significant time to the requirements gathering process?
  - Is the customer willing to establish rapid communication links with the developer?
  - Is the customer willing to participate in reviews?
  - Is the customer technically sophisticated in the product area?
  - Does the customer understand the software process?

- Risks should be investigated if the answer to any of these questions is “NO”.

Process Risks

- An ill defined software process and/or an *ad hoc* approach to analysis, design, and testing can introduce risks.
- The following are **sample** questions that should be asked to identify process risk:
  - Do you have a consistent repeatable process that is actually used?
  - Do you train all developers in the process?
  - Are formal technical reviews part of this process?
  - Do you have a mechanism for managing change? (i.e. formal RFC system + configuration management).
  - Do you have specific methods that you use for each phase of the process?
  - Is the process supported by tools?
  - Do you manage the process through use of metrics?
- Risks should be investigated if the answer to any of these questions is “NO”.

Technology Risks

- Pushing the limits of technology is challenging & exciting, yet very risky.
- Questions to identify risk include:
  - Is the technology to be built new to your organization?
  - Do the requirements require the creation of new algorithms?
  - Does the software interface with new or unproven hardware or unproven vendor products?
  - Do the requirements require the creation of components that are unlike anything your organization has previously built?
  - Do requirements demand the use of new analysis, design, or testing methods?
  - Do requirements put excessive performance constraints on the product?
- Risks should be investigated if the answer to any of these questions is “YES”.

Development Risks

- The software engineering environment supports the project team, the process, and the product.
- If the environment is flawed, it can be a source of significant risk:
  - Is a software project management tool available?
  - Are tools for analysis and design available?
  - Are compilers and code generators available and suitable for the product to be built?
  - Are testing tools available and suitable?
  - Are the software tools integrated with each other?
  - Are team members trained in the use of the tools?
  - Are tool mentors available?
- Risks should be investigated if the answer to any of these questions is “NO”.

Staff Size and Experience Risks

- CEOs have frequently observed that “people” make the most significant difference to the success of the organization.
  - Are the best people available?
  - Do the people have the right combinations of skills?
  - Are enough people available?
  - Are staff committed for the duration of the product?
  - Are some people working on multiple projects?
  - Have staff received necessary training?

Output: Risk Register

- The output of the Risk Identification process is the risk register
- All information gathered and generated during the Risk Identification process is documented in the risk register
- Risk register contains the following elements [and more]:
  - List of identified risks
  - List of potential responses
  - Root causes of risks
  - Risk categories

This part of the table (in blue) is still empty at this point

Risk No	Business Unit Level	Risk Title	Category	Risk Business Unit	Owner	Risk Assessment Period	Likelihood	Impact	Risk Level	Residual Score Direction	Count of Risk Controls	Count of Open Actions	Count of Incidents
R115	2	Risk RR002	Financial	TF London	Carole White	2021-Q4	Almost Certain	High	Very High	New Risk	1	0	0
R118	2	Tested Risk T001	Financial	Liverpool	Carole White	2021-Q4	Almost Certain	Very High	Very High	New Risk	0	0	0
R122	2	Tom Risk	Operational	TF EMEA		2021-Q4	Almost Certain	High	Very High	New Risk	0	0	0
R127	2	Out of support phase	Operational	TF EMEA		2021-Q4	Almost Certain	High	Very High	New Risk	0	0	0
R095	2	Virus Attack	Operational	TF New York	Risk Owner Test	2021-Q4	Almost Certain	Moderate	High	⇩	0	0	0
R097	2	External Threat	Operational	TF EMEA	Risk Owner Test	2021-Q4	Possible	Very High	High	⇩	0	0	0
R129	2	Faulty Risk 01	Strategic	TF EMEA	Risk Owner	2021-Q4	Almost Certain	Moderate	High	New Risk	0	0	0

Risk Analysis

Risk assessment

Objectives

- Analyze risk in a cost-efficient manner
- Determine source of risk
- Determine risk exposure
- Determine time frame for action
- Determine highest-severity risks

