

Chapter 1

Risk Culture

1.1 Risk Thinking

What makes us think of risks? Is it backward thinking or forward thinking? Will it allow us to grow and progress or slow us down? Such questions confront us when we think of risk management. In growth-oriented management cultures of the past, negative aspects were not mentioned. The drive was to reach out and move ahead. In those days, to reflect upon failure was a sign of weakness. The entrepreneur was a go-getter who crossed all barriers and achieved.

Thinking about failure came into management paradigms through different avenues. First, the market demanded fail-safe products. The product developer was forced to look at failure possibilities and come up with a robust design. He struggled to remove what we refer to today as “[product risks](#).” The discipline of technology management accepted risk thinking rather elegantly. It made sense to product developers to design a product with minimum risks for the user. The success of risk management in product development also fuelled technological progress and expansion. To identify product risks, a fuller and more mature technical knowledge was required. It was not a smooth beginning. Although designers enjoyed the creative pleasures and excitement of design, they disliked risk analysis of their products. In due course, product risk analysis was accepted by the industry.

Second, for finance management, risk became an investment question. Credit risk was studied, defined, and measured religiously in finance institutions. Variation in ROI was a measure of risk, striking a sympathetic chord with the age-old concept that “variation is trouble.”

Third, risk considerations became an integral part of project management. Project managers (PMs) saw risk more clearly than anybody else. Projects were clearly risky. Building a dam in a jungle involved risks of all kinds. Constructing an underwater oil line also entailed huge risks. In such cases, a project was synonymous with risks. Managing a project implied living with risks around the clock.

All these influences have finally touched software project management. We all know that projects are associated with risks. Today, risk thinking is a part of software project life and is a basic step for project survival. Modernism in management manifests as “failure thinking,” or predating failure probabilities in endeavors, and a freedom to communicate potential failures to stakeholders, without fear of being misread. This new culture accommodates risk thinking.

1.2 What Is Risk?

The original meaning of risk is associated with gambling — to risk is to gamble. When we take risks, there is a chance of gaining and perhaps an equal chance of losing.

Uncertainty in business ventures has come to be known as risk. Every business venture is basically risky. In new business ventures and new product development, there are unknown factors and their impacts on the venture are equally unknown. The unknown factors could be favorable or unfavorable. There is a probability that one may either gain or lose. However, a loss may hurt the venture. Most business ventures like to assess the probability of loss and compare it with the probability of gain. The decision to go ahead depends on whether the odds are favorable or unfavorable. Risk is the probability of suffering loss. Using this approach, the business house will not pursue a venture that has a risk probability greater than 49 percent. The odds must be in favor of winning the gamble, even though the tilt is marginal.

Definition 1.1: Risk is the probability of suffering loss.

A refinement of this definition is to include goals, gains, or opportunities in the statement. Perhaps it is implied and obvious that risks are connected with gains. Nevertheless, if risks are divorced from the associated goals, then one sees just a set of problems. A risk list should not be reduced to a problem list. Risks have a much broader role to play.

Definition 1.2: Risk is the probability of suffering loss while pursuing goals.

Then there is the consideration of the magnitude of harm from the risk. What will its impact be? The consequence of the risk is evaluated. If the harm is tolerable but the gains are attractive, new decision rules emerge. One may even take a risk where the occurrence probability is greater than 50 percent. The threshold is not 49 percent. Risk is seen as a weighed parameter. The weight is based on the magnitude of loss due to risk, if the risk ever occurs. Risk is defined as the combination of probability of occurrence and the magnitude of loss it causes. This combination is also known as risk exposure.

Definition 1.3: Risk is the combination of probability and magnitude of loss.

Currently, risk is defined and measured using Definition 1.3. Measurement of risk is often a subjective process. Both the probability and loss are measured using linguistic measures such as “high,” “medium,” and “low.” What matters is not just the risk, but its intensity, measured as risk exposure. Will the risk occur? What will the harm be? These are more significant questions than, “What is the risk?”

