

# Chapter 35

---

## ■ Risk Management

*Slide Set to accompany*

*Software Engineering: A Practitioner's Approach, 7/e*

**by Roger S. Pressman**

Slides copyright © 1996, 2001, 2005, 2009 by Roger S. Pressman

***For non-profit educational use only***

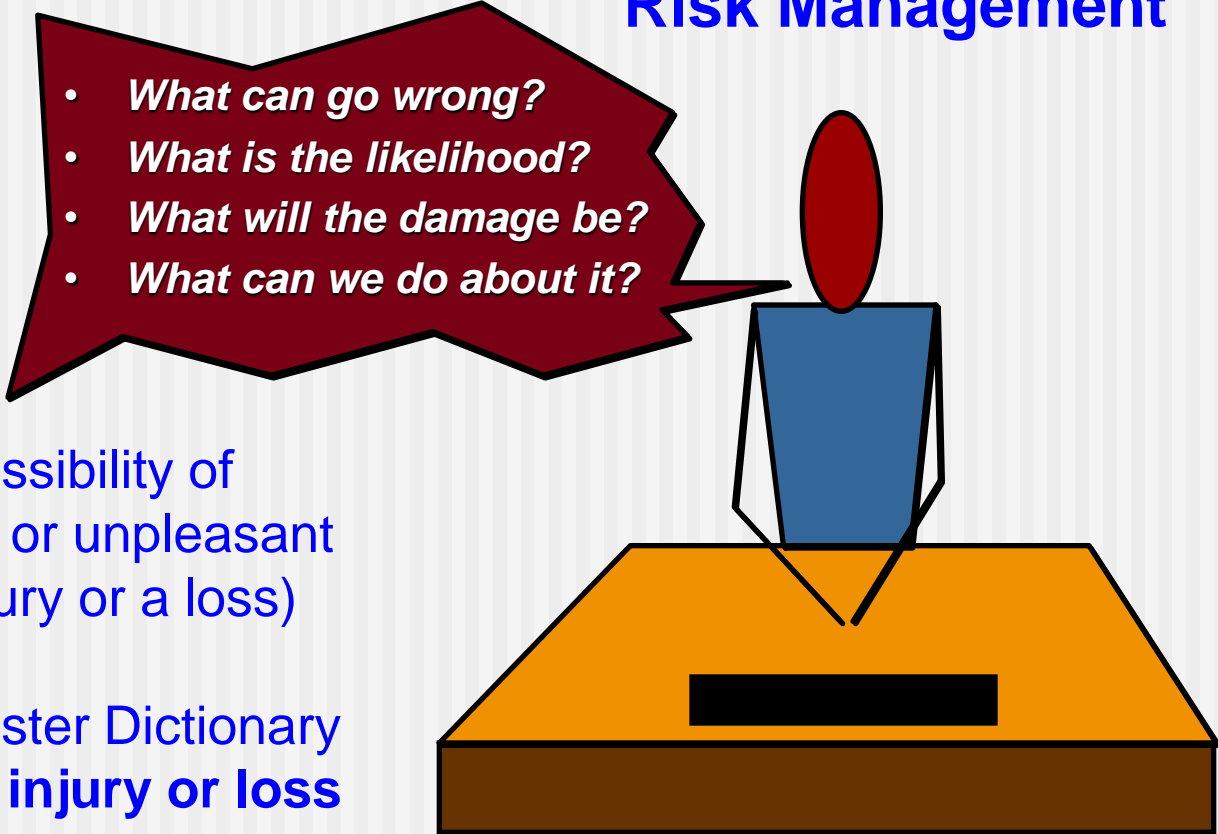
May be reproduced ONLY for student use at the university level when used in conjunction with *Software Engineering: A Practitioner's Approach, 7/e*. Any other reproduction or use is prohibited without the express written permission of the author.

All copyright information MUST appear if these slides are posted on a website for student use.