Risk Analysis

- Numerical analysis of risk allows to:
  - Make response decisions
  - Determine overall project risk
  - Add probability to predictions
  - Prioritize risks
  - Factor risk into cost, schedule, or scope targets
- Calculating Risk Exposure

$RE = P * I$	P = Probability
	I = Impact

Estimate the impact (e.g., weeks lost, cost units) and probability (0 to 1)

Risk Exposure

g2

- Risk Exposure Examples
  - “Facilities not ready on time”
    - Probability is 25%, size is 4 weeks, RE is 1 week : Risk exposure is delaying the project by 1 week
  - “Inadequate design – redesign required”
    - Probability is 15%, size is 10 weeks, RE is 1.5 weeks
- How to Estimate
  - Impact: The size of the loss – break into chunks
  - Probability:
    - Use team member estimates and have a risk-estimate review
    - Use Delphi or group-consensus techniques
    - Use gambling analogy” “how much would you bet”
    - Use “adjective calibration”: highly likely, probably, improbable, unlikely, highly unlikely
- Sum all RE’s to get expected overrun: quantitative forecast of how much delay (or cost) the project might face due to risks.

Quantifying risk probability

- For most situations, use of a five-point ***Likert scale*** is appropriate:
  - Highly unlikely ($p < 20\%$)
  - Unlikely ($20\% < p < 40\%$)
  - About even ($40\% < p < 60\%$)
  - Likely ($60\% < p < 80\%$)
  - Highly likely ($p > 80\%$)
- For less well-defined situations, use a three-point scale:
  - High ($p > 75\%$)
  - Moderate ($35\% < p < 75\%$)
  - Low ($p < 35\%$)
- **Likert Scale**: psychometric scale commonly used in surveys and questionnaires to measure people's attitudes, opinions, or perceptions.

Impact

- *Impact* is the amount of pain or gain the risk event poses to the various project objectives: cost, time, scope, and quality
  - Like probability, risk impact may be characterized on a subjective scale (low, medium, high)
  - Like probability, a cardinal (numeric) scale of impact is needed for the probability and impact matrix
- Employ consistent decision criteria when using a subjective scale
  - Establish a consistent means of determining what moves a borderline impact into one impact category or another

Probability and impact matrix

- Risk probability and impact values are nice, but what we need is a *single* value to characterize the combined effects of these two risk influences: the *risk rating (or exposure or level)*
- This is what a *probability and impact matrix* does: it assigns an overall risk rating to each risk
- The combination of probability and impact results in an *ordinal* (order-based) risk rating usually expressed as low, medium, or high
- A risk with high probability and high impact (and hence, high risk rating) warrants further analysis and a formal response plan in the *Risk Response Planning* process

Probability and Impact Matrix

Risk Management Matrix		Impact				
		Negligible	Marginal	Moderate	Critical	Catastrophic
Probability	Almost Certain	Low Risk	Moderate Risk	High Risk	Extreme Risk	Extreme Risk
	Likely	Minimum Risk	Low Risk	Moderate Risk	High Risk	Extreme Risk
	Possible	Minimum Risk	Low Risk	Moderate Risk	High Risk	High Risk
	Unlikely	Minimum Risk	Low Risk	Low Risk	Moderate Risk	High Risk
	Rare	Minimum Risk	Minimum Risk	Low Risk	Moderate Risk	High Risk

Risk Prioritization

- Remember the 80-20 rule (a principle that suggests that 80% of outcomes come from 20% of causes): Focus on high impact risks

- Possibly group ‘related risks’
- Helps identify which risks to Ignore
  - Those at the bottom
- Use Risk Register

