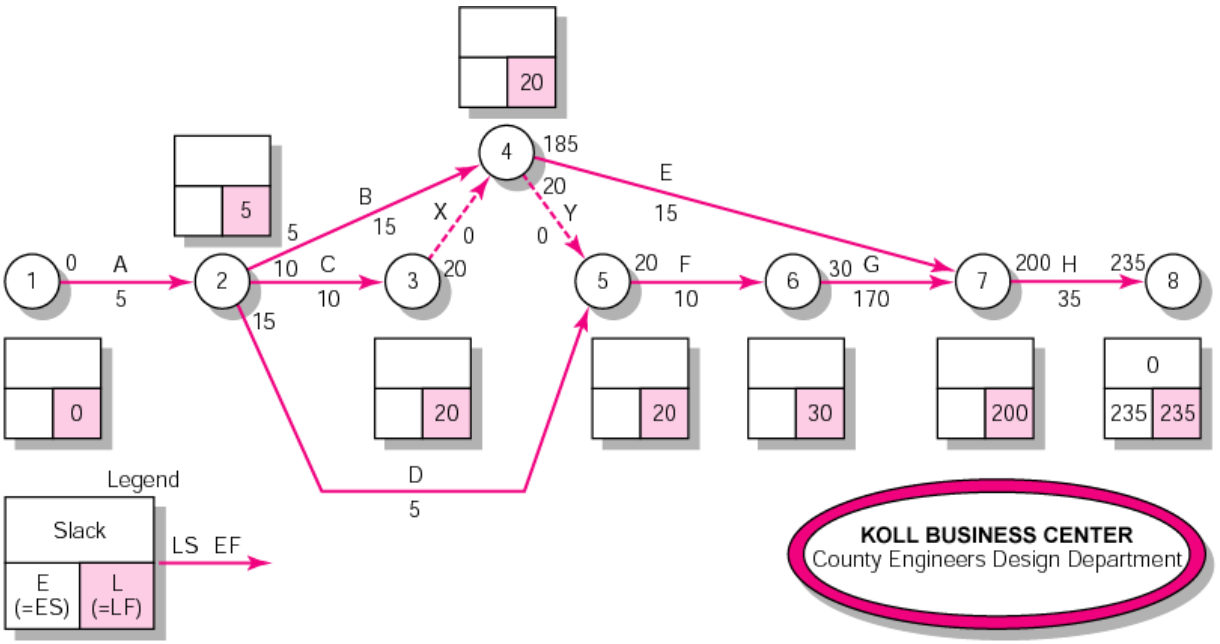


20. RiskManagement

The proactive management of risks throughout the software development lifecycle is important for project success.

- The risk management practice, which involves risk identification, analysis, prioritization, planning, mitigation, monitoring, and communication
- software development risks that seem to reoccur in educational and industrial projects
- a risk-driven process for selecting a software development model

20.1Risk Identification

In the risk identification step, the team systematically enumerates as many project risks as possible to make them explicit before they become problems. There are several ways to look at the kinds of software project risks.

There are some specific factors to consider when examining project, product, and business risks. Some examples of these factors are listed here, although this list is meant to stimulate your thinking rather than to be an all-inclusive list.

People risks are associated with the availability, skill level, and retention of the people on the development team.

Size risks are associated with the magnitude of the product and the product team. Larger products are generally more complex with more interactions. Larger teams are harder to coordinate.

Process risks are related to whether the team uses a defined, appropriate software development process and to whether the team members actually follow the process.

Technology risks are derived from the software or hardware technologies that are being used as part of the system being developed. Using new or emerging or complex technology increases the overall risk.

Tools risks, similar to technology risks, relate to the use, availability, and reliability of support software used by the development team, such as development environments and other Computer-Aided Software Engineering (CASE) tools.

Organizational and managerial risks are derived from the environment where the software is being developed. Some examples are the financial stability of the company and threats of company reorganization and the potential of the resultant loss of support by management due to a change in focus or a change in people.

Customer risks are derived from changes to the customer requirements, customers' lack of understanding of the impact of these changes, the process of managing these requirements changes, and the ability of the customer to communicate effectively with the team and to accurately convey the attributes of the desired product.