# Project Risks

---

## Risk Management

- 
- *What can go wrong?*
  - *What is the likelihood?*
  - *What will the damage be?*
  - *What can we do about it?*

**Risk :** “The possibility of something bad or unpleasant (such as an injury or a loss) will happen.”

- Merriam-Webster Dictionary

☛ **NOT actual injury or loss**

# Table of Contents

---

35.1 Reactive vs. Proactive Risk Strategies

35.2 Software Risks

35.3 Risk Identification

35.4 Risk Projection

35.5 Risk Refinement

35.6 Risk Mitigation, Monitoring, and Management

35.7 The RMMM Plan

# 35.1 Reactive vs. Proactive Risk Strategies

---

## Reactive Risk Management

- Project team reacts to risks when they occur
- **Mitigation** — plan for additional resources in anticipation of fire fighting
- **Fix on failure** —resource are found and applied when the risk strikes
- **Crisis management** —failure does not respond to applied resources and project is in jeopardy

# Proactive Risk Management

---

- Formal risk analysis is performed
- Organization corrects the root causes of risk
  - TQM concepts and statistical SQA
  - Examining risk sources that lie beyond the bounds of the software
  - Developing the skill to manage change

# 35.2 Software Risks

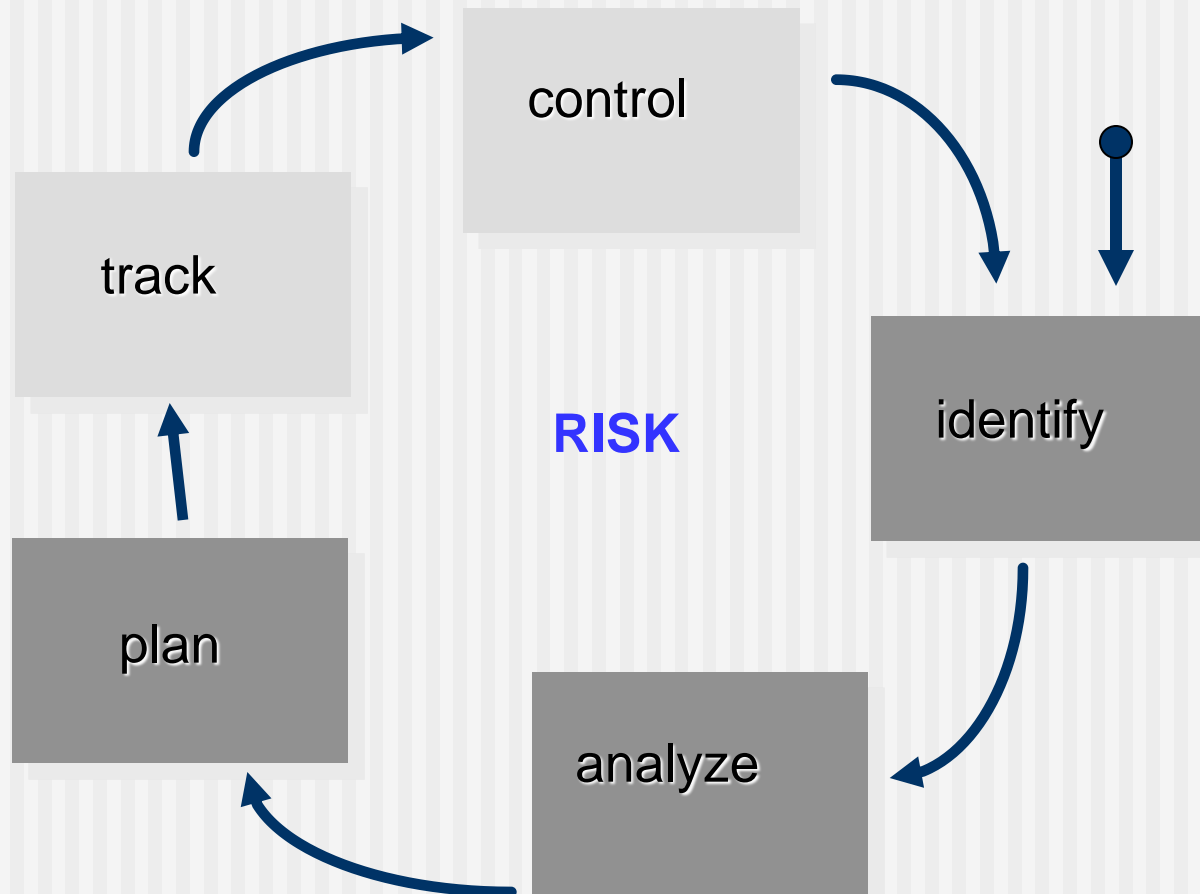
## Seven Principles of Risk Management

---

- **Maintain a global perspective**— view software risks within the context of system and the business problem
- **Take a forward-looking view**— think about the risks that may arise in the future; establish contingency plans
- **Encourage open communication**— if someone states a potential risk, don't discount it.
- **Integrate**— a consideration of risk must be integrated into the software process
- **Emphasize a continuous process**— the team must be vigilant throughout the software process, modifying identified risks as more information is known and adding new ones as better insight is achieved.
- **Develop a shared product vision**— if all stakeholders share the same vision of the software, it likely that better risk identification and assessment will occur.
- **Encourage teamwork**— the talents, skills and knowledge of all stakeholder should be pooled

# Risk Management Paradigm

---



## 35.3 Risk Identification

---

- **Product size** —risks associated with the overall size of the software to be built or modified.
- **Business impact** —risks associated with constraints imposed by management or the marketplace.
- **Customer characteristics** —risks associated with the sophistication of the customer and the developer's ability to communicate with the customer in a timely manner.