A clarification is due at this juncture. If loss occurs because of factors within our control, it is not considered as a risk. Factors beyond our control give rise to risk. This is the general perception that makes risk management simple. Internal factors are within our control. Hence, only external factors that contribute to loss, which are not under our direct control, qualify as risk factors. When this notion prevailed, people believed that they had not caused the risks.

Sometimes, processes are not in control and results are not predictable or what were intended. Such losses become risks. In this case, the origin is not the criterion — predictability and control are important factors. Hence, a complete risk definition would be:

Definition 1.4: Risk is the probability of suffering loss while pursuing goals due to factors that are unpredictable or beyond.

1.3 A Boundary Problem

What is risk? The answer to this question depends on who answers it and the boundaries the individual establishes around himself or herself. If the answer comes from someone who is responsible for all processes within the boundary, a clear answer can be expected. Risk is obvious when people own their processes. The owner is anxious about resources being well spent and not wasted, and that the results are acceptable. He wants

to maximize the chance of success and looks for clues to act upon. In other words, the owner deliberately sees risks and responds to them. If he grows nonchalant and detached, he does not see many risks or does not feel like acting upon them. When nonowners see risks and communicate them to those who run the process, the result is conflict.

Risk arises from factors beyond our control. A designer may consider requirement analysis as a source of risk because it is external to him and he is not sure whether the analysis results will be communicated completely and correctly. This is a “dependency risk.” A boundary is drawn around the process, and risks that threaten the process from across the boundary are seen. Risk perception has a built-in boundary perception. Risk definition has meaning only with reference to this boundary.

Within the process owner’s boundary, a problem is not immediately seen as a risk, even if it happens to be vague and uncertain. The propensity is to assign the problem to process control and process management.

Across the boundary, the propensities change. A process owner has no influence beyond his boundary. Neighboring processes are alien and appear to be sources of risk. Problems tend to get labeled as risks.

When the boss of the SBU (strategic business unit) looks at the same risk from a larger perspective, the risk looks smaller and local. The risk appears to have occurred due to lack of cooperation between two process owners. He does not want to think of this local issue as a major risk, as things can improve through better management. If provoked, he may term this an internal risk that can be solved by taking internal measures. The SBU boss realizes that the better the management, the fewer the internal risks.

There are some sensitive internal conditions, such as when a PM chooses to run a project without adequate resources and authority. The processes have weaknesses that are well known to the stakeholders. Process weaknesses are potential breeding grounds for risks. But he may not have the resources, power, and influence to improve process capabilities. All he can do is mitigate the harmful effects, promote awareness of the risks, and prepare contingency plans. Risks have a different connotation in this case.

It is important to define internal risks, because they contribute to more than 65 percent of risks in a typical business environment.

Internal risks are solved by internal response plans. Most internal risks evoke short-term plans that operate within the life of the project. These are dependency risks that are solved by better coordination and risk communication. Some internal risks arise because of lack of process capability. There is no quick solution to such problems. This calls for a well-designed process improvement plan. The nature of improvement can be a series of continual improvements or kaizens, or a major breakthrough

improvement of the Six Sigma style. Such improvements require more resources and time.

Yet another type of internal risk is seen on comparing growth objectives with current performance levels. Today is fine, but tomorrow may bring hurdles. Perception of such risks comes from long-term vision. If growth goals are taken seriously, one finds more risks. If growth goals are taken as secondary concerns, one does not see risks. The architects of the organization detect growth-related risks.

When an organization is divided, more boundaries appear and employees see more internal risks. When the organization is integrated, internal risks are called process management issues. In an integrated organization with boundaries, collaborative efforts make up for weaknesses and create an organizational capability that is greater than the sum of individual process capabilities. In fragmented organizations, risks multiply. An organization without boundaries has the least possible number of internal risks.

Definition 1.5: Internal risk is the probability of suffering losses while pursuing performance and growth goals because of inadequacies in process capability (including core and support processes) and organizational structure.

Beyond the organizational boundary, however, things are different. External conditions are beyond our control. There are risk factors beyond our sphere of influence. Competitors cut prices and marketing times almost ruthlessly. Social forces may erode staff loyalty. The PM sees external risks as threats and develops strategies to deal with them.

