Faculty of ECMS / School of Computer Science

Software Engineering & Project Risk Management

Risk Management

Lecture 7

Chapter 25 in the course text book

Outline

- Case Study: Denver Automated Baggage Handling System
- Risk Management
- Risk Identification
- Risk Analysis
- Risk Control and Mitigation
- Risk Monitoring
- Documenting Risks

DIA Automated Baggage Handling System

- Denver International Airport ABHS is a synonymous with failed software projects
- System started in **November 1989**
- Due for completion in **October 1993**
- Partial semi-automated system delivered in **February 1995**
  - Incoming flights never made use of the system
  - Only United used it for out going
- System was scrapped in **August 2005**
- Blamed on failure of software team
- BUT, real blame lies in lack of risk management

Risk analysis for ABHS

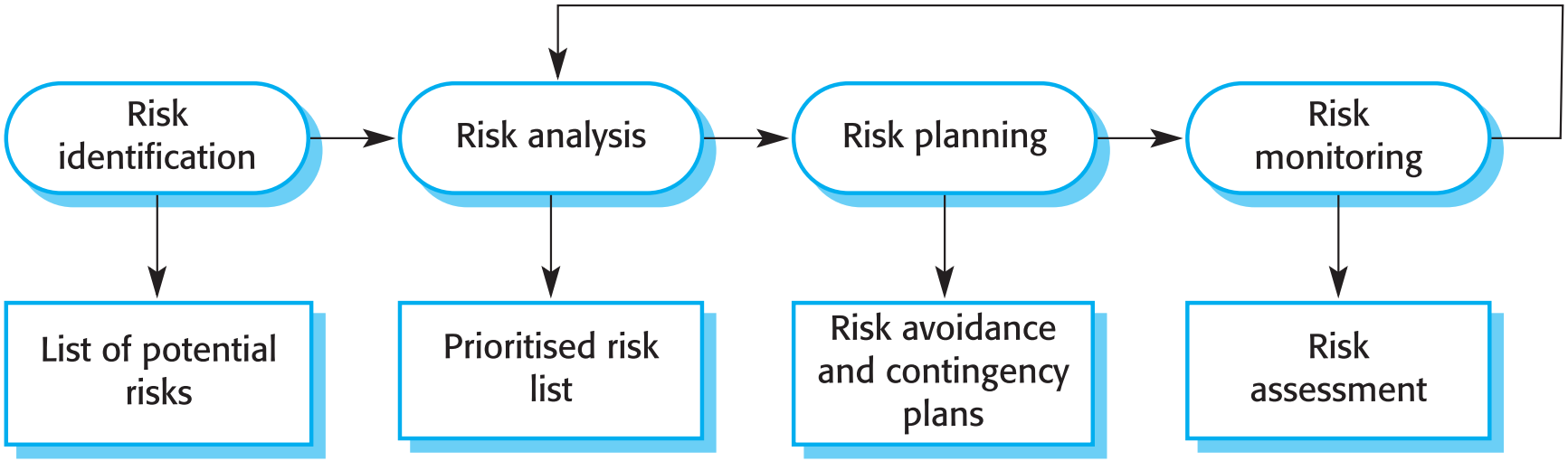
- Software was on the critical path
  - System could not operate without the software
  - No other way to move baggage around
  - Tunnels too low for trucks and personnel to get around

- Risk 1: Late Delivery of Software
  - Severity = High
  - Likelihood = High
  - Control measures = None
  - Mitigation = None

Risk Management

- All projects have risks that can affect
  - Timeliness of delivery(or indeed whether the product is delivered at all!)
  - Quality of product
- Risk management is concerned with
  - Identifying risks
  - Defining strategies for preventing or controlling the risk
- Risk analysis should happen at start of project
  - Improve the likelihood of a realistic project plan
  - Increase the chance of completing project on-time and on-budget
- Risks should be reassessed throughout the lifecycle

Risk Management Process



Risk Types

- Technology risks
- People risks
- Organisational risks
- Tool risks
- Requirements risks
- Estimation risks

Risk Types (Cont.)

Risk type	Possible risks
Technology	The database used in the system cannot process as many transactions per second as expected. Software components that should be reused contain defects that limit their functionality.
People	It is impossible to recruit staff with the skills required. Key staff are ill and unavailable at critical times. Required training for staff is not available.
Organisational	The organisation is restructured so that different management are responsible for the project. Organisational financial problems force reductions in the project budget.
Tools	The code generated by CASE tools is inefficient. CASE tools cannot be integrated.
Requirements	Changes to requirements that require major design rework are proposed. Customers fail to understand the impact of requirements changes.
Estimation	The time required to develop the software is underestimated. The rate of defect repair is underestimated. The size of the software is underestimated.

Risk Types (Cont.)