- **Process definition** —risks associated with the degree to which the software process has been defined and is followed by the development organization.
- **Development environment** —risks associated with the availability and quality of the tools to be used to build the product.
- **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.
- **Staff size and experience** —risks associated with the overall technical and project experience of the software engineers who will do the work.



## 35.3.1 Assessing Project Risk

---

1. Have top software and customer managers formally committed to support the project?
2. Are end-users enthusiastically committed to the project and the system/product to be built?
3. Are requirements fully understood by the software engineering team and their customers?
4. Have customers been involved fully in the definition of requirements?
5. Do end-users have realistic expectations?

- 
6. Is project scope stable?
  7. Does the software engineering team have the right mix of skills?
  8. Are project requirements stable?
  9. Does the project team have experience with the technology to be implemented?
  10. Is the number of people on the project team adequate to do the job?
  11. Do all customer/user constituencies agree on the importance of the project and on the requirements for the system/product to be built?

## 35.3.2 Risk Components and Drivers

---

- **Cost risk** —the degree of uncertainty that the project budget will be maintained.
- **Schedule risk** —the degree of uncertainty that the project schedule will be maintained and that the product will be delivered on time.
- **Performance risk** —the degree of uncertainty that the product will meet its requirements and be fit for its intended use.
- **Support risk (= Maintenance risk)** —the degree of uncertainty that the resultant software will be easy to correct, adapt, and enhance.

**FIGURE 28.1**

Impact  
assessment.

Source: [Boe89].

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

Drivers

Note: (1) The potential consequence of undetected software errors or faults.

(2) The potential consequence if the desired outcome is not achieved.

IOC: Inversion of Control

## 35.4 Risk Projection

---

- Risk projection, also called risk estimation, attempts to rate each risk in two ways
  - the likelihood or probability that the risk is real
  - the consequences of the problems associated with the risk, should it occur.
- Risk projection steps:
  1. establish a scale that reflects the perceived likelihood of a risk
  2. delineate the consequences of the risk
  3. estimate the impact of the risk on the project and the product,
  4. note the overall accuracy of the risk projection so that there will be no misunderstandings.

