



BAIT3153 Software and  
Project Management (SPM)

---

# Risk Management

## Chapter 5

---



# Table of Contents

---

- 5.1 Introduction**
- 5.2 Risk Management Processes**
- 5.3 Risk Management Planning**
- 5.4 Risk Identification**
- 5.5 Risk Projection**
- 5.6 Risk Refinement**
- 5.7 Risk Mitigation, Monitoring, & Management (RMMM)**
- 5.8 Safety Risks and Hazards**

# 5.1 Introduction

---

## ➤ What is Risk?

- *An uncertain event or condition that, if it occurs, has a positive or negative effect on a project's objectives*

- A risk is something that you would prefer not to have happen

➤ **Project risk management** is the art and science of identifying, assigning, and responding to risk throughout the life of a project in the best interests of meeting project objectives

✓ Involves understanding potential problems that might occur on the project and how they might impede project success.

✓ **The goal of project risk management is to minimize potential risks while maximizing potential opportunities.**

✓ **Is often overlooked in projects**, but it can help to improve project success by helping select good projects, determining project scope, and developing realistic estimates



# 5.1 Introduction

---

## Reactive Risk Strategies:

- Actions to **deal with risks** are taken **only when problems arise**.
- **Aka Fire-fighting**

## Proactive Risk Strategies:

- ✓ Started long before technical work begun
- ✓ Potential risks are identified, their probability and impact are assessed, ranked by importance.
- ✓ A contingency plan is developed to enable them to respond to the risk in a controlled and effective manner.
- ✓ Primary objective is to avoid risk.

This chapter focuses on **proactive risk strategies**  
**Reason is ...**

## 5.2 Risk Management Processes

---

### **Risk planning:**

Deciding how to approach and plan the risk management activities for the project

### **Risk identification:**

Determining which risks are likely to affect a project and documenting their characteristics

### **Qualitative risk analysis:**

Characterizing and analysing risks and prioritizing their effects on project objectives

### **Quantitative risk analysis:**

Measuring the probability and consequences of risks

### **Risk response planning:**

Taking steps to enhance opportunities and reduce threats to meeting project objectives

### **Risk monitoring and control:**

Monitoring known risks, identifying new risks, reducing risks, and evaluating the effectiveness of risk reduction

## 5.3 Risk Management Planning

---

A **Risk Management Plan** should cover the followings areas:

- ❑ **Why** it is important to take or not to take this risk in relation to the project objectives?
- ❑ **What** is the specific risk?
- ❑ **How** is the risk going to be mitigated?
- ❑ **Who** are the individuals responsible for implementing the risk management plan?
- ❑ **How** much effort is required in terms of resources to mitigate the risk?

## 5.3 Risk Management Planning

---

A **Risk Management Plan** should cover the followings areas:

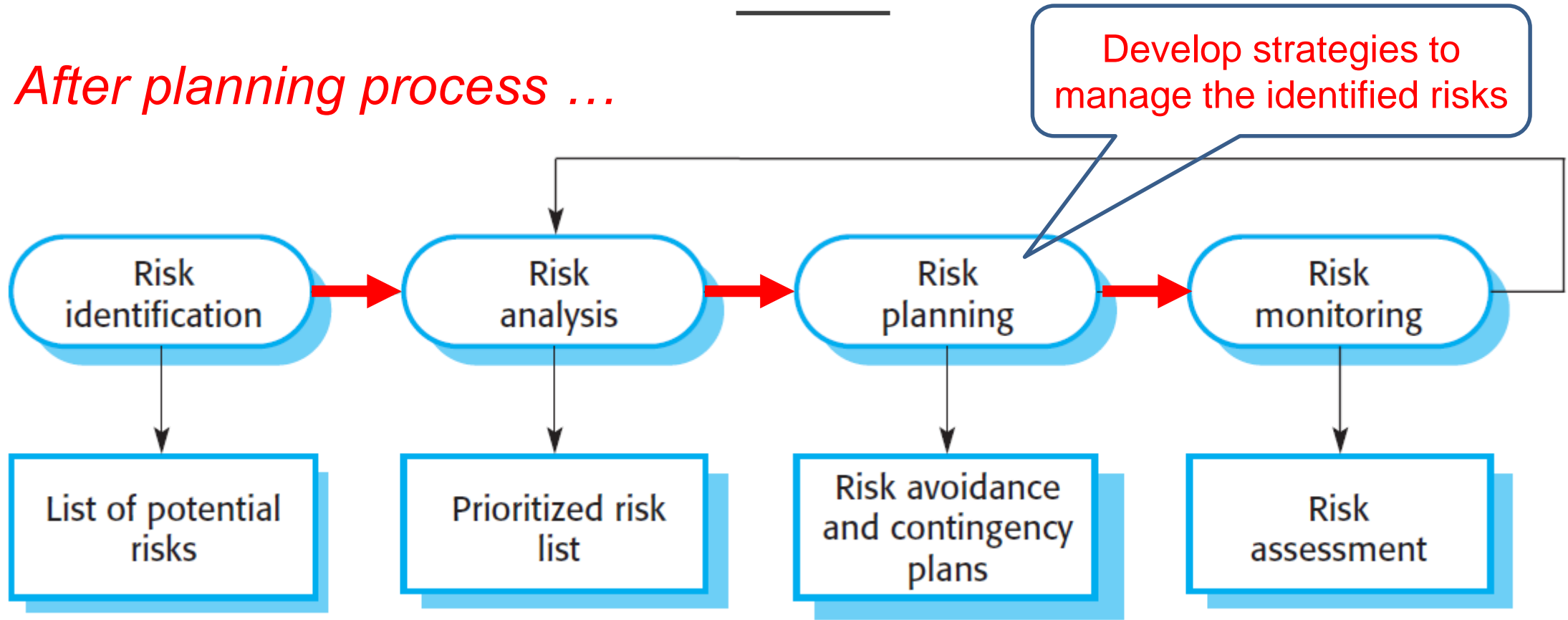
- ❑ **Why** it is important to take or not to take this risk in relation to the project objectives?
- ❑ **What** is the specific risk?
- ❑ **How** is the risk going to be mitigated?
- ❑ **Who** are the individuals responsible for implementing the risk management plan?
- ❑ **How** much is required in terms of resources to mitigate the risk?