Risk No	Business Unit Level	Risk Title	Category	Risk Business Unit	Owner	Risk Assessment Period	Likelihood	Impact	Risk Level	Residual Score Direction	Count of Risk Controls	Count of Open Actions	Count of Incidents
R115	2	Risk RR002	Financial	TF London	Carole White	2021-Q4	Almost Certain	High	Very High	New Risk	1	0	0
R118	2	Tested Risk T001	Financial	Liverpool	Carole White	2021-Q4	Almost Certain	Very High	Very High	New Risk	0	0	0
R122	2	Tom Risk	Operational	TF EMEA		2021-Q4	Almost Certain	High	Very High	New Risk	0	0	0
R127	2	Out of support phase	Operational	TF EMEA		2021-Q4	Almost Certain	High	Very High	New Risk	0	0	0
R095	2	Virus Attack	Operational	TF New York	Risk Owner Test	2021-Q4	Almost Certain	Moderate	High	⇩	0	0	0
R097	2	External Threat	Operational	TF EMEA	Risk Owner Test	2021-Q4	Possible	Very High	High	⇩	0	0	0
R129	2	Faulty Risk 01	Strategic	TF EMEA	Risk Owner	2021-Q4	Almost Certain	Moderate	High	New Risk	0	0	0

This part of the table (in blue) is still empty at this point

Risk data quality assessment

- Low-quality data renders qualitative risk analysis almost useless
- Quality assessment examines:
  - Quality of data used
  - Availability of data for identified risks
  - How well the risk is understood
  - Reliability and integrity of data
  - Accuracy of data
- Risk categorizations
  - Entries in the RBS can help identify the concerned project phase and determine the elements of the project that are affected by risk

Risk data quality assessment: How risk averse is the PM?

The quality of the risks analysis depends on the personality of the person who made the analysis:

Risk averse people:

- ❑ I like being dependable/reliable and I'm usually punctual.
- ❑ I am not likely to take risks.
- ❑ I am responsible and prefer to work efficiently.
- ❑ I am more service oriented than self oriented.
- ❑ I value institutions and observe traditions

Risk seeking people:

- ❑ I like action, and I act impulsively at times.
- ❑ I seek excitement for the thrill of the experience.
- ❑ I am resourceful and prefer not to plan or prepare.
- ❑ I am more self oriented than service oriented.
- ❑ I like to anticipate another person's position.

Risk neutral people:

- ❑ I trust my intuition, and I am comfortable with unknowns.
- ❑ I think about the future and have long-range objectives.
- ❑ I am naturally curious and often ask, "Why?"
- ❑ I enjoy generating new ideas.
- ❑ I work best when I am inspired.

Outputs: Updates to the risk register

- Update risk register with the following information:
  - *Risk ranking of identified risks*. Order the identified risks by risk rating (exposure)
  - *Risks grouped by categories.* Identify low, medium, and high risk groups to allow easier risk urgency assessment and planning
  - *List of risks requiring near-term responses*
  - *List of risks for additional analysis and response*
  - *Watch list of low-priority risks.* Low-priority risks can still impact a project, monitor them
  - *Qualitative Risk Analysis trends.* Look for patterns that might help in response planning

Risk Planning

Introduction

- ***Risk Management Planning*** addresses how to approach, plan, and execute all of the project risk management activities
- The risk management plan is critical to the overall risk management process
  - A well-defined, comprehensive risk management plan enhances the chances of success of the risk management process
- Risk analysis and planning should continue throughout the project
- Develop risk response strategies

Risk urgency assessment

- Do not try to deal with all risks at the same time
- Analogous to rolling wave planning: determine how soon potential risks might occur
- Develop risk response plan for those risks that might occur soon
- For greater efficiency and effectiveness, only the top ten risks should be actively managed
- Maintain a watch list of the remaining risks to replace those on the 'top 10’ list that are mitigated, controlled, eliminated, or that don't materialize

Input to risk management planning

Risk management planning doesn't happen in isolation, it draws from key foundational documents/sources of information and strategic considerations:

- **Enterprise environmental factors**
  - Concerned with aspects of the enterprise outside of project
  - One source may be enterprise historical information
  - Industry or academic research is another excellent source
    - *Example:* Consulting Firms Reports (Provide expert analysis on technology trends, vendor landscapes, and strategic risks)
    - comp.risks (Usenet discussion group/mailing list, see reading list): A long-running forum for discussing computer-related risks, including software failures, cybersecurity, and ethical concerns.