- Core Risks:
  - Schedule Flaw
  - Requirements inflation(requirements “churn”)
  - Staff Turnover
  - Specification breakdown
    - The customer and developer cannot come to an agreement on what is to be developed
  - Team underperformance

Source: DeMarco and Lister, Waltzing with Bears: Managing Risk on Software Projects, Dorset House, 2003

Risk Discovery

- Risk Discovering Process (from DeMarco and Lister; Waltzing with Bears)

- Work backwards from the catastrophic outcomes
- Consider situation that could lead to these outcomes
- Figure out the root causes for the scenario

Catastrophe Brainstorm Ploys

- Frame the question explicitly in terms of a nightmare
  - Ask people what their worst fears are for the project
- Use a crystal ball
  - Future shows a disaster, but what disaster?
- Switch perspectives
  - Describe best dreams of project, then discuss an inverted version
- Ask about blame-free disasters
  - How could the project go awry and have it be a software fault? The user's fault? Management fault? Hardware fault?
- Imagine partial failure
  - How could the project succeed in general but leave one stakeholder unsatisfied?

Example

- **Catastrophic Outcome**: On final presentation day the group is unable to check out and build (in a timely manner) a working version of their software

- **Scenario**: A day before the presentation a working version exists, however somebody in the group then checks in a “fix” which breaks the code. Your group is unable to easily retrieve a working version.

- **Root Cause**: Lack of appropriate Configuration Management policy, process and practice.

Exercise

- Work through one or more catastrophic situations that might be applicable to your project (use catastrophe brainstorm ploys)
- For each of the catastrophes, develop one or more scenarios and root causes that may lead to the catastrophe

Risk Analysis

- Assess probability and seriousness of each risk.
- Probability may be very low, low, moderate, high or very high.
- Risk effects may be catastrophic, serious, tolerable or insignificant
  - You may wish to use the following mapping as a guide:
    - Catastrophic -> Death or destruction
    - Serious -> Injury, damaged, impediment
    - Tolerable -> Inefficient
    - Insignificant -> Mild annoyance
  - Note: these can shift around depending on the project

Risk Analysis Example

Risk	Probability	Effects
Organisational financial problems force reductions in the project budget.	Low	Catastrophic
It is impossible to recruit staff with the skills required for the project.	High	Catastrophic
Key staff are ill at critical times in the project.	Moderate	Serious
Software components that should be reused contain defects which limit their functionality.	Moderate	Serious
Changes to requirements that require major design rework are proposed.	Moderate	Serious
The organisation is restructured so that different management are responsible for the project.	High	Serious

Risk Analysis Example (Cont.)

Risk	Probability	Effects
The database used in the system cannot process as many transactions per second as expected.	Moderate	Serious
The time required to develop the software is underestimated.	High	Serious
CASE tools cannot be integrated.	High	Tolerable
Customers fail to understand the impact of requirements changes.	Moderate	Tolerable
Required training for staff is not available.	Moderate	Tolerable
The rate of defect repair is underestimated.	Moderate	Tolerable
The size of the software is underestimated.	High	Tolerable
The code generated by CASE tools is inefficient.	Moderate	Insignificant

Exercise

- For each of the risks the previous exercise, write down the associated severity and likelihood
- Justify your answer!

Risk Planning

- Consider each risk and develop a strategy to manage that risk.
- Avoidance strategies
  - The probability that the risk will arise is reduced
- Minimisation strategies
  - The impact of the risk on the project or product will be reduced
- Contingency plans
  - If the risk arises, contingency plans are plans to deal with that risk

Risk Management Strategy Examples

Risk	Strategy
Organisational financial problems	Prepare a briefing document for senior management showing how the project is making a very important contribution to the goals of the business.
Recruitment problems	Alert customer of potential difficulties and the possibility of delays, investigate buying-in components.
Staff illness	Reorganise team so that there is more overlap of work and people therefore understand each other's jobs.
Defective components	Replace potentially defective components with bought-in components of known reliability.

Risk Management Strategy Examples (Cont.)

Risk	Strategy
Requirements changes	Derive traceability information to assess requirements change impact, maximise information hiding in the design.
Organisational restructuring	Prepare a briefing document for senior management showing how the project is making a very important contribution to the goals of the business.
Database performance	Investigate the possibility of buying a higher-performance database.
Underestimated development time	Investigate buying in components, investigate use of a program generator

Exercise

- Derive a risk management strategy for the risks derived in the previous exercise
- Think about:
  - Avoidance Strategies
  - Minimisation Strategies
  - Contingency Plans

Risk Monitoring

- Assess each identified risk regularly to decide whether or not it is becoming less or more probable.
- Also assess whether the effects of the risk have changed.
- Each key risk should be discussed at the management progress meetings.

Risk Indicator Examples

Risk type	Potential indicators
Technology	Late delivery of hardware or support software, many reported technology problems
People	Poor staff morale, poor relationships amongst team member, job availability
Organisational	Organisational gossip, lack of action by senior management
Tools	Reluctance by team members to use tools, complaints about CASE tools, demands for higher-powered workstations
Requirements	Many requirements change requests, customer complaints
Estimation	Failure to meet agreed schedule, failure to clear reported defects

Recording Risks

- In documenting risks should include:
  - Risk Name
  - Description
  - Likelihood
  - Severity (eg. Effect on budget, effect on delivery date)
  - Risk Indicator
  - Mitigation/Control strategies
- Since risks may change over time we need to also include a history of changes in risk