Definition 1.6: External risk is the probability of suffering loss while pursuing performance and growth goals because of uncertainties in external conditions.

There cannot be a better example of external risk than requirements. The requirements keep changing; they “creep.” The volatility of requirements is a perennial source of uncertainty and, hence, risk. Requirements go through a metamorphosis, becoming bigger and clearer in each phase of their evolution. Requirement evolution is a subject for continuous observation and modeling. Requirement volatility is beyond our control and is uncertain. Change is inevitable and is beyond prediction. When the requirement risk occurs, it can cause numerous problems for the project. Managers are aware of this. They cannot avoid it, but are prepared. Those who have mastered this risk experience fewer surprises when requirements change.

1.4 Expressing Risk: The Basic Terms

A culture is propagated by words. Risk culture also thrives on clear definitions of risk terms. Some terms used to describe risks are:

Risk ID	A unique reference number given to each risk for traceability.
Risk probability	The probability of risk occurrence.
Risk impact	The level of damage if risk occurs.
Risk exposure	The combination of risk probability and risk impact.
Risk origin	Source of risk (internal or external).
Risk category	A group or class with a set of similar risks.
Risk owner	Process owner whose objectives are likely to be harmed by risk.

1.4.1 *Additional Terms*

The preceding list is arbitrary and may be updated. Cost and causes of risks can be added to the minimum list. Several attributes can also be used to describe risk in more detail. Risk expression is enabled by a risk classification system, which defines all the perceived attributes of risks.

1.5 Risk Vocabulary

In building a risk culture, it is essential to share the glossary with all decision makers and achieve common terms of reference. Terms that may be used to build a risk culture are listed in the following text. Each organization should define them in a way that makes sense to it. These terms may be common and have obvious meanings. But defining the meaning in plain language will avoid differences in interpretation. Such differences, even if they are small, have been known to create conflict and disagreement during implementation of risk mitigation plans.

Here are some key terms that need definition for clear understanding and usage:

- Risk
- Risk identification
- Risk analysis
- Risk tracking
- Risk ranking
- Risk mitigation plan
- Risk contingency plan
- Risk prevention plan

Risk escalation
Risk elevation
Risk acceptance
Risk avoidance
Risk transfer

Additional terms are given in the **glossary**. Each organization should publish its own definitions of these terms and make them known to all stakeholders.

Publish a glossary of risk terms in your organization to support your risk management practices.

1.6 Risk-Driven Project Management

1.6.1 *Project Visibility*

Risks eclipse all projects, more so in the case of software projects. Projects with abstract work products and intangible results are particularly vulnerable to risks. As good road visibility prevents accidents, visibility in projects reduces risks. Process maturity improves visibility and minimizes risks.

1.6.2 *Goal Setting*

Every goal is shadowed by risks. When we define goals, we must recognize these risks. Risk perception enhances goal clarity. Seeking great opportunities that others have missed entails taking risks others have not taken. The aggressive pursuit of aspirations embodies aggressive risk taking. Building capability reduces risk. When we are knowledgeable, risks are less. Lack of information and knowledge breeds risk. The entrepreneur takes risks, and risk culture is another term for the entrepreneurial spirit. Successful entrepreneurs have their business sense and their sixth sense tuned up to perceive risks and deal with them.

Figure 1.1 presents a risk–gain grid. All projects occupy positions in this grid. By understanding where the project milestones sit on this grid, the PM can set practical goals.

1.6.3 *Product Development*

Product development companies are paranoid about risk. The stakes and investments are huge, and several risks threaten the product before it hits the market. Products may be scrapped prior to release because the market