Input to risk management planning

- **Enterprise environmental factors**
  - Most critical environmental factors are the *risk tolerance levels* of the organization and the stakeholders
    - Risk tolerance expresses an inherent trade-off decision between benefits and cost
    - Stakeholders will take a risk if the benefits to be gained outweigh what could be lost
    - Conversely, stakeholder will avoid taking a risk because the cost or impact is too great for the amount of benefit that can be derived

Input to risk management planning

- **Organizational process assets**
  - Organization may already have policies and guidelines that define its risk tolerance
- **Project scope statement**
  - Project assumptions, constraints, and initial defined risks in scope statement
  - The project scope statement contains several information sources for risk management **planning**:
    - Project deliverables
    - Project constraints
    - Project assumptions
    - Initial project organization
    - Initial defined risks
    - Schedule milestones

Input to risk management planning

- **Risk management plan**
  - Risk categories (*e.g.* as defined in RBS) are primary source of input
  - Planning for risk requires resources: Budget and schedule for risk management activities
- **Project management plan**
  - Risk management plan becomes an integral part of the project management plan
  - All other project management processes and guidelines comprising the project management plan should be considered in light of potential risks
  - Risk management plan should be consistent with the overall direction and management approach of the project

Risk management planning: tools & output

- **Risk management planning tools**
  - *Planning meetings* are the main tool for risk management planning
  - Attendees should include the project manager, members of the project management team, and stakeholders who can contribute risk-related information
  - Meetings will involve *analysis* of risk for the project, risk tolerance of the organization, and calibrating risk to the project and organization
- **Risk management planning output**
  - The *risk management plan* is the only output from the risk management planning process

Meetings are the main tool.

Risk management plan content

In addition to the information already prepared during the analysis phase:

- *Methodology:* How risk management will be performed, including methods, tools, and sources of data
- *Roles and responsibilities:* Team of people responsible for managing identified risks and responses, the risk ‘owners’
- *Budgeting:* Assign resources and estimate costs of risk management and its methods
- *Timing:* Timing and frequency of the risk management processes
- *Risk categories:* May need to refine risk categories

Risk management plan content

Revised stakeholder tolerances: Risk planning may result in changes in stakeholder tolerance

Reporting formats: Describes the content and format of the *risk register,* the dictionary of risks for project

Tracking: Describes how the risk activity history will be documented and how risk processes will be audited

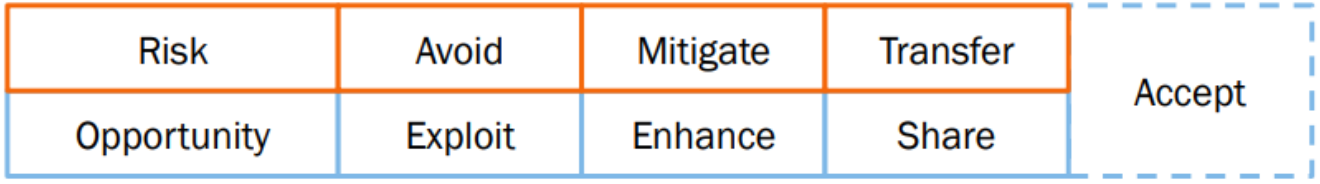
Risk Response Planning: Introduction

- *Risk response* planning is concerned with developing options and possible reactions to mitigate threats and exploit opportunities discovered during the risk analysis processes
- The severity of the risk dictates the level of **risk response planning** that should be performed
- A risk with low severity is not worth the time it takes to develop a detailed risk response plan
- Risk responses should be cost effective
  - If the response cost is more than the cost of the risk, formulate a less-costly risk response

Risk Response Planning: Introduction

- Risk responses must be timely
  - An untimely risk response itself becomes a risk
- Risk responses must be agreed to by all the project stakeholders
- Risk responses must be assigned to an individual (the *risk owner*) who is responsible for monitoring the risk and executing the risk response plan if needed

Risk Resolution



- Risk Avoidance
  - Don’t do the project at all
  - Reduce project scope
- Problem control (Mitigation)
  - Develop contingency plans
  - Allocate extra resources
- Knowledge Acquisition
  - Investigate/ research
  - Buy information or expertise about it
- Risk Transfer
  - To another part of the project (or team)
  - Move off the critical path