### Also useful to have:

- **Contingency plans** - predefined actions to **take if an identified risk event occurs** (*e.g. if the latest OS is not available in time then the contingency plan is to use the older version*)
- **Contingency reserves or allowances** – reserved funds to mitigate costs or schedule risk if it does occur (*e.g. paying an outside consultant to train inexperienced staffs when inexperienced staffs are underperform*)

## 5.4 Risk Identification

*After planning process ...*



(Source: Software Engineering, 10th edition, by Ian Sommerville, Pearson Education, 2016, p. 646)



## 5.4 Risk Identification

---

- Identify risks that could threaten the software engineering process, the software being developed or the development organization.
- E.g. \_\_\_\_



## 5.4 Risk Identification – Types of Risks

Standish Group's IT success potential risk scoring sheet

| Success Criterion               | Points |
|---------------------------------|--------|
| User Involvement                | 19     |
| Executive Management support    | 16     |
| Clear Statement of Requirements | 15     |
| Proper Planning                 | 1      |
| Realistic Expectations          | 10     |
| Smaller Project Milestones      | 9      |
| Competent Staff                 | 8      |
| Ownership                       | 6      |
| Clear Visions and Objectives    | 3      |
| Hard-Working, Focused Staff     | 3      |
| Total                           | 100    |

McFarlan's Risk Questionnaire

- What is the project estimate in calendar (elapsed) time?
  - ( ) 12 months or less Low = 1 point
  - ( ) 13 months to 24 months Medium = 2 points
  - ( ) Over 24 months High = 3 points
- What is the estimated number of person days for the system?
  - ( ) 12 to 375 Low = 1 point
  - ( ) 375 to 1875 Medium = 2 points
  - ( ) 1875 to 3750 Medium = 3 points
  - ( ) Over 3750 High = 4 points
- Number of departments involved (excluding IT)
  - ( ) One Low = 1 point
  - ( ) Medium = 2 points
  - ( ) Two or more High = 3 points
- Is additional hardware required for the project?
  - ( ) None Low = 0 points
  - ( ) Central processor type change Low = 1 point
  - ( ) Peripheral/storage device changes Low = 1 point
  - ( ) Medium = 2 points
  - ( ) Change of platform, for example PCs replacing mainframes High = 3 points

## 5.4 Risk Identification

### Common SOURCES of Risk on IT Projects:

- **Financial risk:**
  - Can the organization afford to undertake the project? IF ANS = "NO" ...
  - Is this project the best way to use the company's financial resources? IF ANS = "NO" ...
- **People risk:**
  - Does the organization have the people with appropriate skills to complete the project successfully? IF ANS = "NO" ...
  - Does senior management support the project? IF ANS = "NO" ...
- **Technology risk**
  - Is the project technically feasible?
  - Will hardware, software and networks function properly?
- **Structure/Process risk:**
  - What degree of change will the new project introduce into user areas and business procedures? IF ANS = "HIGH" ...
  - With how many other system does the new system need to interact? IF ANS = "THERE ARE MANY" ...

### Market risk:

- **Will someone else create a better product or service faster, making the project a waste of time & money?**
- **Will users accept and use the product or service?**

(source: Schwalbe)

## 5.4 Risk Identification

---

- Categories of risks:

- *Project risks* – those that could prevent the achievement of project objectives given to the project manager and the project team (*source: Hughes*)
- *Technical risks* – those that could threaten the project schedule & quality (e.g. using new programming language)
- *Business risks* – e.g. an application is successfully implemented but is a business failure (e.g. costs > benefits gained) - *source: Hughes*



# 5.4 Risk Identification

## Categories of risks: \_\_\_\_\_

### Common SOURCES of Risk on IT Projects:

- **Financial risk:**
  - Can the organization afford to undertake the project?
  - Is this project the best way to use the company's financial resources?
- **People risk:**
  - Does the organization have the people with appropriate skills to complete the project successfully?
  - Does senior management support the project?
- **Technology risk**
  - Is the project technically feasible?
  - Will hardware, software and networks function properly?
- **Structure/Process risk:**
  - What degree of change will the new project introduce into user areas and business procedures?
  - With how many other system does the new system need to interact?