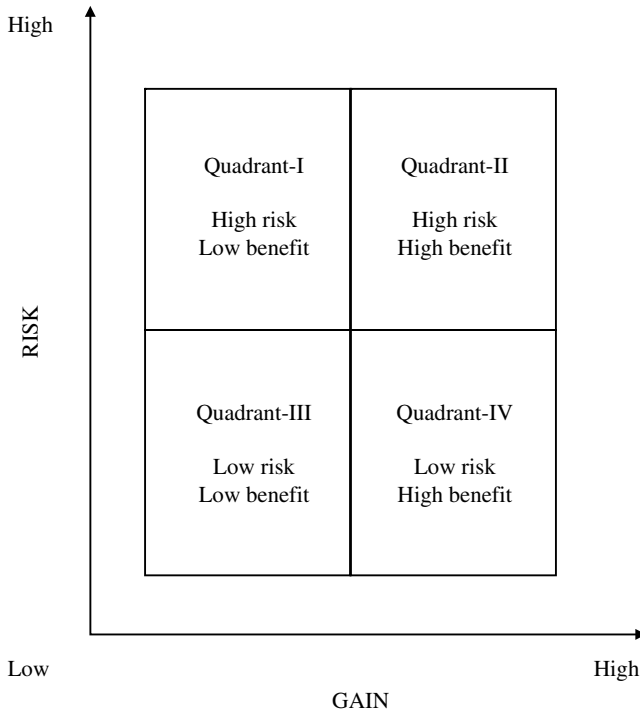


Figure 1.1 Risks versus benefits.

for them has disappeared or because of lack of the right people to maintain the products. When competitors launch products ahead of us, we feel that we have lost time, and with it, the race. Such risks are not always predictable. Risks are carefully examined at every milestone in product development environments.

1.6.4 *Development*

In software development projects, risk-driven approaches are known to pay rich dividends. Phase-end risk reviews and appropriate responses enable projects to sail smoothly. Risks are seen as roadblocks and barriers, and diversions are taken to reach project objectives. The project team looks at risks and treats them. They are told to watch out for risks, handle them, or escalate the risk upward for higher-level involvement.

A few software development methods have admirable inherent risk treatment abilities. The evolutionary development model exposes risks

clearly at every increment. The project reviews at these increments are ideally suited to detecting risks and acting upon them. Natural risk detection is superior to forced risk detection. Another life-cycle model worth considering from a risk point of view is the agile process. Certain types of risks melt in the face of organic communication methods in the agile process. For example, the ubiquitous dependency risks are weakened by the communication speeds of agile development.

1.6.5 Maintenance

Maintenance projects need risk management. Some maintenance projects go through routine and repetitive bug-fixing cycles. They can use operational risk management concepts. Risk management reduces the cycle time and customer satisfaction is improved. Some maintenance projects deal with enhancements. Uncontrolled enhancements blow up all expectations and precipitate a lot of risks. Instead of life-cycle-based risk approaches, calendar-based regular risk reviews are useful in maintenance projects.

1.6.6 Supply Chain

In Time and Material (T&M) projects, where the customer manages the project execution, most risks appear to be external. The customer selects the process flow and the customer's processes establish a master-slave relationship with the supplier's processes. Risk perception may not be on the agenda or a part of the contract. Nevertheless, the supplier may look at risks and report them to the customer. This risk communication from supplier to customer in T&M projects is often a turbulent path if the customer does not want the supplier to think beyond the contractual boundary.

The end user is likely to see both the supplier and customer as a single entity. As the customer pays for services, he eventually "owns" the risks in the supply chain.

Definition 1.7: Supply-chain risk is the cumulative probability of suffering loss injected by all steps in the supply chain, irrespective of differences in business ownership.

The supply chain is a system and risks must be treated in a similar manner. It profits little to divide the system and take a fragmented view of risks. A new organizational culture is needed to achieve this mature view of risks.

1.7 Controlling the Process, Environment, and Risk

1.7.1 Process Management and Risk Management

Business results are achieved by processes, most of which are well defined. But the process environment is not well defined. In some ways, it may seem that well-defined processes are managed by process management, and an ill-defined environment is managed by risk management. Any ambiguities and uncertainties present in processes also get lumped under the banner of risk management. The two initiatives go well together.