Strategies for negative risks or threats

- **Avoidance**
  - *Risk avoidance* evades a risk, eliminates the cause of the risk event, or changes the project plan to protect the project objectives from the risk event
  - Risk avoidance eradicates the risk by removing the risk or its cause
  - Risk avoidance is most suitable in the early stages of a project, through improved communications, additional resources, or more-clearly defined scope

  - *Example:*

  Risk of interfacing Membership Management System (MMS) to external art museum membership systems can be avoided by eliminating requirement to do so

Strategies for negative risks or threats

- **Risk transfer**
  - *Risk transfer* moves the risk and the consequences of that risk to a third party
  - Responsibility for the management of that risk now rests with another party
  - Risk transfer comes in many forms but is most effective for financial risks
    - *Example:* transfer KYC legal requirements to an external KYC services provider

Strategies for negative risks or threats

- **Contracting**
  - *Contracting* is a form of risk transfer
  - The contractor accepts certain aspects of the risk and responsibility for the cost of failure
  - Types of contracts:
    - Fixed-price contract: If costs exceed expectations, the contractor absorbs the loss. Contractor increases cost of the contract to compensate for the level of risk they are accepting.
    - Cost reimbursable contract: The contractor tracks and bills for direct costs and receives compensation for additional costs. Majority of the risk remains with the buyer.

Risk Mitigation, Monitoring, and Management

- **Mitigation** – how can we avoid the risk?
- **Monitoring** – what factors can we track that will enable us to determine if the risk is becoming more or less likely?
- **Management** – what contingency plans do we have if the risk becomes a reality?

Strategies for negative risks or threats

- **Mitigation**
  - *Risk mitigation* attempts to reduce the probability of a risk event and/or its impacts to an acceptable level
  - Risk mitigation takes the viewpoint that fixing a problem earlier in a project is less costly than fixing it later
  - Examples: Performing more tests, using simpler processes, perform simulations, choose vendors for reliability over cost
- **Risk acceptance**
  - The risk is acknowledged, but no action is taken unless the risk occurs
  - Appropriate when it is not possible or cost-effective to address a specific risk in any other way
  - *Passive acceptance* simply documents that the acceptance strategy has been adopted and leaves the project team to deal with the risks
  - *Active accept*ance set aside risk reserves, such as a pool of funds, time, or resources to be used in response to a risk event

Strategies for negative risks or threats

- **Risk contingency plans** q
  - *Contingency planning* involves planning alternatives to deal with the risks, should they occur
  - Contingency plans do not seek to reduce the probability or impact of risks, the strategy accepts that the risk may occur and plans ways to respond to the risk
  - A contingency plan is executed when the risk event occurs
  - Contingency plans must be in place well before the time the risk may occur
  - Contingency plans are developed for risks:
    - With very high impact or:
    - With response strategies that may themselves be risky (require preparation)
  - Contingency plans usually entail a significant alternative path through part of the project
  - *Example:* disaster recovery plan

Contingency planning tools

- *Contingency allowances (or reserves):* Contingency allowances provide a pool of funds, time, or resources that are held for use in response to an **unavoidable** risk event
  - *Example:* Including contingency time in case of loss of key personnel
- *Fallback plans:* Fallback (or 'Plan B') plans are developed for risks with high impact or for risks with strategies that may in themselves be risky
  - Fallback plans may be used to address *secondary risks*
  - *Example:* Use of a relational database plus object-oriented interface (ORM) in place of pure O-O database.

