Risk Management

Characteristics Of Risk

1) Uncertainty(Probability of Occurrence)
2) Loss

Types of Risk

Two ways in which we may categorize them:

1)Generic Risk 2)Product Specific Risk

Or

1)Unknown Risk

2)Known Risk

3)Predictable Risk

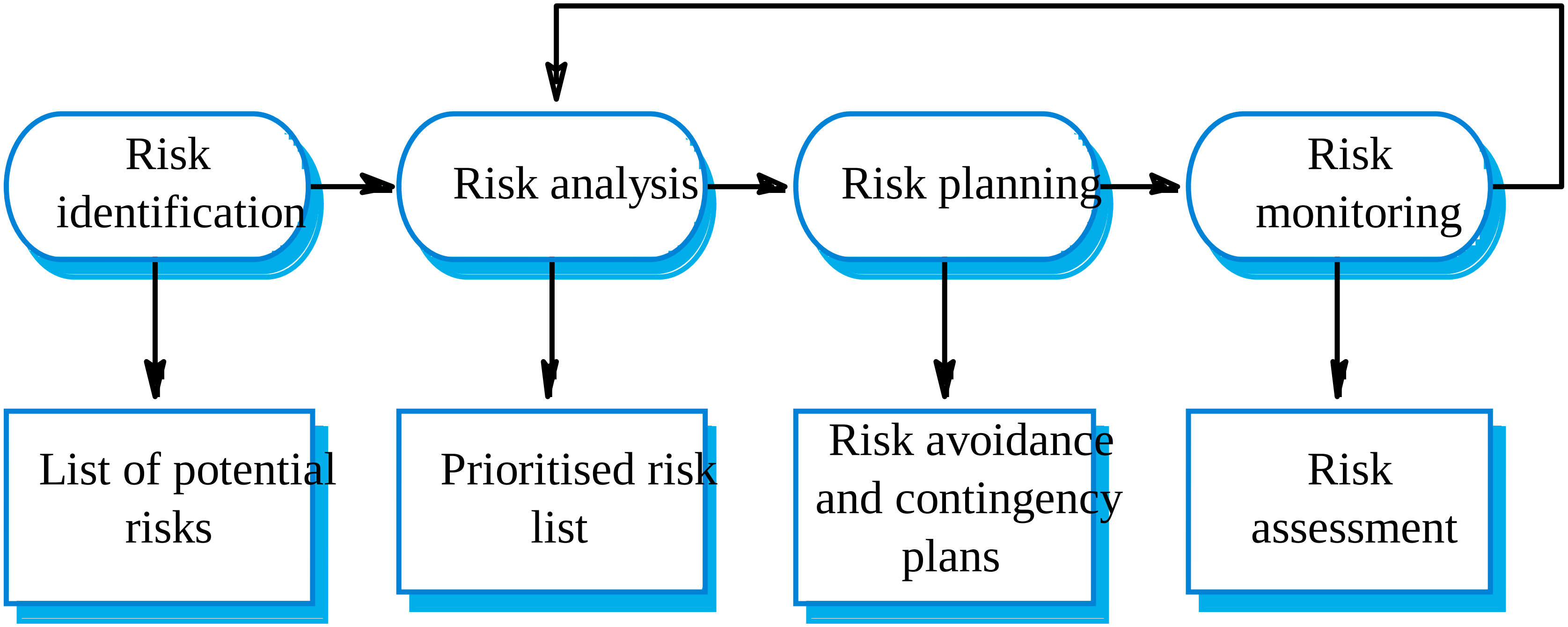
Software Risks

Risk	**Affects**	**Description**
Staff turnover	Project	Experienced staff will leave the project before it is finished.
Management change	Project	There will be a change of organisational management with different priorities.
Hardware unavailability	Project	Hardware that is essential for the project will not be delivered on schedule.
Requirements change	Project and product	There will be a larger number of changes to the requirements than anticipated.
Specification delays	Project and product	Specifications of essential interfaces are not available on schedule
Size underestimate	Project and product	The size of the system has been underestimated.
CASE tool under-performance	Product	CASE tools which support the project do not perform as anticipated
Technology change	Business	The underlying technology on which the system is built is superseded by new technology.
Product competition	Business	A competitive product is marketed before the system is completed.

Risk Management Process

- **Risk identification**
  - Identify project, product and business risks;
- **Risk analysis**
  - Assess the likelihood and consequences of these risks;
- **Risk planning**
  - Draw up plans to avoid or minimise the effects of the risk;
- **Risk monitoring**
  - Monitor the risks throughout the project;

Risk Management Process



Risk Management Strategies

1) Proactive Risk Management
2) Reactive Risk Management (Fire-fighting Mode)

Reactive Risk Management

- Software team does nothing about risks until something goes wrong.
- Then team flies into action in an attempt to correct the problem rapidly. This is called as **“Fire Fighting Mode”**.
- When this fails, **“Crisis Management”** takes over and the project is in real jeopardy.