1.7.2 SPC and Risk

It is beneficial to consider statistical process control (SPC) and compare it with risk perception. They are both attempts to keep the house in order. SPC scans internal processes, whereas risk perception scans even the external world. SPC thrives on feedback, whereas benefits from risks are obtained by “feed”–“Forward.” SPC is reactive, whereas risk-driven efforts are proactive. Sometimes the difference between these tends to blur, especially when one looks at internal risks. An SPC chart finds anomalies in process behavior. The SPC system detects defects and statistical outliers. The outlier events earn z scores, which are probabilistic judgments. In such pronouncements, SPC detects process risk from historical data. Risk management may use historical data to detect process tendencies that may fail. But risk mitigation is not a corrective action for existing problems; it is a proactive control of future problems.

1.7.3 Five S and Risk

It is important to remember that risk perception is based on vision and calls for unflinching foresight. The Japanese Five S methodology demands that we keep both the mind and environment in order. Cleanliness in Five S is kept at a high level, and disorder is detected instantly. The effect of the environment on both the psychological and physical aspects is the theme behind Five S. Quintessential risk control requires controlling the risk environment. Disorder in the environment, both internal and external, is detected by the risk identifier.

To see risks in perspective, one must clearly distinguish between defects, issues, and risks. Defects are the results of mistakes and are found by inspection, testing, and analysis. Issues are discrepancies between planned and actual results, and are found out by reviews. Risks are futuristic problems that may either materialize or melt away with time. When risks are solved, defects and issues decrease.

Definition 1.8: Defects, issues, and risks have something in common: they are all problems and disorders. But there is a major difference: defects and issues are historic, things of the past, whereas risks are futuristic.

1.7.4 Defect Prevention and Risk Management

There are remarkable similarities between defect prevention and risk management practices. Both aim to prevent trouble and result in a problem-solving cycle. Both have similar challenges in detection and response. Defect prevention ensures product health. Risk management ensures a clean process environment and attacks the root causes behind defects. Understanding the connection between these two great innovations has a beneficial influence on taking risk decisions.

1.8 Maturity in Risk Culture

As the risk culture matures, the paradigm shifts. Previously known and imminent risks are attacked, as in crisis management. With experience, internal risks are mitigated. After the house is in reasonable order, the external risks are engaged. Then project-level risk management is supported by enterprise risk management. The larger problems are solved using long-term strategies. This is the time when risks are exploited. As risks are solved, the associated opportunities are seen with clarity and pursued with added focus.

When risk perception is respected, there are many risk owners. These employees own the risks because risks affect their goals and objectives. They do not shun risks but welcome risk discovery and appreciate its positive aspects.

Decision analysis practitioners take risk analysis in their stride. All decision analysis methods consider risk and payoffs in decision alternatives and allow the decision maker to make optimum choices. The decision analysts examine risks in a scientific manner. They value risk perception as a way to make the right choice. To take a decision is to choose among risks. They choose the least harmful option and acknowledge the fact that risks prevail in the real world.

When the organization matures and possesses prediction models, risk forecasting becomes an obvious output. Such models are not only used to predict the steady state-values of processes but also to simulate dynamic variations and risks. All estimation models are potential risk forecasters.

The growth architects of an organization cautiously hunt for opportunities. Their caution is actually risk perception. Soon the employees realize