### **Market risk:**

- Will someone else create a **better product or service faster**, making the project a **waste of time & money**?
- Will users accept and use the **product or service**?

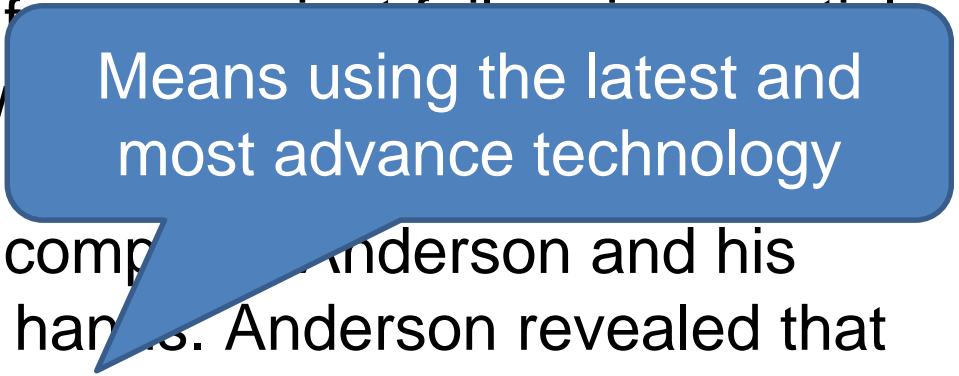
(source: Schwalbe)

### Categories of risks:

- **Project risks** – those that could prevent the achievement of project objectives given to the project manager and the project team (source: Hughes)
- **Technical risks** – those that could threaten the project schedule & quality (e.g. using new programming language)
- **Business risks** – e.g. an application is successfully implemented but is a business failure (e.g. costs > benefits gained) - source: H

# What Went Wrong?

Many information technology projects fail because of technology risk. One project manager learned an important lesson on a large IT project: focus on business needs first, not technology. David Anderson, a project manager for Kaman Sciences Corp., shared his experience for CIO Enterprise Magazine. After spending two thousand dollars on a project to provide new client human resources information systems for their company, Anderson and his team finally admitted they had a failure on their hands. Anderson revealed that he had been too enamored of the use of cutting-edge technology and had taken a high-risk approach on the project. He "ramrodded through" what the project team was going to do and then admitted that he was wrong. The company finally decided to switch to a more stable technology to meet the business needs of the company.



Means using the latest and most advance technology

Hildebrand, Carol. "If At First You Don't Succeed," CIO Enterprise Magazine, April 15, 1998

## 5.4 Risk Identification - **Techniques**

A project team get together to brainstorm possible risks

- **Brainstorming**
- The Delphi technique

A group of experts contribute ideas on a specific issue, they then further refine those ideas and lastly finalise on what is acceptable

- **Interviewing**
- **SWOT analysis**

- Ask people who have used particular hardware & software in his previous project  
- Ask people who have worked with a particular customer before you ...

Strengths, weaknesses, opportunities and threats. Use SWOT analysis to compare your company with another company to see who is more likely to win a project.

# 5.4 Risk

## Identification

Potential Risk Conditions Associated with Each Knowledge Area

| Knowledge Area  | Risk Conditions  |
|-----------------|--|
| Integration     | Inadequate planning; poor resource allocation; poor integration management; lack of post-project review                            |
| Scope           | Poor definition of scope or work packages; incomplete definition of quality requirements; inadequate scope control                 |
| Time            | Errors in estimating time or resource availability; poor allocation and management of float; early release of competitive products |
| Cost            | Estimating errors; inadequate productivity, cost, change, or contingency control; poor maintenance, security, purchasing, etc.     |
| Quality         | Poor attitude toward quality; substandard design/materials/workmanship; inadequate quality assurance program                       |
| Human Resources | Poor conflict management; poor project organization and definition of responsibilities; absence of leadership                      |
| Communications  | Carelessness in planning /communicating; lack of consultation with key stakeholders  |
| Risk            | Ignoring risk; unclear assignment of risk; poor insurance management   |
| Procurement     | Unenforceable conditions or contract clauses; adversarial relations  |