Proactive Risk Management

- It begins long before technical work is initiated.
- Potential risks are identified, their probability and impacts are assessed and ranked by their importance.
- The software team establishes a plan for managing risk.

Risk Identification

- It is a symmetric attempts to specify threats to the project plan(estimates, schedule, resources, loading).
- By identifying known and predictable risks, the project manager takes a first step toward avoiding them when possible and controlling them when necessary.
- Two types of risks:
  - **Generic Risks** are potential threat to every software project.
  - **Product-specific Risks** can be identified only by those with a clear understanding of the technology, the people and the environment that is specific to the project at hand.
- **Risk item checklist** is one of the method to identify risks. The checklist can be used and focus on some subset of known and predictable risks in generic subcategories.

Generic Subcategories of Risk Item Checklist

1. **Product Size:** Risks associated with the overall size of the software to be built or modified. Some of the questions related with this which need to be answered are as:
   - Estimated size of product in LOC or FP?
   - Degree of confidence in estimated size estimate?
   - Estimated size of product in number of programs, files, transactions?
   - Size of database created or used by the product?
   - Number of users of the product?
   - Percentage deviation in size of product from average for previous products?
   - Number of projected changes to the requirements for the product? (before delivery and after delivery)?
   - Amount of reused software?

Generic Subcategories of Risk Item Checklist

2. **Business Impact:** Risks associated with the constraints imposed by management or the market place. Some of the questions related with this which need to be answered are as:
   - Affect of this product on company revenue?
   - Visibility of this product by senior management?
   - Amount and quality of product documentation that must be produced and delivered to the customer?
   - Governmental constraints on the construction of the product?
   - Costs associated with late delivery?
   - Costs associated with defective delivery?
   - Number of other products/systems with which this product must be interoperable?

Generic Subcategories of Risk Item Checklist

3. **Customer Characteristics:** Risks associated with the sophistication of the customer and the developer’s ability to communicate with the customer in a timely manner. Some of the questions related with this which need to be answered are as:

   - Have you worked with the customer in the past?
   - Does the customer have solid idea of what is required?
   - 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 engineering process?

Generic Subcategories of Risk Item Checklist

4. **Process Definition:** Risks associated with the degree to which the software process has been defined and is followed by the development organization. Some of the questions related with this which need to be answered are as:
   - Has your organization developed a written description of the software process to be used on this project?
   - Are staff members signed-up to the software process as it is documented and willing use it?
   - Is the software process used for other projects?
   - Are formal technical reviews of the requirements specification, design and code conducted regularly?
   - Is a mechanism used for controlling changes to customer requirements that impact the software?

Generic Subcategories of Risk Item Checklist

5. **Development Environment:** Risks associated with the availability and quality of the tools used to build the product. Some of the questions related with this which need to be answered are as:
   - Is a software project management tool available?
   - Is a software process management tool available?
   - Are tools for analysis, design and testing available and appropriate for the product to be built?
   - Are software configuration management tools available?
   - Are all the software tools integrated with one another?
   - Are local experts available to answer questions about the tools?
   - Is on-line help and documentation for the tools adequate?

Generic Subcategories of Risk Item Checklist

6. **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. Some of the questions related with this which need to be answered are as:
   - Is the technology to be built new to your company?
   - Does the software interface with new or unproven hardware?
   - Is a specialized user interface demanded by product requirements?
   - Do requirements put excessive performance constraints on the product?
   - Is the customer uncertain that the functionality requested **“do-able”**.
   - Do requirements demand the use of new analysis, design or testing methods?
   - Do the customer requirements demand the creation of new algorithm, input or output technology?

Generic Subcategories of Risk Item Checklist

7. **Staff size and Experience:** Risks associated with the overall technical and project experience of the software engineers who will do the work. Some of the questions related with this which need to be answered are as:
   - Are the best and enough people available?
   - Do the people have right combination of skills?
   - Are staff committed for entire duration of project?
   - Will some staff be working only part time on this project?
   - Do staff have right expectations about the job at hand?
   - Have staff received necessary training?
   - Will turnover among the staff be low enough to allow continuity?

Assessing overall Project Risk

- The following questions have derived from risk data obtained by surveying experienced software project managers.
  - Have top software and customer managers formally committed to support the project?
  - Are end-users enthusiastically committed to the project and the system/product to be built?
  - Are requirements fully understood by the software engineering team and their customers?
  - Have customers been involved fully in definition of requirements?
  - Do end-users have realistic expectations?
  - Is project scope stable?
  - Does the software engineering team have the right mix of skills?
  - Are project requirements stable?

