

UNIT 5

Risk Management

(5 Hours) — Software Project Management (CACS407)

NOTE: These notes may contain errors. Please verify important points, definitions and calculations with your textbook and teacher before relying on them.

5.1 Introduction to Risk

A **risk** is an uncertain event or condition that, if it occurs, has a negative (or sometimes positive) effect on project objectives such as cost, schedule, scope or quality. A risk is something that *might* happen; a **problem** (or issue) is a risk that has already happened.

Risk management is the systematic process of identifying, analysing and responding to risks so that their probability and impact are kept at an acceptable level. Software projects are particularly risky because of changing requirements, new technology, complexity and people-related issues.

Term	Meaning
Risk event	The uncertain event itself (e.g. a key developer leaves).
Probability (likelihood)	Chance that the risk event occurs, 0 to 1.
Impact (loss)	Effect on the project in money, time or quality if it occurs.
Risk exposure (RE)	RE = Probability × Impact ; expected loss from the risk.
Risk trigger	A sign that a risk is about to occur or has occurred.
Contingency plan	Planned response to be used if the risk occurs.

5.2 Categories of Risk

Category	Examples
Project risks	Budget, schedule, staffing, resources, customer and requirements problems; threaten the project plan.
Technical risks	Design, implementation, interface, verification, maintenance problems; ambiguous specification; new/unproven technology.
Business risks	Building a product nobody wants, loss of market position, strategic mismatch, lack of sales support, loss of budget.

Category	Examples
Known risks	Found after careful evaluation of the plan and environment (e.g. unrealistic delivery date).
Predictable risks	Extrapolated from past projects (e.g. staff turnover, poor communication).
Unpredictable risks	Very hard to foresee (e.g. a sudden regulatory change).

5.2.1 Other useful classifications

- **By source:** requirements, estimation, people, technology, process, external (vendors, laws, market).
- **By Hughes-Cotterell:** risks may relate to application, environment, product, people, process, size, structure, management and external factors.
- **By stage:** planning risks, development risks, deployment and operational risks.

5.2.2 Boehm's top ten software risk items

#	Risk item
1	Personnel shortfalls
2	Unrealistic schedules and budgets
3	Developing the wrong software functions
4	Developing the wrong user interface
5	Gold plating (adding unnecessary features)
6	Continuing stream of requirements changes
7	Shortfalls in externally performed tasks
8	Shortfalls in externally furnished components
9	Real-time performance shortfalls
10	Straining computer-science capabilities

5.3 Framework for Dealing with Risk

Risk management is an ongoing cycle with the following stages:

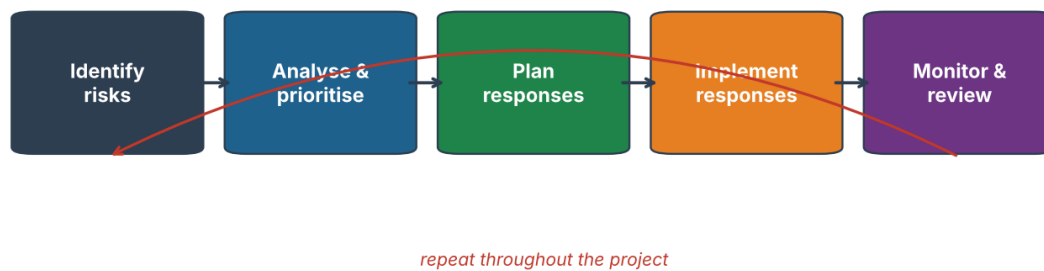


Figure 5.1 — Risk management cycle

5.3.1 Risk identification

The aim is to produce a list of risks. Techniques include:

- **Checklists** of risks seen in earlier projects (for example Boehm's list).
- **Brainstorming** with the team and stakeholders.
- **Delphi technique** — experts list risks anonymously and refine them over rounds.
- **Interviews** and review of project documents, assumptions and WBS.
- **Lessons learned** and risk databases from past projects.
- **SWOT** analysis and cause-effect (fishbone) diagrams.

5.3.2 Risk analysis and evaluation (prioritisation)

Qualitative analysis ranks risks as high/medium/low using a probability-impact matrix.

Quantitative analysis assigns numbers: probability, loss, and risk exposure ($RE = P \times L$).

Example 5.1 — Risk register

The project manager of the online admission project has identified the risks below (impact in Rs. '000).

ID	Risk	Probability	Impact (Rs. '000)	$RE = P \times L$
R1	Key developer leaves	0.30	400	120
R2	Requirements change late	0.50	300	150
R3	Payment gateway integration delayed	0.40	150	60
R4	Server hardware delivered late	0.20	100	20
R5	Test environment unstable	0.10	50	5

Solution

Ranking by risk exposure (highest first): R2 (150), R1 (120), R3 (60), R4 (20), R5 (5).

Total expected loss = 355 (Rs. '000). Management attention should go first to the top-ranked risks (R2 and R1 account for 76% of the total exposure).