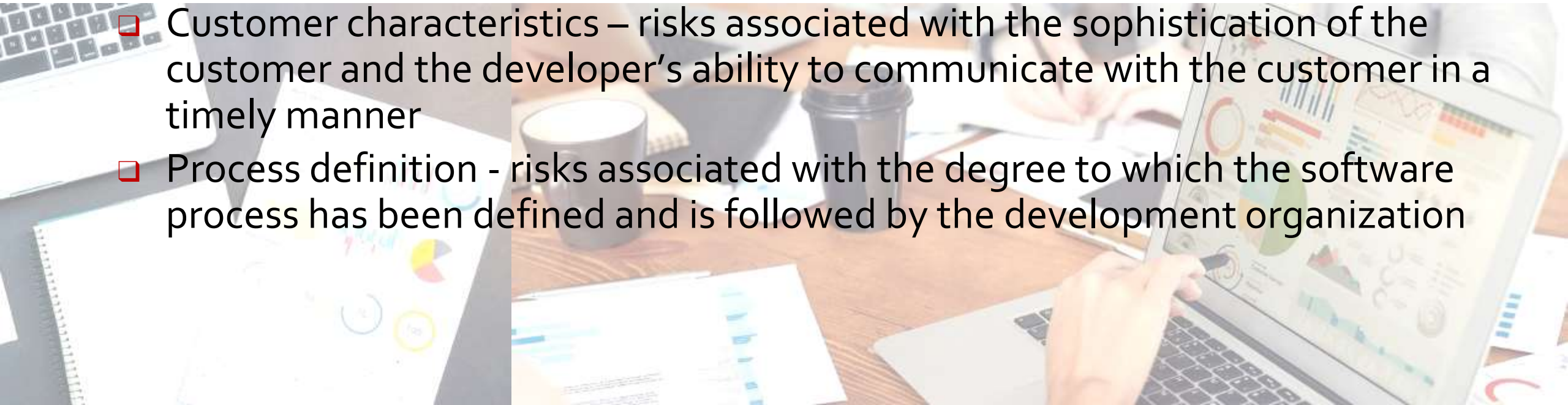


## 5.4 Risk Identification - Risk Item Checklist

---

Risk item checklist was created to identify risks in the following generic subcategories:

- ❑ Product size – risks associated with the size of software
- ❑ Business impact – risks associated with the 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

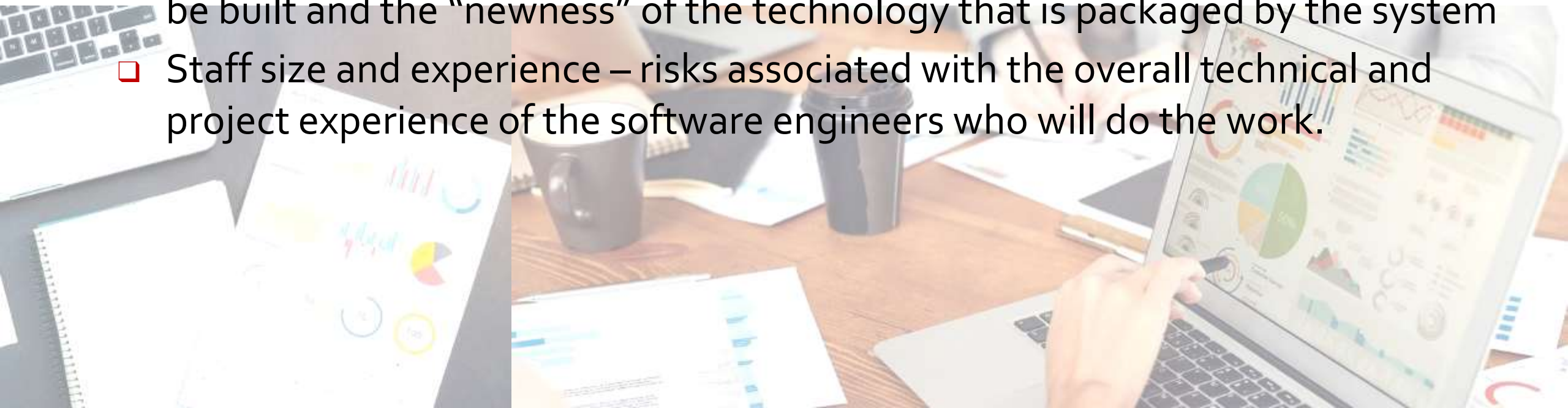


## 5.4 Risk Identification - Risk Item Checklist

---

Risk item checklist was created to identify risks in the following generic subcategories:

- ❑ 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.



## 5.4 Risk Identification - Assessing Overall Project Risk

Use Questions to identify and assess overall project risks. Rank them by their relative importance to the success of a project, e.g.:

1. Have **top management** formally committed to support the project? IF ANS = "YES"  
CHANCES OF  
PROJECT SUCCESS  
IS? \_\_\_\_\_
2. Are **end-users** enthusiastically committed to the project and the system/product to be built?
3. Are **requirements fully understood** by the SE team and their customers? IF ANS = "YES"  
CHANCES OF  
PROJECT  
SUCCESS IS?  
\_\_\_\_\_
4. Have customers been **involved** fully in the definition of requirements?
5. Do end-users have **realistic expectations**?
6. Is project **scope stable**?
7. Is the number of people on the project team **adequate** to do the job? IF ANS = "YES"  
CHANCES OF  
PROJECT SUCCESS  
IS? \_\_\_\_\_

If any ANSWER to these questions is "NO", mitigation, monitoring & management steps should be implemented.