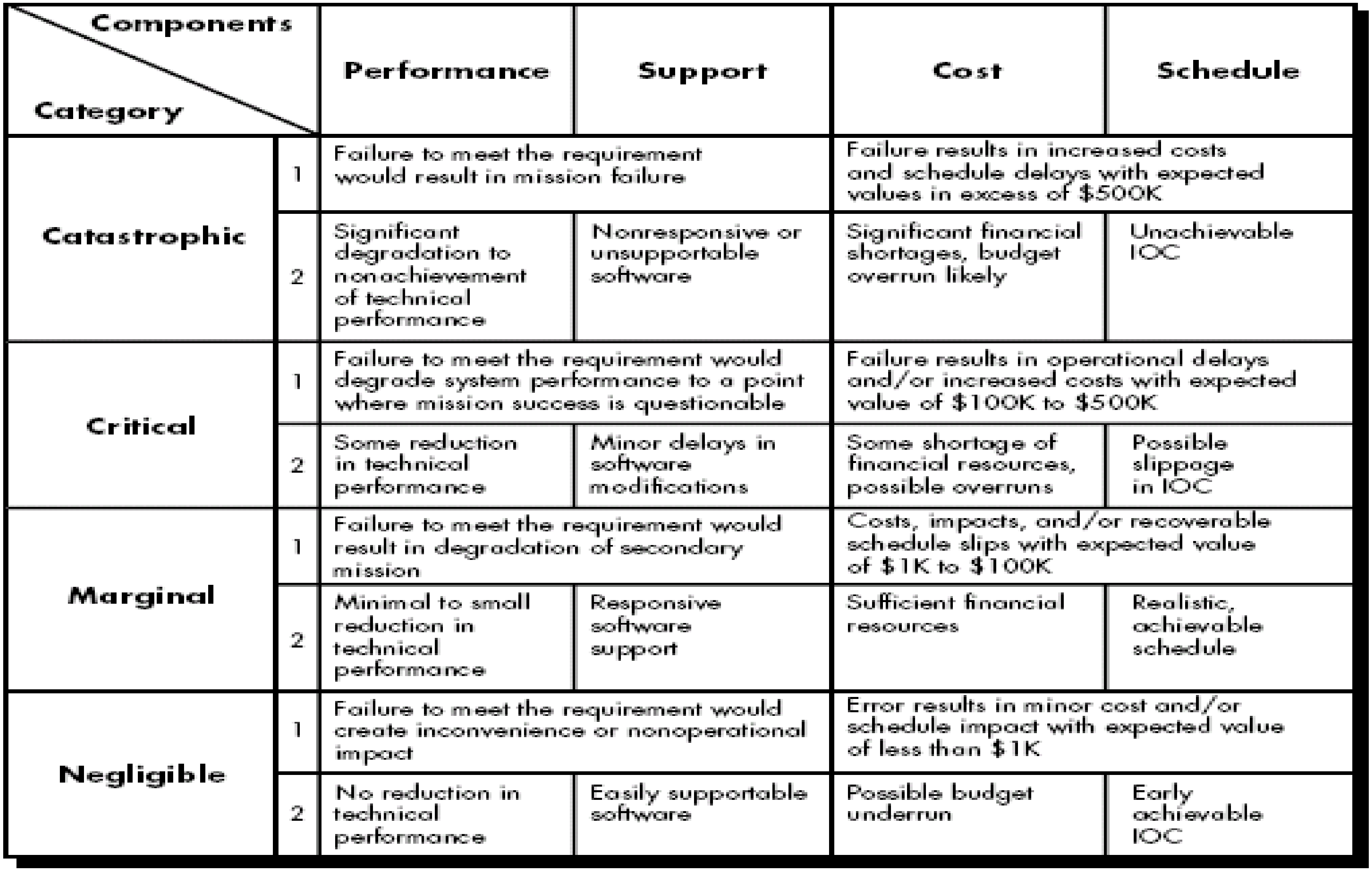
Assessing overall Project Risk

- Does the project team have experience with the technology to be implemented?
- Is the number of people on the team adequate to do the job?
- Do all customer/user constituencies agree on the importance of the project and on the requirements for the system/product to be built.

- If anyone of these questions is answered negatively, Mitigation, Monitoring and Management steps should be initiated without fail.
- The degree to which the project is at risk is directly proportional to the number of negative responses to these questions.

Risk Components and Drivers

- **Performance Risk:** The degree of uncertainty that the product will **meet its requirements** and be fit for its intended use.
- **Cost Risk:** The degree of uncertainty that the **project budget** will be maintained.
- **Support Risk:** The degree of uncertainty that the resultant software will be easy to **correct, adapt and enhance.**
- **Schedule Risk:** The degree of uncertainty that the project **schedule will be maintained** and that the product will be **delivered on time**.
- The impact of each risk driver on the risk component is divided into one of four impact categories: negligible, marginal, critical or catastrophic.