Estimation risks are derived from inaccuracies in estimating the resources and the time required to build the product properly.

Sales and support risks involve the chances that the team builds a product that the sales force does not understand how to sell or that is difficult to correct, adapt, or enhance.

20.2 Strategies for Risk Management:

During the software development process various strategies for risk management could be identified and defined according to the amount of risk influence. Based upon the amount of risk influence in software development project, risk strategies could be divided into three classes namely careful, typical, and flexible (Boban, M. et.). Generally, careful risk management strategy is projected for new and inexperienced organizations whose software development projects are connected with new and unproven technology; typical risk management strategy is well-defined as a support for mature organizations with experience in software development projects and used technologies, but whose projects carry a decent number of risks; and flexible risk management strategy is involved in experienced software development organizations whose software development projects are officially defined and based on proven technologies (Boban, M. etc.).

20.3 Categories of risks:

Schedule Risk:

Project schedule get slip when project tasks and schedule release risks are not addressed properly.

Schedule risks mainly effect on project and finally on company economy and may lead to project failure.

Schedules often slip due to following reasons:

- Wrong time estimation
- Resources are not tracked properly. All resources like staff, systems, skills of individuals etc.
- Failure to identify complex functionalities and time required to develop those functionalities.
- Unexpected project scope expansions.

Budget Risk:

- Wrong budget estimation.
- Cost overruns
- Project scope expansion

Operational Risks:

Risks of loss due to improper process implementation, failed system or some external events risks.

Causes of Operational risks:

- Failure to address priority conflicts
- Failure to resolve the responsibilities
- Insufficient resources
- No proper subject training
- No resource planning
- No communication in team.

Security in System Development

- Risk Analysis & Management needs to be a part of system development, not tacked on afterwards
- Baskerville's three generations of methods

1st Generation: Checklists

Example: BS 7799 Part 1

2nd Generation: Mechanistic engineering methods

Example: this risk analysis method

3rd Generation: Integrated design

Not yet achieved

Definitions:

The meanings of terms in this area are not universally agreed. We will use the following

- **Threat**: Harm that can happen to an asset
- **Impact**: A measure of the seriousness of a threat
- **Attack**: A threatening event
- **Attacker**: The agent causing an attack (not necessarily human)
- **Vulnerability**: a weakness in the system that makes an attack more likely to succeed
- **Risk**: a quantified measure of the likelihood of a threat being realised
- **Risk Analysis** involves the identification and assessment of the levels of risk, calculated from the
    - Values of assets

- Threats to the assets
- Their vulnerabilities and likelihood of exploitation

- **Risk Management** involves the identification, selection and adoption of security measures justified by
  - The identified risks to assets
  - The reduction of these risks to acceptable levels

Goals of Risk Analysis:

- All assets have been identified
- All threats have been identified
  - Their impact on assets has been valued
- All vulnerabilities have been identified and assessed

Problems of Measuring Risk

- Businesses normally wish to measure in money, but
- Many of the entities do not allow this
  - Valuation of assets
    - Value of data and in-house software - no market value
    - Value of goodwill and customer confidence
  - Likelihood of threats
    - How relevant is past data to the calculation of future probabilities?
    - The nature of future attacks is unpredictable
    - The actions of future attackers are unpredictable
  - Measurement of benefit from security measures
    - Problems with the difference of two approximate quantities
    - How does an extra security measure affect a $\sim 10^{-5}$ probability of attack?

Risk Levels

- Precise monetary values give a false precision

- Better to use levels, e.g.
  - High, Medium, Low
    - High: major impact on the organisation
    - Medium: noticeable impact (“material” in auditing terms)
    - Low: can be absorbed without difficulty
  - 1 - 10
- Express money values in levels, e.g.
  - For a large University Department a possibility is
    - High
    - Medium
    - Low

Risk Analysis Steps

- Decide on scope of analysis
  - Set the system boundary
- Identification of assets & business processes
- Identification of threats and valuation of their impact on assets (impact valuation)
- Identification and assessment of vulnerabilities to threats
- Risk assessment

Risk Analysis – Defining the Scope

- Draw a context diagram
- Decide on the boundary
  - It will rarely be the computer!
- Make explicit assumptions about the security of neighbouring domains
  - Verify them!