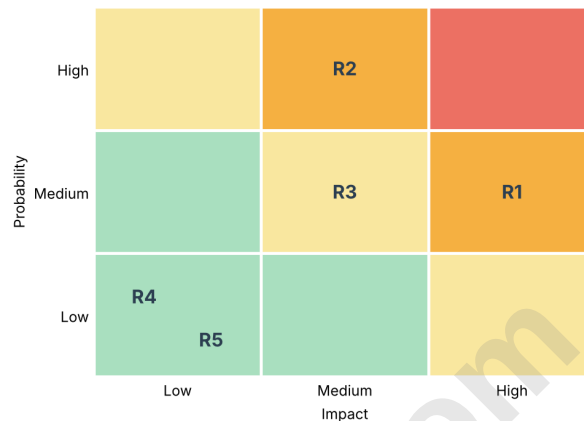


Figure 5.2 — Probability-impact matrix for the risks of Example 5.1

5.3.3 Risk planning (response strategies)

Strategy	Idea	Example
Avoid	Change the plan so the risk cannot occur.	Drop a risky feature; use a proven technology.
Reduce / mitigate	Lower probability or impact.	Training, prototypes, extra testing, pair programming, documentation to reduce dependence on one person.
Transfer	Shift the consequences to a third party.	Insurance, fixed-price contract with a vendor, outsourcing.
Accept (contingency)	Do nothing now; prepare a fallback plan or reserve.	Contingency budget, schedule buffer, backup plan.

A **risk reduction leverage (RRL)** measure can be used to compare options: **RRL = (RE before – RE after) ÷ Cost of risk reduction**. A leverage greater than 1 means the action is worth its cost.

Example 5.2 — Risk reduction leverage

Risk R1 has RE = 120 (Rs. '000). Training a backup developer costs Rs. 30 thousand and reduces the probability from 0.30 to 0.10 (impact stays 400).

Solution

RE after = $0.10 \times 400 = 40$.

RRL = $(120 - 40) / 30 = 2.67$. Since $RRL > 1$, the training is worthwhile.

5.3.4 Risk monitoring and control

- Maintain a **risk register** (risk, owner, probability, impact, response, trigger, status).
- Review the top risks at every progress meeting; watch for triggers.
- Re-assess risks at milestones; close the ones that have passed and add new ones.
- Invoke contingency plans when a risk occurs and record lessons learned.

5.4 Evaluating Risks to the Schedule

Schedule risk arises because activity durations are uncertain. A single critical-path estimate hides this uncertainty. Techniques to evaluate it are described below.

5.4.1 Critical path and float analysis

Activities on the critical path and *near-critical* activities (small float) are the main sources of schedule risk. A delay in any critical activity delays delivery. See Unit 2 for the calculation.

5.4.2 PERT three-point estimates

With optimistic, most likely and pessimistic times, the expected duration and standard deviation of the critical path are computed, giving the probability of meeting a given date (Z-value method). For the network in Unit 2, the expected duration is 17 days with a standard deviation of about 1.25 days, giving about 95% chance of finishing by 19 days.

*Note: PERT considers only the critical path, so it tends to be **optimistic**: other paths can overtake it in some outcomes.*

5.4.3 Monte Carlo simulation

Monte Carlo simulation repeatedly picks a random duration for every activity from its probability distribution (for example triangular, using o, m, p) and computes the project duration, thousands of times. The results give a probability distribution of the completion date.

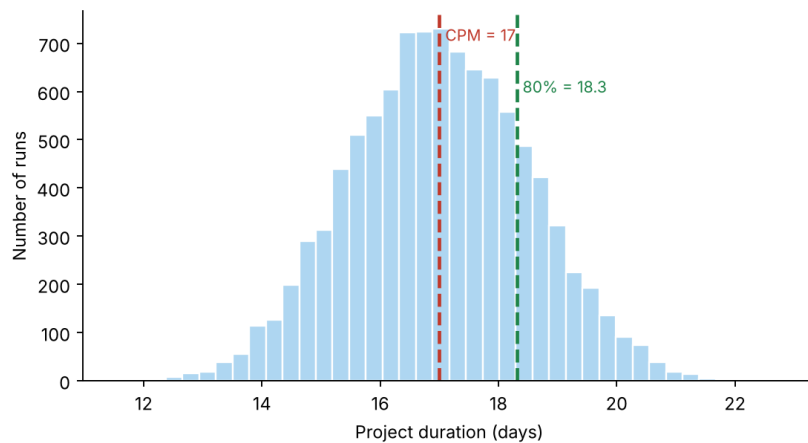


Figure 5.3 — Simulated project duration (10,000 runs) for the Unit 2 network

Simulation result (triangular distributions, same network as Unit 2)

Mean duration ≈ 17.0 days; median ≈ 17.0 ; 80th percentile ≈ 18.3 ; 90th percentile ≈ 18.9 .

Probability of finishing within the CPM estimate of 17 days $\approx 50\%$; within 19 days $\approx 91\%$.

So the deterministic CPM date of 17 days is much less likely than it appears; a plan with an 80% confidence level needs a longer deadline. (Exact percentages depend on the random seed and the assumed distributions.)

5.4.4 Other schedule-risk techniques

- **Schedule buffers / contingency** added to critical activities or to the end of the project.
- **Critical chain method** — aggregate safety time into a project buffer instead of padding every task.
- **Schedule risk checklist**: unrealistic deadlines, unclear requirements, dependence on external deliveries, staff availability, learning curve.
- **Re-estimation and tracking** using earned value or milestone trend charts to detect slippage early.

Key Takeaways

- ✓ A risk is an uncertain event; risk exposure $RE = \text{probability} \times \text{impact}$.
- ✓ Categories: project, technical and business risks; also known, predictable and unpredictable risks.
- ✓ Framework: identify → analyse and prioritise → plan response → implement → monitor, repeated through the project.
- ✓ Responses: avoid, reduce/mitigate, transfer, accept with contingency. $RRL = (RE \text{ before} - RE \text{ after}) \div \text{cost}$.
- ✓ Schedule risk is evaluated through critical-path/float analysis, PERT, Monte Carlo simulation and buffers.
- ✓ A risk register reviewed regularly is the main working tool.

— *End of Unit 5* —

bcalink.com