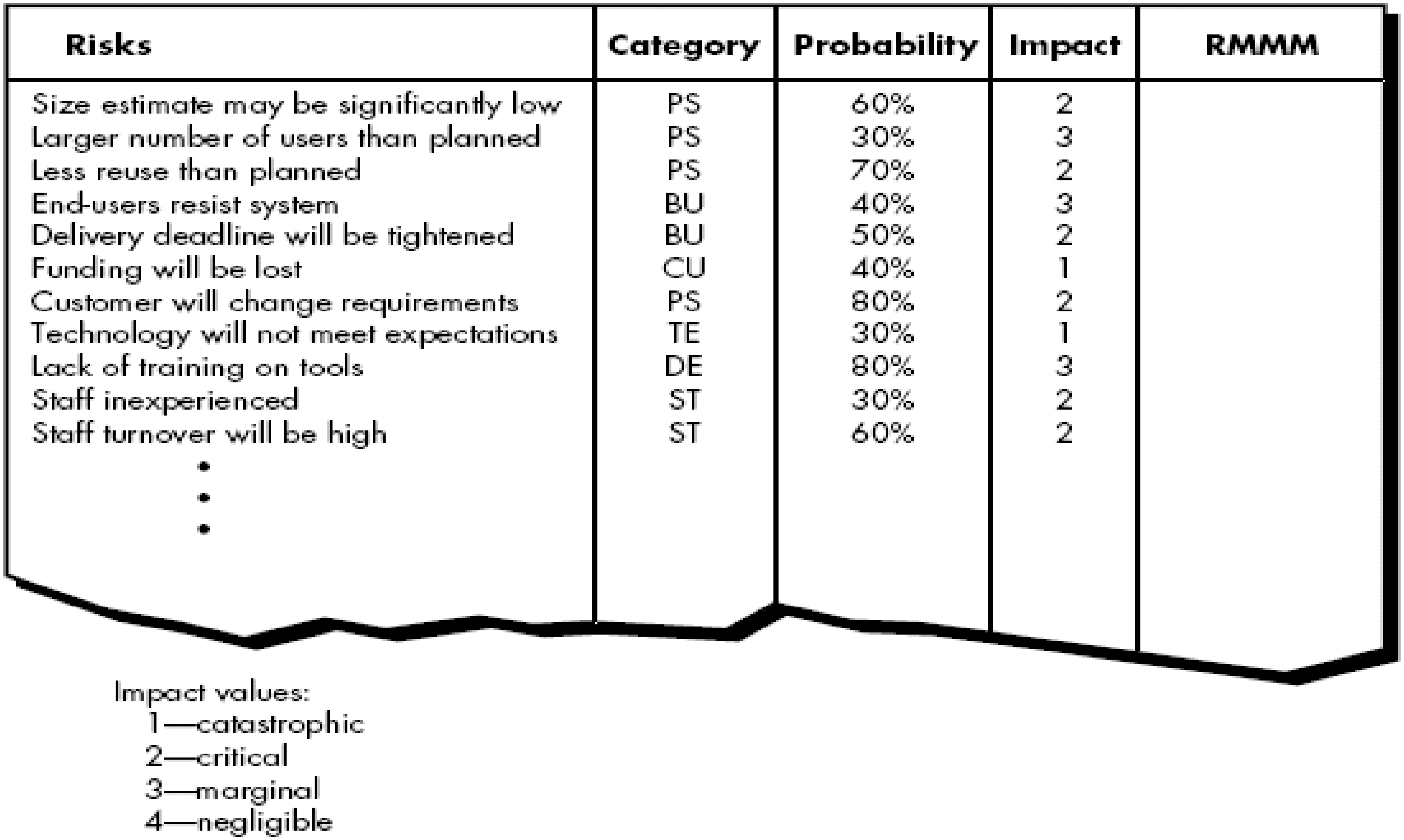


Components / Category		Performance	Support	Cost	Schedule
Catastrophic	1	Failure to meet the requirement would result in mission failure		Failure results in increased costs and schedule delays with expected values in excess of $500K	
	2	Significant degradation to nonachievement of technical performance	Nonresponsive or unsupportable software	Significant financial shortages, budget overrun likely	Unachievable IOC
Critical	1	Failure to meet the requirement would degrade system performance to a point where mission success is questionable		Failure results in operational delays and/or increased costs with expected value of $100K to $500K	
	2	Some reduction in technical performance	Minor delays in software modifications	Some shortage of financial resources, possible overruns	Possible slippage in IOC
Marginal	1	Failure to meet the requirement would result in degradation of secondary mission		Costs, impacts, and/or recoverable schedule slips with expected value of $1K to $100K	
	2	Minimal to small reduction in technical performance	Responsive software support	Sufficient financial resources	Realistic, achievable schedule
Negligible	1	Failure to meet the requirement would create inconvenience or nonoperational impact		Error results in minor cost and/or schedule impact with expected value of less than $1K	
	2	No reduction in technical performance	Easily supportable software	Possible budget underrun	Early achievable IOC

Risk Projection

- Also called risk estimation, attempts to rate each risk in two ways –
  - The **likelihood** or **probability** that risk is real.
  - The **consequences** of the problem associated with the risk, should it occur.**(Loss)**
- The project planner along with other team managers performs four risk projection activities:
  - **Establish a scale** that reflects the perceived likelihood of a risk.
  - **Delineate the consequences** of the risk.
  - **Estimate the impact** of the risk on the project and the product.
  - Note the overall **accuracy of the risk projection** so that there will be no misunderstandings.