## 5.4 Risk Identification - Risk Components & Drivers

---

- The US Air Force has written a pamphlet that contains excellent guidelines for risk identification.
- It requires the project manager identify the risk drivers that affect software risk components: Performance risk, Cost risk, Support risk and Schedule risk.
- The impact of each risk driver on the risk component is divided into one of 4 impact categories (negligible, marginal, critical & catastrophic)





| Components<br>Category |   | Performance   | Support                                 | Cost   | Schedule                      |
|------------------------|---|---|---|--|-------------------------------|
| <b>Catastrophic</b>    | 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              |
| <b>Critical</b>        | 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      |
| <b>Marginal</b>        | 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 |
| <b>Negligible</b>      | 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 Impact Categories

Note: (1) The potential consequence of undetected software errors or faults.  
(2) The potential consequence if the desired outcome is not achieved.

## 5.5 Risk Projection (**Risk Estimation**)

---

- Risk projection/estimation attempts to rate each risk in 2 ways:
  - the **likelihood or probability** that the risk is real
  - the **consequences** associated with the risk
- 4 risk projection activities:
  1. **Establish a scale** that reflects the perceived likelihood of a risk
  2. **Identify the consequences** of the risk
  3. **Estimate the impact** of the risk
  4. **Ensure accuracy** (of 1,2,3) to avoid misunderstandings.

## 5.5 Risk Projection – Risk Table

---

- The **risk table** provides PM with a simple technique for risk projection.
- **Steps to develop risk table:**
  - Column 1 – **list all risks**
  - Column 2 – **category of risk**
  - Column 3 – **probability for each risk**
  - Column 4 – **impact of each risk (1 to 4 or 1 to 10)**
  - Column 5 – **RMMM** (risk mitigation, monitoring, management)



## 5.5 Risk Projection – Risk Categories

| RISK CATEGORIES   | DESCRIPTION: Risks associated with  |
|---|---|
| <input type="checkbox"/> Product size (PS)              | the overall size of the software to be built or modified.   |
| <input type="checkbox"/> Business impact (BU)           | constraints imposed by management or the marketplace.   |
| <input type="checkbox"/> Customer characteristics (CU)  | the sophistication of the customer and the developer's ability to communicate with the customer in a timely manner. |
| <input type="checkbox"/> Process definition (PR)        | the degree to which the software process has been defined and is followed by the development organization.          |
| <input type="checkbox"/> Development environment (DE)   | the availability and quality of the tools to be used to build the product.  |
| <input type="checkbox"/> Technology to be built (TE)    | the complexity of the system to be built and the "newness" of the technology that is packaged by the system.        |
| <input type="checkbox"/> Staff size and experience (ST) | The overall technical and project experience of the software engineers who will do the work.                        |



## 5.5 Risk Projection – Risk Impact Assessment

*Risk impact assessment* is carried out based on this Risk Impact Categories. The categories for each of the 4 risk components – performance, support, cost and schedule – are averaged to determine an overall impact value.

Note:

- (1) The potential consequence of undetected software errors or faults.
- (2) The potential consequence if the desired outcome is not achieved.

| Components<br>Category |             |   |   |  |
|------------------------|-------------|---|---|--|
|                        | Performance | Support   | Cost                                    | Schedule   |
| Catastrophic<br>4      | 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   |
| Critical<br>3          | 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  |
| Marginal<br>2          | 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   |
| Negligible<br>1        | 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   |

## 5.5 Risk Projection – Risk Table Example

Risk Mitigation,  
Monitoring &  
Management Plan

| Risks                                  | Category | Probability | Impact | RMMM                    |
|--|----------|-------------|--------|-------------------------|
| Less reuse than planned                | PS       | 70%         | 3      |                         |
| End-users resist system                | BU       | 40%         | 2      |                         |
| Funding will be lost                   | CU       | 40%         | 4      |                         |
| Lack of training on tools              | DE       | 80%         | 2      |                         |
| High staff turnover                    | ST       | 60%         | 3      | Miti=<br>Moni=<br>Mgmt= |
| Staff inexperienced                    | ST       | 30%         | 3      |                         |
| Size estimate may be significantly low | PS       | 60%         | 3      |                         |
| Larger number of users than planned    | PS       | 30%         | 2      |                         |
| Delivery deadline will be tightened    | BU       | 50%         | 3      |                         |
| Customer will change requirements      | PS       | 80%         | 2      |                         |
| Technology will not meet expectations  | TE       | 30%         | 4      |                         |

**Categories:**  
 PS – Project size risk  
 BU – Business risk  
 CU – Customer characteristics  
 TE – Technology to be built  
 ST – Staff size & experience  
 DE – development environment

Impact values: 1 – negligible, 2 – marginal, 3 – critical, 4 – catastrophic

## 5.5 Risk Projection – Risk Prioritization

- Once the first 4 columns of the risk table have been completed, sort the table by **probability** and by **impact**.
- The PM studies the sorted table and defines a **cutoff line**.
- Risks above the cutoff line to be given further **attention**. Risks below the line are to be re-evaluated
- Pay attention to **High-impact risks** with moderate to high probability and low-impact risks with **high probability**
- The column labeled **RMMM** contains a pointer to a risk mitigation, monitoring, and management plan or a collection of risk information sheets developed for all risks that lie above the cutoff.

