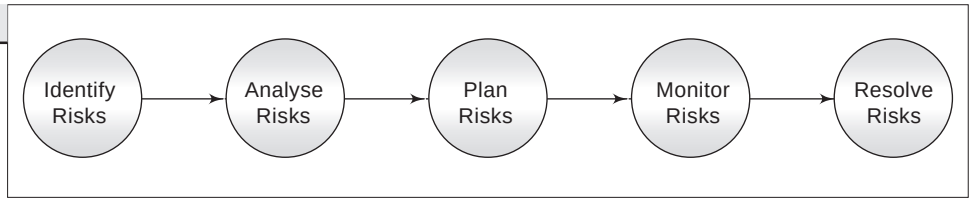
3.3 SOFTWARE RISK MANAGEMENT (SRM)

SRM is a process built in five steps. The steps are:

• Identify • Analyse • Plan • Track • Resolve

The process is continuous in nature and handled dynamically throughout lifecycle of development. Figure 3.2 shows the SRM process model.

Fig. 3.2 *SRM Process Model*



3.3.1 Identify Risks

Risk identification is a process to handle certain inputs that produce a set of outputs, namely, a list of risks, their types and its importance in the context of the software proposed to be developed.

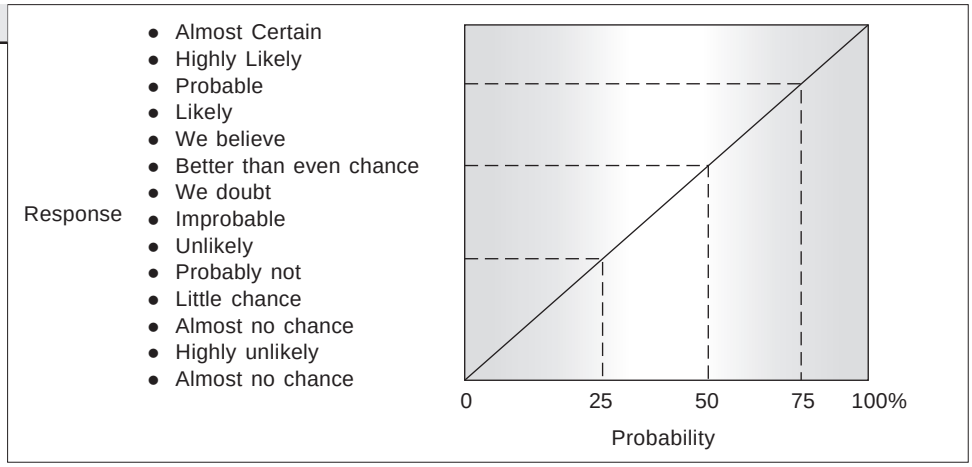
The inputs are the degree of uncertainty on a number of features such as requirements, technology, people allocation, insufficient domain and application knowledge, concerns about lack of skills and knowhow, and issues regarding the technical and commercial aspects of the software development. These inputs help to identify the risks and their nature. In order to ensure that risk identification is complete, organisations develop checklists that are used to identify the risks. Mature organisations also maintain a risk database if they handle a number of small and large software development projects. The checklists, risk database, and risk assessment forms are the facilitation in the identification process. The inputs mentioned so far are external, arising out of software development proposals. The other set of inputs that help to identify and to some extent assess the risk are proposed resource allocations based on the software requirement specifications.

The risk identification process begins with an assessment using the checklists. The assessment is best done when it is conducted as a participatory activity. The risk analyst conducts interviews with experienced personnel who have worked earlier in similar software projects. Periodic meetings are conducted with persons to identify the risk. It should be noted that risk identification is not a one-time task undertaken at the beginning of the life cycle; it is an exercise that continues till the software is delivered satisfactorily. Some risks, which were not perceived in first review, may emerge later in the life cycle.