Developing a Risk Table



Risks	Category	Probability	Impact	RMMM
Size estimate may be significantly low	PS	60%	2	
Larger number of users than planned	PS	30%	3	
Less reuse than planned	PS	70%	2	
End-users resist system	BU	40%	3	
Delivery deadline will be tightened	BU	50%	2	
Funding will be lost	CU	40%	1	
Customer will change requirements	PS	80%	2	
Technology will not meet expectations	TE	30%	1	
Lack of training on tools	DE	80%	3	
Staff inexperienced	ST	30%	2	
Staff turnover will be high	ST	60%	2	
• • •				

Impact values:
1—catastrophic
2—critical
3—marginal
4—negligible

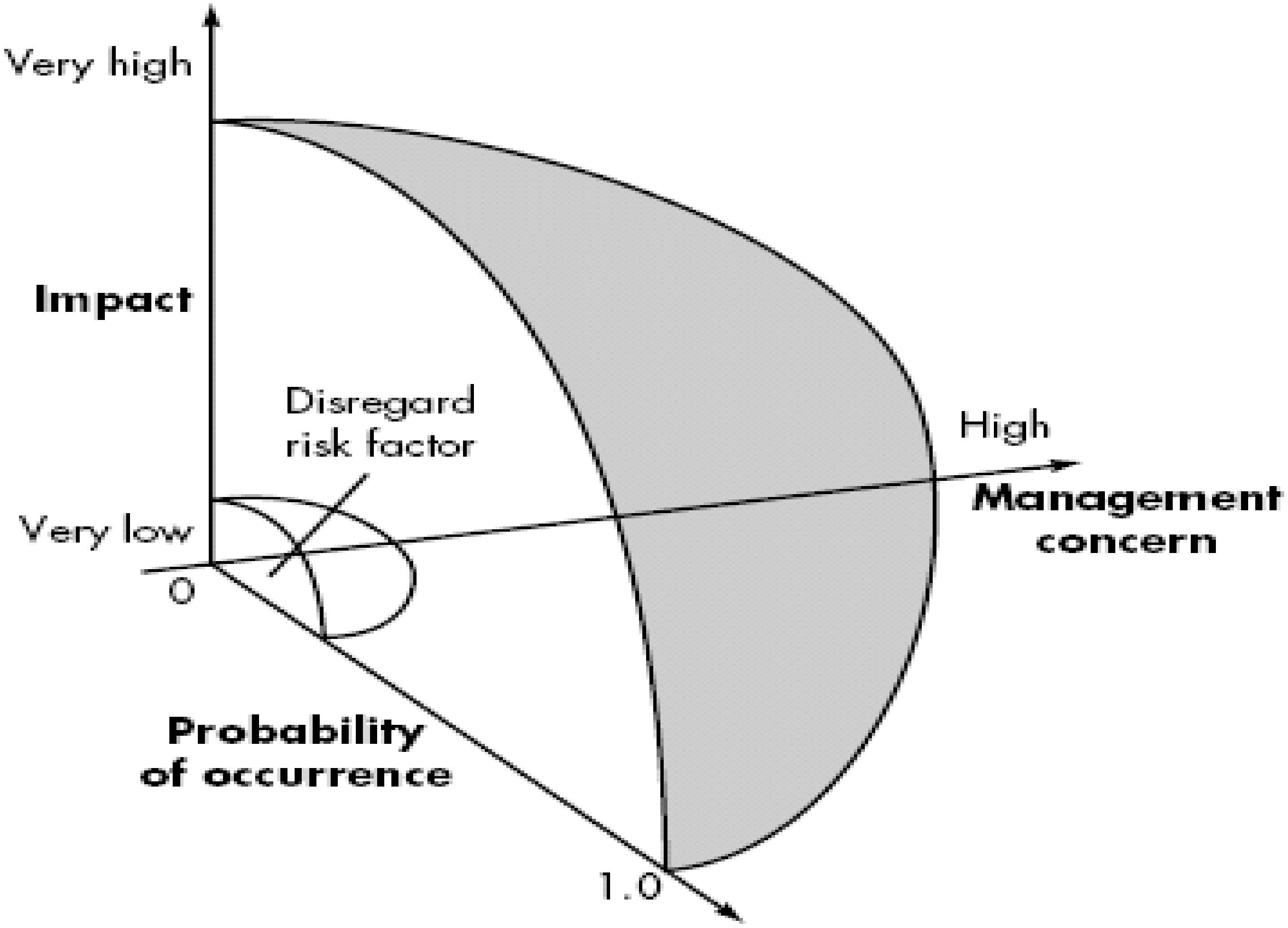
Developing a Risk Table

- Listing all risks in first column. This can be accomplished with the help of the risk item checklists.
- Each risk is categorized in the second column.
- The **probability** of occurrence of each risk is entered in the next column of the table which can be estimated by team members.
- Impact of each risk is assessed. Each ***risk component*** is assessed using the characterization and an impact categories like ***catastrophic***, ***critical***, ***marginal*** *and* ***negligible*** are determined.
- Once table is completed, manger will give order of prioritization to the risk. Therefore, the table is sorted by probability and by impact.
- High-probability, high-impact risks get into the top of the table, and low-probability risks drop to the bottom. (First order prioritization).