Or calculate the **Risk Score** for each risk.

**Risk Score** = Probability of occurrence \* Impact

**Sort** the risk table by Risk Score in descending order.

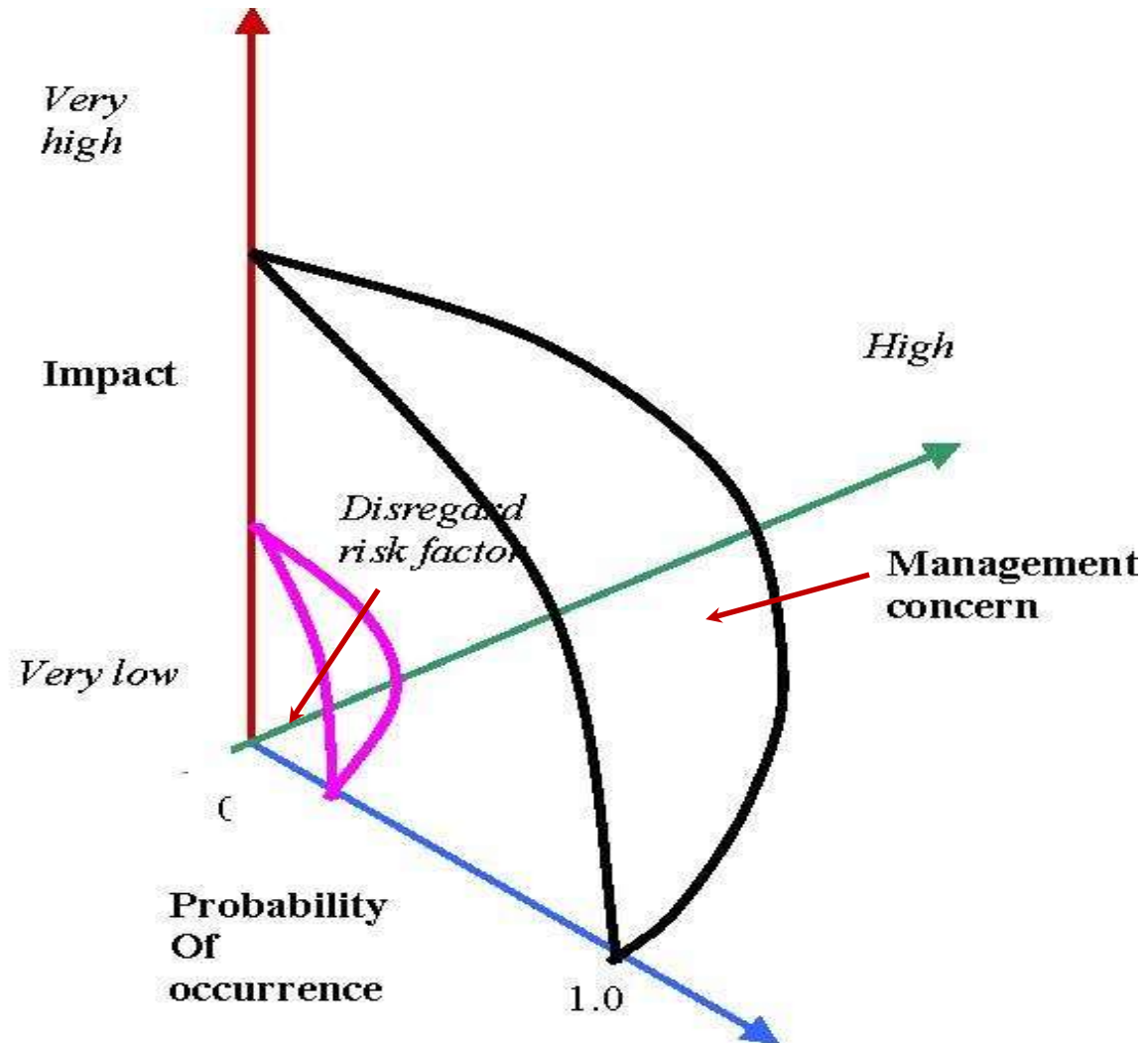
Pay attention those risks with **high score**.

# Exercise

Rank the following risks:

| Risks                   | Category | Probability | Impact | Risk score           |
|-------------------------|----------|-------------|--------|----------------------|
| Less reuse than planned | PS       | 70%         | 2      | $0.7 \times 2 = 1.4$ |
| End users resist system | BU       | 40%         | 3      | $0.4 \times 3 = 1.2$ |
| Funding will lost       | CU       | 40%         | 1      | $0.4 \times 1 = 0.4$ |
| Lack of training tools  | DE       | 80%         | 3      | $0.8 \times 3 = 2.4$ |
| High staff turnover     | ST       | 60%         | 2      | $0.6 \times 2 = 1.2$ |

## 5.5 Risk Projection – Risk & Management Concern





## 5.5 Risk Projection – Consequences

---

During risk assessment, we consider 3 factors affect the consequences that are likely if a risk does occur:

### Nature

- the problems that are likely if it occurs
- e.g. a poorly defined external interface to customer hardware (a technical risk) will preclude early design and testing and will likely lead to system integration problems late in a

### Scope

- How serious is the risk (severity) with its overall distribution (how much of the project will be affected or how many customers are harmed?)