Risk Analysis - Identification of Assets

- Types of asset
    - Hardware
    - Software: purchased or developed programs
    - Data
    - People: who run the system
    - Documentation: manuals, administrative procedures, etc
    - Supplies: paper forms, magnetic media, printer liquid, etc
    - Money
    - Intangibles
        - Goodwill
        - Organization confidence
        - Organisation image

Risk Analysis – Impact Valuation

Identification and valuation of threats - for each group of assets

- Identify threats, e.g. for stored data
    - Loss of **confidentiality**
    - Loss of **integrity**
    - Loss of **completeness**
    - Loss of **availability** (Denial of Service)
- For many asset types the only threat is loss of availability
- Assess impact of threat
    - Assess in levels, e.g H-M-L or 1 - 10
    - This gives the valuation of the asset in the face of the threat

Risk Analysis – Vulnerabilities

- Identify vulnerabilities against a baseline system

For risk analysis of an existing system

- Existing system with its known security measures and weaknesses

For development of a new system

- Security facilities of the envisaged software, e.g. Windows NT
- Standard good practice, e.g. BS 7799 recommendations of good practice

For each threat

- Identify vulnerabilities
  - How to exploit a threat successfully;
- Assess levels of likelihood - High, Medium, Low
  - Of attempt

    Expensive attacks are less likely (e.g. brute-force attacks on encryption keys)
  - Successful exploitation of vulnerability;
- Combine them

Risk Assessment

Assess risk

- If we had accurate probabilities and values, risk would be
  - Impact valuation x probability of threat x probability of exploitation
  - Plus a correction factor for risk aversion
- Since we haven't, we construct matrices such as

Impact valuation

Risk	**Low**	**Med**	**high**
low	**Low**	**Low**	**med**
med	**Low**	**Med**	**High**
high	**Low**	**Med**	**High**

Responses to risk

- Avoid it completely by withdrawing from an activity
- Accept it and do nothing
- Reduce it with security measures

Risk management

- Risk management is concerned with identifying risks and drawing up plans to minimisetheir effect on a project.
- A risk is a probability that some adverse circumstance will occur

  Project risks affect schedule or resources;

  Product risks affect the quality or performance of the software being developed;

  Business risks affect the organisation developing or procuring the software.

The risk management process

Risk identification

Identify project, product and business risks;

Risk analysis

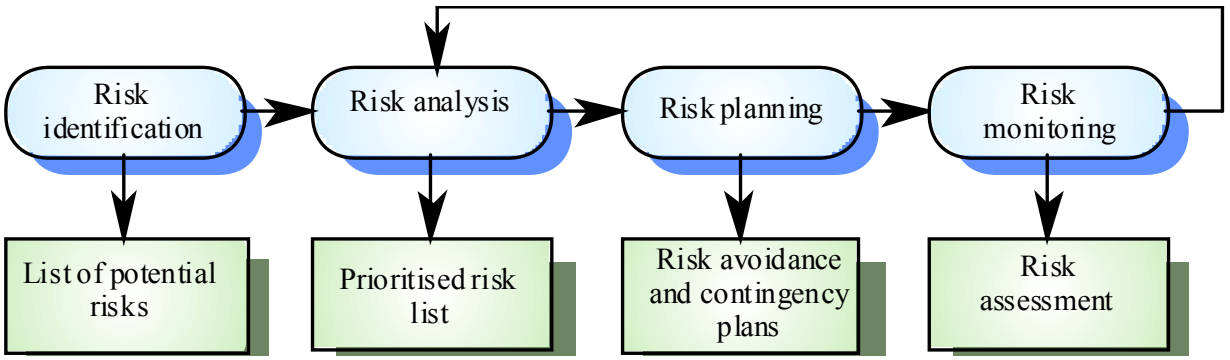
Assess the likelihood and consequences of these risks;

Risk planning

Draw up plans to avoid or minimise the effects of the risk;

Risk monitoring

Monitor the risks throughout the project;



21. Hazard Identification

Systematic Processes

What Constitutes a Hazard?

A real or potential condition that, when activated, can transform into a series of interrelated events that result in damage to equipment or property and or injury to people.

Safety Managers View

- Hazard
  - An implied threat or danger, a potential condition waiting to become a loss