## 35.4.1 Developing a Risk Table

---

- Estimate the **probability** of occurrence
- Estimate the **impact** on the project on a scale of 1 to 5, where
  - 1 = low impact on project success
  - 5 = catastrophic impact on project success
- Sort the table by probability and impact  
(=> **Cutoff line**)

# Risk Table

Sample risk  
table prior to  
sorting

Risks	Category	Probability	Impact	RMMM
Size estimate may be significantly low	PS	60%	2	Risk Mitigation, Monitoring and Management
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	
Σ				
Σ				
Σ				

Product Size  
 Business Impact  
 Customer characteristics  
 Development Environment  
 Technology to be built  
 Staff size and experience

## 35.4.2 Assessing Risk Impact

---

### Example

- **Risk identification.** Only 70 % of the software components scheduled for reuse will, in fact, be integrated into the application. The remaining functionality will have to be custom developed.
- **Risk probability.** 80% (likely).
- **Risk impact.** 60 reusable software components were planned. If only 70 % can be used, 18 components would have to be developed from scratch (in addition to other custom software that has been scheduled for development).  
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  
$$18 \times 100 \times 14 = \$25,200.$$



# Risk Exposure

---

The overall **risk exposure, RE**, is determined using the following relationship [Hal98]:

$$RE = P \times C$$

where

**P**: the probability of occurrence for a risk

**C**: the cost to the project (= impact), should the risk occur.

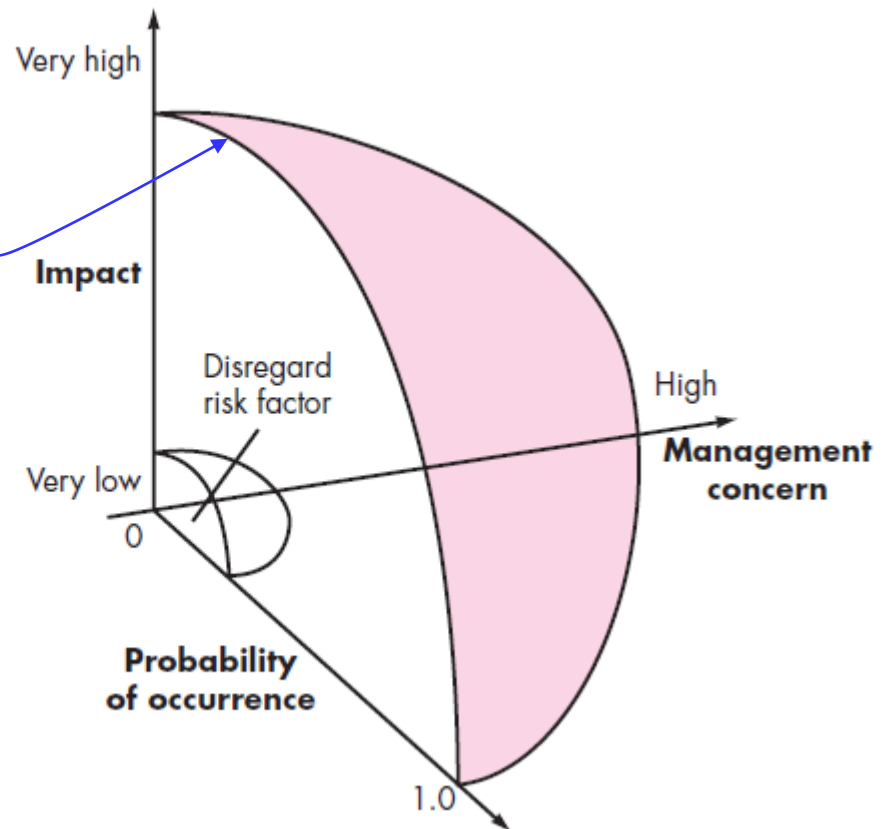
## Example (Continued)

**Risk exposure.**  $RE = 0.80 \times 25,200 \sim \$20,200.$

**FIGURE 28.3**

Risk and  
management  
concern

Cutoff line



# 35.5 Risk Refinement

---

- Represent the risk in **condition-transition-consequence** (CTC) format [Glu94]

*Given that <condition> then there is concern that (possibly) <consequence>*

- Using the CTC format you could rewrite:

"Only 70 % of the software components scheduled for reuse will, in fact, be integrated into the application.