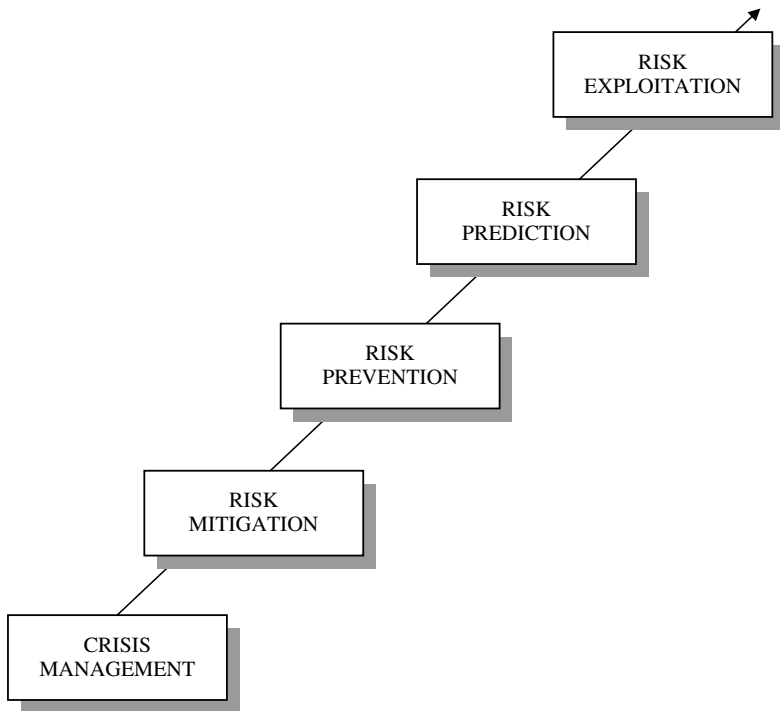


Figure 1.2 Maturity phases of risk management culture.

that perceiving and responding to risks will pave the foundation for growth. An organization that does not see risks is blind. An organization that does not respond to risks is dead.

Figure 1.2 shows a popular maturity model for risk management. As the organization achieves capability, the risk response shows progress that is continual but subtle. Here is a list of risk-response types, illustrating a progression in risk management:

- Risk mitigation
- Risk prevention
- Risk prediction
- Risk exploitation

Mature risk cultures imbibe an ability in project teams to perceive and solve risks with speed and energy. The mature teams make detailed project plans and map risks to subtle shifts in microlevel tasks; thus, they are able to detect risk symptoms at the task level and predict risk early in the project. The frequent sharing of risk information, exchange of successes and failures in risk mitigation, and a frequently visited common risk repository all have

RISK NAME	CHANCE (P)	IMPACT (I)	EXPOSURE (P) × (I)

Figure 1.3 Risk exposure table.

one significant consequence: the mature project team cultivates a sixth sense for risk from the continual corroboration of risk data and assimilation of risk practices. Risk culture fills gaps in the risk management process, makes the project team vigilant well beyond the scope of defined processes, equips people with an organic power to detect and solve problems posed by risks, and empowers processes with an everlasting vision and energy to hunt for risks. Although, most risk management processes are capable of dealing with known risks, a risk culture has the power to see unknown risks. When it comes to project survival in the midst of catastrophic risks, one relies more on risk culture than on defined processes. Risk culture, which is the accumulation of risk practices, experiences, and practical wisdom, is a worthy complement to defined risk management processes. Maturity involves years of practice and mastery over risk management processes.

1.9 Risk Scale

Is there a scale for risk, like the scales for measuring temperature or earthquake intensity? Is there a similar universal risk scale? This must be considered very carefully as wrong risk scales can misguide project teams.

It is common to measure the risk exposure number (REN) for every identified risk, and to use the REN as a scale. This is a good place to begin the game of risk evaluation. REN aims to bring as much objectivity as possible to risk perception.

Before using REN as a risk scale, REN should be used for risk expression in the format given in Figure 1.3.

RISK EXPOSURE					
LEVEL : 0 SENIOR MANAGER					
RISK	PROBABILITY	LOSS	RISK EXPOSURE	REN	RE %
PRICE CUT	9	6	54	54	43.37
ORDER CANCEL	2	10	20	74	59.44
REVIEW FAILURE	4	4	16	90	72.29
WRONG REQ	2	5	10	100	80.32
ATTR	1	9	9	109	87.55
DEFECT LEAKAGE	6	3	9	118	94.78
DEL SLIP PENALTY	1	5	5	123	98.80
TECH CHANGE	.05	3	1.5	124.5	100.00

Figure 1.4 Risk exposure numbers — senior manager level.

The four columns in the format are risk name, chance, impact, and exposure.

Defining these four attributes has subjective differences that affect the REN scale. If different people identify risks, it is likely that each will come out with a different judgment of REN. The REN scale is subjective and local. Within a project, the REN scale can have a closed set of meanings, whereas the REN scale may not be consistent across projects. Publishing guidelines on rating risk chances and impact reduces the problem of inconsistency to some extent.

1.9.1 Case Study

1.9.1.1 Background Data

Project teams have learned to use REN as a working scale and derive benefits from it.