Once the risk is identified, its attributes, that is, the probability of occurrence and the loss arising out of risk are determined. Both these attributes are based on the subjective judgement of the concerned people. This judgement may be supported by risk database and the experience of people in the field. The loss may not be monetary, but could emerge in the form of adverse effects on software quality, which includes features like flexibility, maintainability, portability, reliability, reusability and so on.

The Defence Systems Management College (DSMC), Fort Belvoir, VA, USA, provides a scale guideline to fix the probability of occurrence based on the response the risk analyst would get in interviews and in review meetings. Figure 3.3 shows the suggested probability against the response to various questions.

Fig. 3.3 *Response versus Probability of Risk Occurrence*



The risk identification process not only identifies the risk but also determines attributes and communicates further to people in the team. The key to successful identification process is the use of checklists. One can use safely the SEI Software Risk Taxonomy as shown in Table 3.3. The SEI risk taxonomy is a structured checklist that organises known risks to specific element attributes. The taxonomy is divided into three parts, namely, product engineering, development environment and program constraints. Further, each part is subdivided into components. Each of these components is discussed for identification of an attribute determination. This exercise gives rise to a list of risk statements with contextual information and details of identification. For example, the risk analyst will discuss **'stability'** of requirements, **suitability** of development process and **personnel** in terms of availability, capability and maturity.

3.3.2 Analyse and Assess Risk

Risk Analysis (RA) is a process that defines activities and methods to estimate and evaluate risk. In estimation, the probability of occurrence is estimated and its consequence. In evaluation, the risk options against certain criteria are discussed.

The risk analysis process begins with list of risks obtained from the earlier process of risk identification. Each risk from this list is taken for estimation and evaluation. To act on this step, the organisation needs an evaluation criteria and the risk database. First, the probability and consequence is estimated and then the Risk Exposure (RE) determined.

Risk Exposure = Probability × Loss

For example, the customer environment suggests that the stability of requirement specification is very low. This is also the experience of the project team with

Table 3.3

SEI Software Risk Taxonomy

Product engineering	*Development environment*	*Program constraints*
1. Requirements	**1. Development Process**	**1. Resources**
a. Stability	a. Formality	a. Schedule
b. Completeness	b. Suitability	b. Staff
c. Clarity	c. Process control	c. Budget
d. Validity	d. Familiarity	d. Facilities
e. Feasibility	e. Product control	**2. Contract**
f. Precedent	**2. Development system**	a. Type of contract
g. Scale	a. Capacity	b. Restrictions
2. Design	b. Suitability	c. Dependencies
a. Functionality	c. Usability	**3. Project Interfaces**
b. Difficulty	d. Familiarity	a. Customer
c. Interfaces	e. Reliability	b. Associate Contractors
d. Performance	f. System support	c. Subcontractors
e. Testability	g. Deliverability	d. Prime contractor
f. Hardware constraints	**3. Management Process**	e. Corporate Management
g. Non developmental software	a. Planning	f. Vendors
3. Code and Unit Test	b. Project organisation	g. Statutory Bodies
a. Feasibility	c. Management experience	
b. Unit test	d. Project Interfaces	
c. Coding/ implementation	**4. Management Methods**	
4. Integration and Test	a. Monitoring	
a. Environment	b. Personnel management	
b. Product	c. Quality assurance	
c. System	d. Configuration management	
5. Engineering Specialities	**5. Work Environment**	
a. Maintainability	a. Quality attitude	
b. Reliability	b. Co-operation	
c. Safety	c. Communication	
d. Security	d. Morale	
e. Human factors		
f. Specifications		

this particular customer. Hence, identified risk, a critical requirement may be missing or may change radically. Based on the risk database and customer experience, probability is 0.50. The loss due to this risk occurrence is a waste of three man-month effort, amounting to a loss of Rs. 1.5 lakhs. Hence, risk exposure is

$$RE = 0.50 \times 1.5 = 0.75 \text{ lakhs}$$

Based on this criteria of risk exposure, it is determined whether it is low, Moderate or high and considered against the time frame as short, medium and long term. Both these attributes are evaluated on common criteria known as risk severity. Table 3.4 shows the index of risk severity.