Developing a Risk Table

- The project manager studies the resultant sorted table and defines a **cutoff line** risks that lie above the line will be given further attention. Risks that fall below the line are considered as second-order prioritization.
- Risk impact and probability have a distinct influence on management concern.
- Risk factor that has a high impact but a very low probability of occurrence then management will give little attention or some time no attention.
- But if risk factor that has high impact and high probability of occurrence then management will give high attention.
- All risks that lie above the cutoff line must be managed and specify in last column of the table under RMMM column.

Developing a Risk Table



Assessing Risk Impact

- Three factors affect the consequences that are likely if a risk does occur:
  - **Nature,**
  - **Scope, and**
  - **Timing.**
- The nature of the risk indicates the problems that are likely if it occurs.
  - For example, a technical risk, development environment change
- The scope of a risk combines the strictness with its overall distribution.
  - For ex. how much of the project will be affected or how many customers are harmed?
- The timing of a risk considers when and for how long the impact will be felt.

To determine the overall consequences of a risk:

- Determine the average probability of occurrence value for each risk component.
- Determine the impact for each component based on the criteria.
- Complete the risk table and analyze the results as described

Now measure, Risk exposure (RE).

$$RE = P \times C$$

W here ***P*** is the **probability of occurrence for a risk** and ***C*** is the **cost of the project.**

Example- the software team defining a project risk

- **Risk Identification** - Only 70% of the software components scheduled for reuse and remaining functionality will have to be custom developed.
- **Risk probability.** 80% (likely).
- **Risk Impact** – Assume total no. of component is 60. If only 70% can be used, 18 components would have to be developed from scratch.
- Since the average component is *100**LOC*** and local data indicate that the software engineering cost for each LOC is $14.00,
- The overall cost (impact) to develop the components would be 18 x 100 x 14 = $25,200.
- **Risk exposure.** *RE* = 0.80 x 25,200 ~ $20,200.

Example- the software team defining a project risk

- Once an estimate of the cost of the risk is derived, compute ***RE*** for each risk in risk table.
- The total risk exposure for all risks (above the cutoff in the risk table) can provide a means for adjusting the final cost estimate for a project.
- The project team should revisit the risk table at regular intervals, re-evaluating each risk to determine when new circumstances cause its probability and impact to change.
- As a consequence of this activity, it may be necessary to add new risks to the table, remove some risks that are no longer relevant, and change the relative positions of still others.
- *Compare* ***RE*** *for all risks to the cost estimate for the project. If* ***RE>50%*** *of project cost, the feasibility of the project must be evaluated*

Risk Assessment

- In the risk management process, a set of triplets have been established:

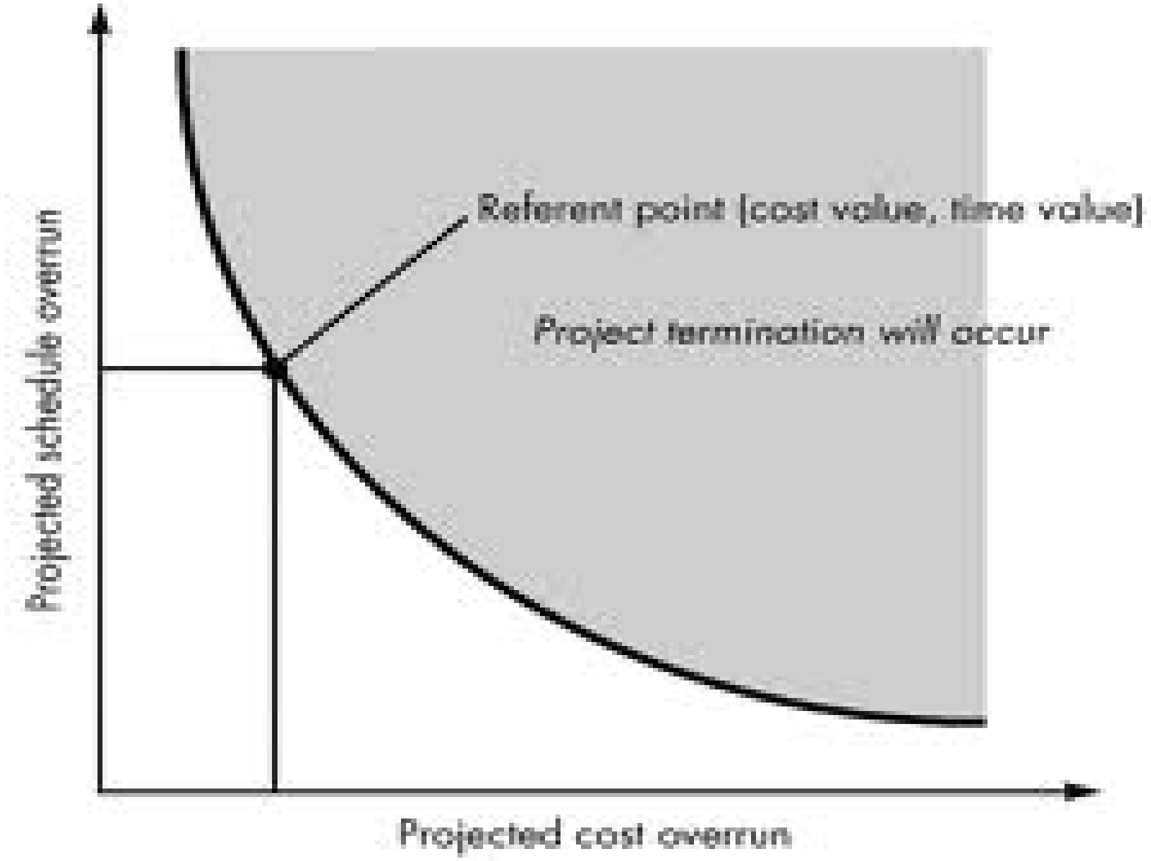
  $$[r_i, l_i, x_i]$$

  where $\boldsymbol{r_i}$ is risk, $\boldsymbol{l_i}$ is likelihood (probability of the risk), $\boldsymbol{x_i}$ is the impact of the risk.
- In the context of software risk analysis, a risk referent level has a single point called the **referent point** or **break point** at which the decision to proceed with the project or terminate it are equally weighted.

Risk Assessment

- During risk assessment, following steps are performed:
  - Define the risk referent levels for the project.
  - Attempt to develop a relationship between each [r_i, l_i, x_i] and each of the referent levels.
  - Predict the set of referent points that define a region of termination bounded by a curve or areas of uncertainty.
  - Try to predict how compound combinations of risks will affect a referent level.

Risk Assessment



Risk Referent Level

Risk Control

- Risk assessment is a passive activity identifying the risks and their impacts, risk control comprises active measures that are taken by project management to minimize the impact of risks.

- Though risk assessment is primarily done during project planning as risk assessment in early stages is most important, like cost and schedule estimation, the assessment should be evaluated and changed, if needed, throughout the project.

Risk Control

- Like any active task (e.g., **configuration management, development**), ***risk control*** starts with ***risk management planning***. Plans are developed for each identified risk that needs to be controlled.
- Many risks might be combined together for the purposes of planning, if they require similar treatment. This activity, like other planning activities, is done during the project initiation phase.
- Risk control has 3 categories :
  - **Risk avoidance(mitigation)**
  - **Risk monitoring**
  - **Risk management**

Risk Mitigation, Monitoring and Management (RMMM)

- A basic risk management plan has five components:
  - Why the risk is important and why it should be managed?
  - What should be delivered regarding risk management and when?
  - Who is responsible for performing the different risk management activities?
  - How will the risk be abated or the approach be taken?
  - How many resources needed?

Risk Mitigation, Monitoring and Management (RMMM)

- **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?

Risk Mitigation

- Meet with current staff to determine causes for turnover (e.g., poor working conditions, low pay, competitive job market).
- Mitigate those causes that are under our control before the project starts.
- Once the project commences, assume turnover will occur and develop techniques to ensure continuity when people leave.
- Organize project teams so that information about each development activity is widely dispersed.
- Define documentation standards and establish mechanisms to be sure that documents are developed in a timely manner.
- Assign a backup staff member for every critical technologist.

Risk Monitoring

- The project manager monitors factors that may provide an indication of whether the risk is becoming more or less likely.
  - General attitude of team members based on project pressures.
  - The degree to which the team has jelled.
  - Interpersonal relationships among team members.
  - Potential problems with compensation and benefits.
  - The availability of jobs within the company and outside it.