In Figure 1.4, risk assessment by a senior manager is presented in the REN format.

In Figure 1.5, risk assessment by a test engineer is given in the same format.

These two are risk assessments from the same organization.

1.9.1.2 Comments

The total REN value in the first assessment is 124.5. In the second assessment, it is 253. Can we conclude that the test engineer finds risks which score 253 on the REN scale, whereas the senior manager’s risk score is 124.5? Does the test engineer estimate double the risk intensity compared to a senior manager? We cannot say that with confidence. The two are looking at different levels of risk and perhaps address different dimensions of the problem.

RISK EXPOSURE					
LEVEL : 4 TEST ENGINEERS					
RISK	PROBABILITY	LOSS	RISK EXPOSURE	REN	RE %
TIME SQUEEZE	10	9	90	90	35.57
LACK OF DOM K	7	6	42	132	52.17
OVER LOAD	9	4	36	168	66.40
REQ NOT CLEAR	3	10	30	198	78.26
DISTRACTION	5	5	25	223	88.14
HLD AMBIGUITY	2	7	14	237	93.68
LACK OF TOOLS	2	5	10	247	97.63
POOR TC REV	3	2	6	253	100.00

Figure 1.5 Risk exposure numbers — engineer level.

But within the risk set identified by the test engineer, the REN score can be used to rank the risks with confidence. The absolute numerical values may not be an accurate universal expression of risk intensity, but the relative order is trustworthy.

The REN scale is used to rank risks.

1.9.1.3 What Do We Learn from This Example?

1. The example shows the differences in risk pictures drawn by people playing different roles. There is a need to register risks from different perspectives.
2. The REN format serves multiple purposes. It helps in risk communication and analysis.
3. The REN scale for measuring risks is not universal. Without calibration, this scale cannot be used to estimate absolute magnitudes for risk intensity.
4. In spite of this shortcoming, the REN scale provides an adequate basis for ranking risks.

1.10 Preparing for Risk

1.10.1 People

If you are starting a risk management system for the first time, then you have to prepare the organization for risk management. This is what culture building is all about. Make sure that all decision makers have a common

definition of risk and will interpret the meaning in an identical manner. Prepare a list of decision makers, as given here:

- Directors
- Senior managers
- PMs
- Project leaders
- Team leaders
- Engineers

Begin the preparation with a human resources list and organization structure. Study who should contribute to risk management, and how. Make sure you have not missed any decision maker.

1.10.2 Communication

The preceding list refers to the risk owners in your organization. They are also the decision makers. Prepare risk management guidelines and circulate them. Make sure all the identified decision makers have a common understanding of the following:

- Risk glossary
- Risk management
- Risk management benefits
- Distinction between risks and defects
- Risk-based project management
- Risk-driven life-cycle management
- Risk-based business planning

Create a Web site and publish this in your organization.

1.10.3 Body of Knowledge

Risk culture is knowledge based. Develop a risk body of knowledge and publish the best practices resulting from risk mitigation.

1.10.4 Metrics

A sound metrics program is of particular support to risk management. Metrics is a system of seeing, observing, and judging. A metrics system is expected to spot trouble in processes and alert the stakeholders. Metrics data could contain risk signals that can be uncovered by analysis.

1.10.5 Estimation Models

Estimation models have a basic potential to predict risks. Collect all the estimation processes that are in circulation and include a risk forecast in the scope of these estimation models and processes.

1.10.6 Detailed Planning

A certain level of depth and detail in planning is an essential “hinterland” for risk management to flourish. Plans provide a neat and clean foil against which risk dots can be seen with ease. Detailed plans provide a clear and noise-free mental landscape that can expose risk for the benefit of the analyst.

1.10.7 Effective Defect Management

To manage risks and unknown problems, we need to be able to manage known problems in projects effectively, namely, defects. If known problems are inadequately controlled, unknown problems are less likely to be addressed. By analogy, techniques used in defect management can be adapted to manage risks. Effective defect management is an inspiration for effective risk management. The economic benefits achieved by defect management will motivate employees to further the gains through risk management.