Table 3.4

Risk Severity by Risk Exposure and Time Frame

Time Frame	*Risk Exposure*		
	Low	*Moderate*	*High*
Short	5	2	[1]
Medium	[7]	4	3
Long	9	8	6

Source: *Software Risk Management* by Ellan H. Hall

Based on the risk severity criteria, the risks are prioritised for action. Index '1' for a short-term time frame and high-risk exposure is considered the highest risk severity. Index '9' is termed as the lowest because of the low exposure and long-term time frame. When you evaluate all risks by these criteria, they come under a common platform, irrespective of whether the risk is of project, product or process.

At the end of risk analysis, you get a prioritised risk list with probability, risk exposure, and risk severity. This forms the basis for constructing a risk action plan for resolution.

3.3.3 Plan Risk

The risk plan proposes various actions to deal with the risks identified and analysed in the earlier processes. The output of the process is the Risk Action Plan (RAP).

RAP takes as input the Prioritised Risk List based on risk severity, and determines resolution strategies for each one on the list. The risk resolution strategies suggested by Ellan H. Hall a researcher and author of the book on Risk management are

- Risk Acceptance
- Risk Avoidance
- Risk Protection
- Risk Reduction
- Risk Research
- Risk Reserves
- Risk Transfer

- **Risk Acceptance:** This strategy is chosen when you have no choice but to live with risk and face the consequences.
- **Risk Avoidance:** This strategy is chosen to eliminate risk altogether or bypass it altogether. This strategy is chosen when you are in lose-lose situation. You will deal with the sources of risk to avoid or eliminate them by management actions.
- **Risk Protection:** This strategy is chosen when there is a possibility to reduce the probability of occurrence and the consequential loss. For example, you may hire a temporary consultant to provide domain knowledge support or the skills required to reduce process delay and product risk.
- **Risk Reduction:** This strategy is chosen over and above risk protection. Based on a cost-benefit analysis, the organisation may take such actions that risk incidence is reduced, giving rise to major reduction in the consequential loss.
- **Risk Research:** This strategy is chosen to reduce the risk by seeking more information about it for better evaluation, and also to deal with it effectively. The firm may, for example, conduct a proof of concept exercise or experiment to reduce the volatility of the requirement specifications. Another example is that the organisation may seek more information from genuine resources on new products or the introduction of new technology. Based on this information, the index of severity will be reduced, and the action plan changed accordingly.
- **Risk Reserves:** This strategy is chosen when the risk severity is low but risk acceptance' is not possible. You build a contingency plan to deal with this risk, in case risk occurs. You may provide extra slack in schedule, keep a reserve on call, reserve funds in case required.
- **Risk Transfer:** This strategy is chosen when it is possible to transfer the risk to somebody else. You may choose outsourcing, subcontracting, buying a resource or tool as a risk transfer strategy.

Though the strategies discussed are six, they can be subsumed under three basic goals about the risk, as shown in Fig. 3.4.