The remaining functionality will have to be custom developed."

=>

"**Given that** all reusable software components must conform to specific design standards and that some do not conform,

**then there is concern that (possibly)** only 70% of the planned reusable modules may actually be integrated into the as-built system,

resulting in the need to custom engineer the remaining 30% of components."

## 35.6 Risk Mitigation, Monitoring and Management

---

- **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 Due to Product Size

---

## Attributes that affect risk:

- Estimated size of the product in LOC or FP?
- Estimated size of product in number of programs, files, transactions?
- Percentage deviation in size of product from average for previous products?
- Size of database created or used by the product?
- Number of users of the product?
- Number of projected changes to the requirements for the product?  
before delivery? after delivery?
- amount of reused software?

# Risk Due to Business Impact

---

## Attributes that affect risk:

- Affect of this product on company revenue?
- Visibility of this product by senior management?
- Reasonableness of delivery deadline?
- Number of customers who will use this product
- Interoperability constraints
- Sophistication of end users?
- Amount and quality of product documentation that must be produced and delivered to the customer?
- Governmental constraints
- Costs associated with late delivery?
- Costs associated with a defective product?

# Risks Due to the Customer

---

## Questions that must be answered:

- Have you worked with the customer in the past?
- Does the customer have a solid idea of requirements?
- Has the customer agreed to spend time with you?
- Is the customer willing to participate in reviews?
- Is the customer technically sophisticated?
- Is the customer willing to let your people do their job — that is, will the customer resist looking over your shoulder during technically detailed work?
- Does the customer understand the software engineering process?

# Risks Due to Process Maturity

---

## Questions that must be answered:

- Have you established a common process framework?
- Is it followed by project teams?
- Do you have management support for software engineering
- Do you have a proactive approach to SQA?
- Do you conduct formal technical reviews?
- Are CASE tools used for analysis, design and testing?
- Are the tools integrated with one another?
- Have document formats been established?



# Technology Risks

---

## Questions that must be answered:

- Is the technology new to your organization?
- Are new algorithms, I/O technology required?
- Is new or unproven hardware involved?
- Does the application interface with new software?
- Is a specialized user interface required?
- Is the application radically different?
- Are you using new software engineering methods?
- Are you using unconventional software development methods, such as formal methods, AI-based approaches, artificial neural networks?
- Are there significant performance constraints?
- Is there doubt the functionality requested is "do-able?"

# Staff/People Risks

---

## Questions that must be answered:

- Are the best people available?
- Does staff have the right skills?
- Are enough people available?
- Are staff committed for entire duration?
- Will some people work part time?
- Do staff have the right expectations?
- Have staff received necessary training?
- Will turnover among staff be low?

# 35.7 The RMMM Plan

## RMMM: Risk Mitigation, Monitoring and Management

Risk information sheet.  
Source: [Wil97].

Risk information sheet			
Risk ID: P02-4-32	Date: 5/9/09	Prob: 80%	Impact: high
<b>Description:</b> 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.			
<b>Refinement/context:</b> 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.			
<b>Mitigation/monitoring:</b> 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.			
<b>Management/contingency plan/trigger:</b> <u>RE</u> 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 7/1/09.			
<b>Current status:</b> 5/12/09: Mitigation steps initiated.			
Originator: D. Gagne		Assigned: B. Laster	