Strategies for positive risks or opportunities

- **Exploitation**
  - *Exploitation* involves looking for opportunities for positive impacts
  - *Example:* Reduce project duration by using more experienced resources on critical tasks
- **Sharing**
  - Sharing assigns opportunity to a third-party owner who is better able to exploit it
  - *Example:* Form a joint venture between a technical software company and marketing and sales firm

Sidebar: Residual and secondary risks

- ***Secondary risks*** arise as a result of implementing a risk response, they are the risks inherent in the response
  - Identify and plan responses for secondary risks using tools such as fallback plans
  - *Example:* O-O/RDB expert consultant becomes ill
- ***Residual risks*** are those that cannot be effectively dealt with within the rest of the risk plan
  - *Example:* Some risk may remain. Residual risks are usually dealt with through contingency reserves
  - *Example:* Developer skills risks (resource planning risk) associated with alternate database solution

Risk response planning outputs

Risk register updates

- List of identified risks, including:
  - Descriptions
  - WBS element or area of the project impacted
  - Root causes
  - Project objectives impacted by the risk impacts
  - Risk owners and their responsibilities
  - Risk triggers: precursors to risk event; Trigger conditions, symptoms, and warning signs of a risk occurrence

Response plans and strategies

- Specific actions to implement the chosen response strategy
- Fallback plans if the primary response strategy proves inadequate

Risk response planning outputs

Risk register updates

- Cost and schedule activities needed to implement risk responses
- Contingency plans
  - Contingency plans and triggers for their execution
  - Contingency reserves for cost, time, and resources
  - Fallback plans
- List of residual and secondary risks
- Probabilistic analysis of the project and other outputs of the risk analysis process: Quantitative analysis (e.g., Monte Carlo simulations, decision tree analysis) to assess the overall impact of risk on project objectives. Outputs may include:
  - Range of possible completion dates or costs
  - Confidence levels (e.g., “There’s an 80% chance we’ll finish within 12 months”)

Risk Monitoring

Risk Monitoring

- Top 10 Risk List
  - Rank
  - Previous Rank (or history)
  - Weeks on List
  - Risk Name
  - Risk Resolution Status (active, mitigated, resolved…)
- This top 10 list is a low-overhead best practice: easy to maintain, easy communication, scalable)
- Interim project post-mortems (reassess this top ten list, evaluate effectiveness of responses, etc.)
  - After various major milestones
- Communicate w/ Stakeholders: Keeps stakeholders informed of evolving risks, builds trust.

Risk Register
Risk Number
Risk Category
Risk Name
Probability (Scale)
Impact (Scale, Areas)
Score/ Risk Impact (P*I)
Indicators
Mitigation
Contingency
Affected Stakeholders
Resource/Response Time

Monitor and Control Risks

- Key Concepts in Risk Monitoring and Control:
  - Workarounds – unplanned corrective action for unanticipated problems
  - Risk Reassessments – periodic risk review and adjustments
  - Risk Audits – proves risk preparedness and provides lessons learned
  - Reserve Analysis – accounting for risk reserves (financial and schedule), which are only for risk
  - Status Meetings – should primarily focus on risks
  - Closing Risks – the conditions surrounding a risk are in the past, and the risk should be closed
- Outputs: Risk Register Updates, Change Requests, PM Plan Updates, Project Document Updates, Lessons Learned

Miniature Milestones: Reduces risk

- Use of small goals within project schedule (1-2 days): By breaking the schedule into smaller units, delays or issues are spotted before they compound
- Reduces risk of undetected project slippage
- Requires a detailed schedule, including early milestones
- Use binary milestones statuses (done or not done)
- Pros
  - Enhances status visibility
  - Good for project recovery
  - Can improve motivation through achievements
  - Encourages iterative development
- Cons
  - Increase project tracking effort

Conclusion: Basic principles

- Risks must be managed
- Risk must always be one of the principle concerns of the project management team
- Risks must be reported
  - Risks should be an agenda item in weekly team meetings
  - Risks should be included in the project status report
  - Weekly project review should review all risks
- Team meeting
  - Should briefly review all outstanding risks
  - Should estimate whether each risk's probability has increased, has decreased, or is unchanged
  - Risk owners should report on their assigned risks

Conclusion: Basic principles

- In the project status report, list all risks for which the degree of risk has changed
- Weekly project review
  - Review all risks, even those that have been eliminated
  - Goal is to uncover new risks or identify those that have reappeared
- Reviewing risks in weekly team meetings keeps the team and risk owners aware and sensitized to risks
- Including risks in the project status report prepares management for the time(s) when risks happen