### Timing

- When and for how long the impact will be felt

## 5.5 Risk Projection – **Assessing Risk Exposure**

If **costs** are associated with each risk table entry, Halstead's **risk exposure** (RE) metric can be computed and added to the risk table using:

$$RE = P \times C$$

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

**C: cost** to the project should the risk occur

### EXAMPLE

**Risk identification:** Only 70% of the software components scheduled for reuse will, in fact, be integrated into the application. The remaining functionality(30%) will have to be custom developed.

**Risk probability:** 80%

**Risk impact:** 60 reusable software components were planned. If only 70% can be used, 18 components would have to be developed from scratch. The average component is **100 LOC** and local data indicate that the SE 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:**  $RE = 0.80 \times 25,200 = \$20,160$

## 5.6 Risk Refinement - Example

---

- The reuse risk stated in CTC format:  
*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.*
- The above general condition may be refined as follows:
  - **Subcondition 1:** Certain reusable components were developed by a 3<sup>rd</sup> 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.

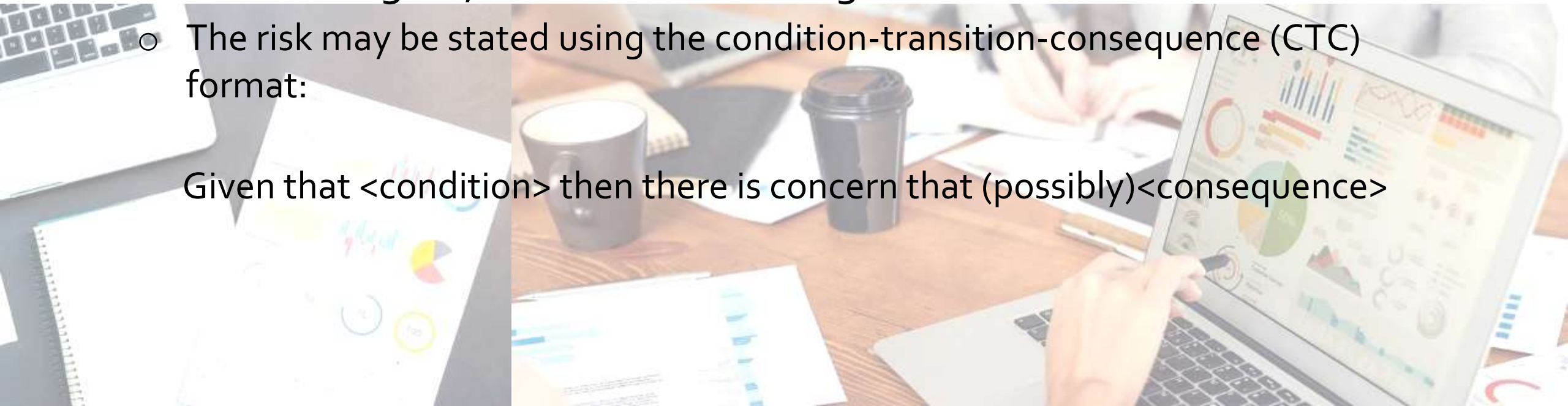
## 5.6 Risk Refinement

---

- During early stages of project planning, a risk may be stated quite generally.
- Over time as more is learned about the project and the risk, it may be possible to refine the risk into a set of more detailed risks to make it easier to mitigate, monitor and manage.

- The risk may be stated using the condition-transition-consequence (CTC) format:

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



# 5.7 Risk Mitigation, Monitoring, & Management (RMMM)

An effective risk management strategy must consider 3 issues:

## a. Risk mitigation

- The process of developing options and actions to enhance opportunities and **reduce threats to project objectives**

## b. Risk monitoring & control

- **A project tracking activity** with 3 objectives: (i) **to assess whether predicted risks do, in fact occur**; (ii) **to ensure that risk aversion steps defined for the risk are being properly applied**; and (iii) **to collect information that can be used for future risk analysis**.
- Controlling risks involves carrying out the risk management plans as risks occur
- The main outputs of risk monitoring and control are corrective action, project change requests, and updates to other plans .

## c. Risk management and contingency planning

- Consists of **actions to be taken in the event of mitigation efforts have failed and that the risk has become a reality**.



## 5.7 Risk Mitigation, Monitoring, & Management (RMMM)

---

### Risk management strategies

- **Risk acceptance:** The “do nothing” option. In the risk prioritization process, it would have been decided for some risks to be ignored in order to concentrate on the more likely or damaging risks. For some risks the **costs of action > the damage inflicted in order to reduce the probability of a risk from happening.**
- **Risk avoidance:** To take the necessary action to avoid the risk altogether.
- **Risk reduction:** Take precautions to reduce the probability of the risk.
- **Risk mitigation:** Take the necessary action(s) to ensure that the impact of the risk is lessened when it occurs.
- **Risk transfer:** Transfer the risk to another person or organization. E.g., outsource the development task to an external organization for a fixed fee.



