Risk management:

identification → quantification → response → control

identification of risks

A **risk** is a possible future event, which, if it happens, will hurt the project. A risk is a problem or disaster looking for an opportunity to happen. The characteristics of a risk are:

- if the risk happens, you lose something: time, money, etc.
- there is some non-zero likelihood that the risk will occur
  (i.e. don't worry about meteors crashing into your project office)
- to some degree, we can minimize the risk.

so what could go wrong?

generic risks:

- unrealistic, unstable, immature or excessive requirements
- misunderstanding the requirements (even if they are reasonable)
- personnel turnover, loss of key people
- inadequate time for testing
- misunderstanding of target environment
- disputes among project teams
- misestimation of project difficulty or complexity

project specific risks:

- failure of research components to converge to successful solution
- failure of sub-contractor to deliver promised hardware/software on schedule
- inadequate budget
- unreasonable schedule
- inadequate personnel or personnel organization
- inadequate, inconsistent development platform, tools
- inadequate resources allocated to project
- uncooperative customers, vendors, subcontractors

business risks:

- no one wants the product
- the organization doesn't want the product
- the organization doesn't know how to sell the product
- senior management loses interest in the project
- loss of budget or personnel allocated to the project
- reorganization that makes the project a non-core activity

Boehm's top 10 risk items

- personnel shortfalls :skill and knowledge levels, staff turnover, team dynamics…

- unrealistic schedules and budgets: requirements demand more time or money…
- developing the wrong software functions: complexity, imperfect understanding…
- developing the wrong user interface: not user-friendly, misleading…
- gold plating: adding unnecessary "nice" features
- continuing stream of requirements changes: requirement volatility forces rework
- shortfalls in externally performed tasks: subcontractors or users don't do what's needed
- shortfalls in externally furnished components: hardware or supporting software is inadequate
- real time performance shortfalls : some or all of the system causes bottlenecks…
- straining computer science capabilities: unstable or unfamiliar technology

risk quantification

Risk exposure is the sum of ((probability of risk) * (cost of risk)) for all risks.
The cost of the risk can be measured in dollars or some other impact measurement.

risk estimation (projection)
- identify likelihood of each perceived risk
- determine the consequence/impact of the risk on the project and/or product
  - nature of the problem associated with the risk
  - scope – how serious is the risk and how much of the project will be affected
  - timing – will the risk arise early or late in the project
- determine uncertainty bounds for risk estimates

risk response

risk avoidance
- change requirements (or the methods, or…) so the risk no longer applies
- take precautions to reduce the probability of the risk
  e.g. delete functionality that looks hard to implement

risk transfer
- make your risk someone else's risk
- look for another way (tool, technique, resources…) to tackle the situation
  e.g. project completion insurance, move risk to client

risk assumption
- accept a potential risk and its consequences as part of the project
- but take preventative actions to reduce probability and impact
- prepare contingency plans
  e.g. arrange for "stand-by" expertise

risk control

All this risk management takes resources and may add delays to the project. The amount of risk management actually done depends on the magnitude of the project and the consequences of the expected risks and the cost of mitigation.

Risk management tracks risk exposure during a project and applies risk control to reduce exposure.

Risk control attempts to minimize the probability of risks occurring and/or minimizes its effect on the project.

The recommended steps are:

1. identify the risks
   - use existing lists (like Boehm's) and make your own lists specific to the politics, culture, technology, etc. that constitutes the project environment
   - review the project plan with skepticism

2. determine the risk exposure
   - calculate the probability of occurrence and the cost or occurrence
   - identify the highest risks that really matter (you probably shouldn't deal with every risk)

3. develop strategies to mitigate the risks
   - decide whether you want to take precautions (risk avoidance), look for other ways to proceed (risk transfer) or create contingency plans (risk assumption)

4. handle the risks
   - monitoring critical tasks, deliverables to detect if the risk has occurred
   - looking for new risks
   - update risk estimates and contingency plans as the project moves along
   - taking timely action

a risk management example

The risk is project high staff turnover.

pre-project prevention
- try to address the causes of the high turnover
- fix any problems that can be fixed (for example, working conditions)
- assume high turnover will occur and structure the project to compensate for the effects of high turnover

intra-project compensation
- organize project teams so information about the project is widely disseminated
- demand detailed documentation in all phases of the project
- monitor to make sure that documentation is kept current
- use peer reviews (inspections, walkthroughs) of all work as a mechanism to disseminate project information
- identify critical personnel and assign a backup person to each and keep the backup person should current with the critical person's work

risk documentation

risk description:
- risk statement (condition-consequences format, "if this happens then that will occur")
- context (circumstances, environment, resources and other issues affecting the risk)
- impact (affected products, schedules, etc.)
- time frame (period during which risk is real, period during which action can/should be taken)
- probability (likelihood of risk occurring)
- mitigation strategy (proposed action or eliminate, reduce or prevent the risk)

risk management and control information:
- status
- priority (high, medium, low)
- risk origin (who identified the risk)
- date opened/identified
- assigned to (person examining risk and recommending mitigation)
- status/date (status changes such as change in probability of key events or a change in the potential impact)
- date closed

There is an example in the slides.
And another example of a risk management worksheet might look like this:

risk		exposure			mitigation	
description	category /priority	proba-bility	impact ($1,000)	exposure ($1,000)	cost of ($1,000)	approved (Y/N)
high staff turnover	med	40%	$2.5	$1.0	$3.0	N
delivery deadline tightened	high	25%	$50	$12.5	$8	Y
change in re-use policy	med	60%	$13	$7.8	$6	N

formal risk management

The Project Management Institute's "A Guide to the Project Management Book of Knowledge" gives the following risk management overview.

Project Risk Management			
1. risk identification	**2. risk quantification**	**3. risk response development**	**4. risk response control**
inputs			
product description, other planning outputs, historical information	stakeholder risk tolerances, sources of risk, potential risk events, cost estimates, activity duration estimates	opportunities to pursue, threats to respond to, opportunities to ignore, threats to accept	risk management plan, actual risk events, additional risk identification
tools and techniques			
checklists, flowcharting, interviewing	expected monetary value, statistical sums, simulation, decision trees, expert judgement	procurement, contingency planning, alternative strategies, insurance	workarounds, additional risk response development
outputs			
sources of risk, potential risk events, risk symptoms, inputs to other processes	opportunities to pursue, threats to respond to, opportunities to ignore, threats to accept	risk management plan, inputs to other processes, contingency plans, reserves, contractual agreements	corrective action, updates to risk management plan