Risk Management and Contingency Plan

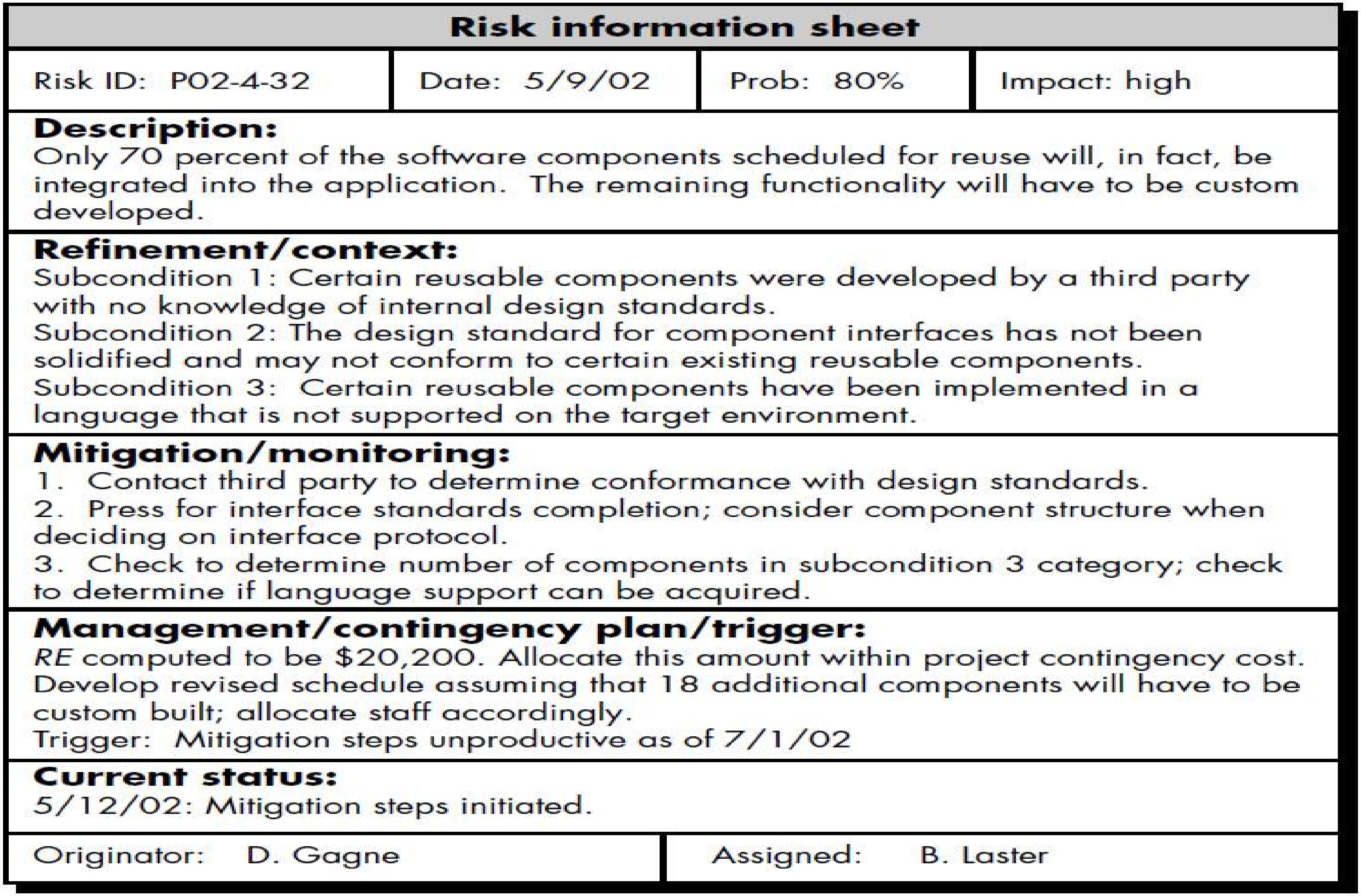
- It assumes that mitigation efforts have failed and that the risk has become a reality.

  Eg – A project is proceeding well and a number of people announce their leaving. If the mitigation strategy have been followed, backup is available, information is documented and knowledge has been dispersed across the team. The project manager may temporarily refocus resources(and readjust the project schedule) to those functions that are fully staffed, enabling newcomers who must be added to the team to **"get-up to speed"**. Those individuals who are leaving are asked to stop all work and spend their last weeks in **"knowledge transfer mode"**. This might include video-based knowledge capture, the development of **"commentary documents"** and/or meeting with other team members who will remain on the project.

RMMM Plan

- It documents all work performed as part of risk analysis and is used by the Project Manager as part of the overall project plan.
- Alternatively, each risk is documented individually using a **Risk Information Sheet**(RIS).

Risk Management and Contingency Plan



Risk information sheet

Risk ID: P02-4-32	Date: 5/9/02	Prob: 80%	Impact: high

Description:
Only 70 percent of the software components scheduled for reuse will, in fact, be integrated into the application. The remaining functionality will have to be custom developed.

Refinement/context:
Subcondition 1: Certain reusable components were developed by a third party with no knowledge of internal design standards.
Subcondition 2: The design standard for component interfaces has not been solidified and may not conform to certain existing reusable components.
Subcondition 3: Certain reusable components have been implemented in a language that is not supported on the target environment.

Mitigation/monitoring:
1. Contact third party to determine conformance with design standards.
2. Press for interface standards completion; consider component structure when deciding on interface protocol.
3. Check to determine number of components in subcondition 3 category; check to determine if language support can be acquired.

Management/contingency plan/trigger:
RE computed to be $20,200. Allocate this amount within project contingency cost. Develop revised schedule assuming that 18 additional components will have to be custom built; allocate staff accordingly.
Trigger: Mitigation steps unproductive as of 7/1/02

Current status:
5/12/02: Mitigation steps initiated.

Originator: D. Gagne	Assigned: B. Laster