## 5.7 Risk Mitigation, Monitoring, & Management (RMMM)

- For a large project, 30 or 40 risks may be identified. If between 3 to 7 steps are identified for each risk, risk management may turn out to be a project itself. So, adopt the **Pareto 80-20 rule** to software risk to include only 20% risks that lead to the highest risk exposure in the RMMM plan.
- Documented each risk individually by using a Risk Information Sheet.



## Risk Information Sheet

Risk ID: P03-1-37

Date: 15/2/2020

Probability: 70%

Impact: Critical

### Description:

Based on past history and management intuition, high staff turnover will have a critical impact on project cost and schedule.

### Mitigation:

- Meet with current staff to determine causes for turnover.
- Mitigate the causes that are within control before the project starts.
- Develop techniques to ensure continuity when people leave.
- Organize project teams so that information about each development activity is widely dispersed.
- Define work product standards and establish mechanisms to be sure that all models and documents are developed in a timely manner.
- Conduct peer reviews of all work.
- Assign backup staff member for every critical technology.

### Monitoring:

- Monitor the general attitude of team members based on project pressures.
- Check the degree to which the team has jelled.
- Assess the interpersonal relationships among team members.
- Check potential problems with compensation and benefits.
- Monitor the availability of jobs within the company and outside.

### Management:

If any staff announce that they will be leaving when the project is under way, following the mitigation strategy will ensure that:

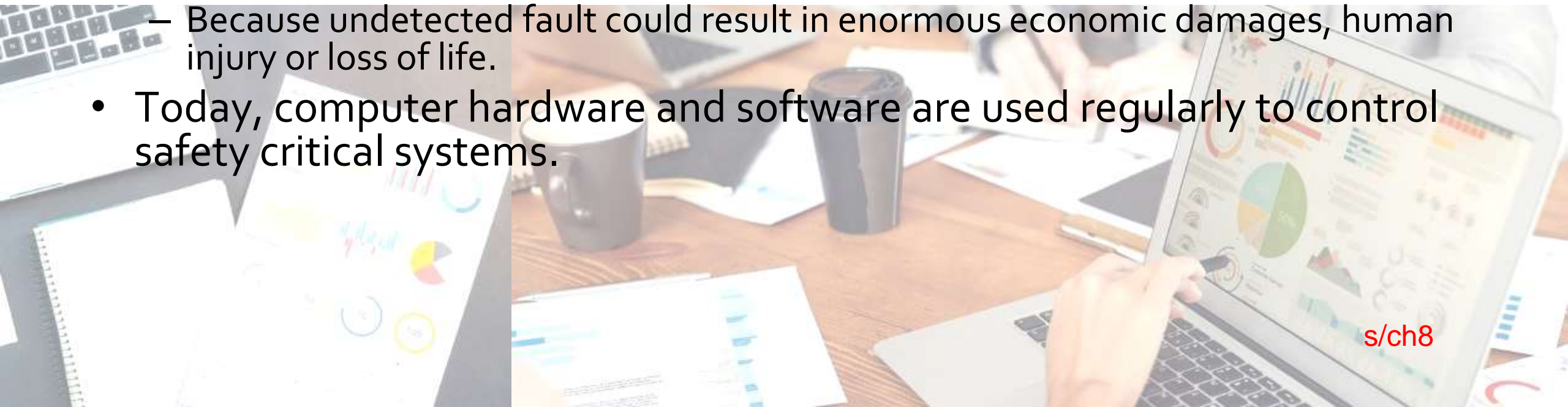
- Backup is available
- Information is well-documented
- Knowledge has been dispersed across the team

In addition, we can 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. The individuals who are leaving will be 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 or Wikis, and/or meeting with other team members who will remain on the project.

## 5.8 Safety Risks and Hazards

---

- Risk is not limited to software project itself but also after software has been successfully developed and delivered to the customer – software failure in the field.
- In the early days of computing, there was reluctance to use computers to control safety critical processes such as nuclear reactors, aircraft flight control, weapons system. Why?
  - Because undetected fault could result in enormous economic damages, human injury or loss of life.
- Today, computer hardware and software are used regularly to control safety critical systems.



## 5.8 Safety Risks and Hazards

---

- Software safety and hazard analysis:
  - Software quality assurance activities that focus on the identification and assessment of potential hazards that may affect software negatively and cause an entire system to fail.
- If hazards can be identified early in the process, software design features can be specified that will either eliminate or control potential hazards.







# Summary

---

- 5.1 Introduction
- 5.2 Risk Management Processes
- 5.3 Risk Management Planning
- 5.4 Risk Identification
- 5.5 Risk Projection
- 5.6 Risk Refinement
- 5.7 Risk Mitigation, Monitoring, & Management (RMMM)
- 5.8 Safety Risks and Hazards