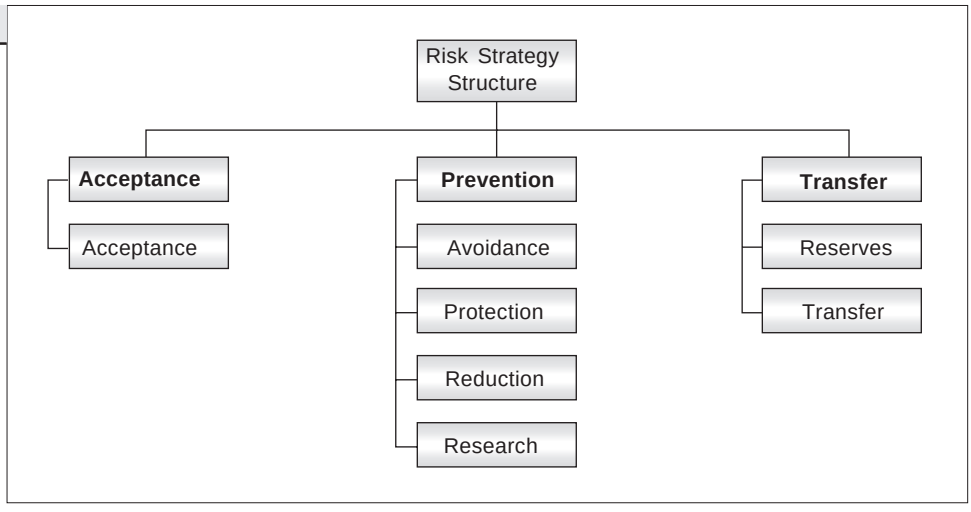


Fig. 3.4

Risk Strategy Structure

Based on these strategies, a more concrete Risk Management action plan is designed for execution.

3.3.4 Track Risk

The risk tracking process monitors risk occurrence, consequence, and exposure and provides triggers to act to resolve the risk. The tracking process provides methods to keep watch on various activities that are likely to be affected by the risk. These methods provide feedback on occurrence and impact, and trigger the predetermined action. The tracking process will have a threshold norm for each risk beyond which the trigger will generate the action to resolve the risk by changing strategy or executing the proposed plan of action. The threshold could be risk exposure or risk severity.

The process has an input on risk status from the project team and from various MIS reports on software development addressing the issues of schedule, cost, delivery and quality. The output of the tracking process is evaluation of exposure, severity and triggers to act where necessary.

For example, risk of delay in delivery is a high severity risk. Assume that over 100 activities are involved which affects the delivery. So, threshold for these activities is a delay of 15% in completion. If delay exceeds 15% it should be reported through MIS for action.

It is important to note that risk occurrence is a possibility at any time. The original estimates and forecasts on occurrence, exposure, timing may change during the life cycle, and tracking risk becomes an essential activity in risk management system, and has to be made7 integrated activity in software development plan.

3.3.5 Resolve Risk

Risk resolution process is defined where risk action plan forms the basis for resolving the risk using resolution tools and techniques and risk database. The objective of the process is to reduce the risk to level of acceptable risk. The output of the risk resolution process is list of acceptable Risk, Reduced rework and corrective actions.

Risk resolution activities are

- Act on the trigger.
- Execute the risk action plan.
- Monitor the action plan and assess the new risk scenario.
- Control the risk exposure through action, and/or action on deviation.

The skills required to resolve risk are creativity and collaboration. Effective implementation of risk action plan calls for generation of new and innovative ideas. This calls for creativity in the project team. Further, the risk action plan implementation is not straight linear action process by an individual. It is a collaborative process, and not a process implementation in isolation. The fundamental risk resolution strategy is to reduce uncertainty, gain additional knowledge and draw upon the experience of others from internal and external sources.

Resolution of risk is not a structured method but a process where creativity and collaboration of team members are key success factors. Table 3.5 gives summary of the steps in the Risk Resolution Process (RRP).

Table 3.5

RRP, Inputs and Outputs

Process steps	*Inputs*	*Outputs*
Identify Risk	Uncertainty, lack of knowledge, concerns, issues, risk database	List of risk by category class, type and context
Analyse Risk and Assess	List of risks, risk database	Risk list with probability, loss, exposure, severity and prioritised risk list
Plan Risk for Resolution	Prioritised risk list determining resolution strategies, and its implementations	Risk action plan i.e. conversion of strategy into concrete steps for action
Track Risk	Risk status through MIS, risk thresholds	Emergence of threshold deviation, triggers to act measures and metrics on to update risk database
Resolve Risk	Risk action plan and use of tools and techniques	Changing risk scenarios into acceptable risk and reduce risk exposure.