Course Material No. 5

SOFTWARE ENGINEERING 2

FE LARWA-HABLANIDA
Course Instructor

RISK MANAGEMENT AND CONFIGURATION CONTROL 1

5

LEARNING OUTCOMES

At the end of the lesson, the learner will be able to:

- Explain the importance of risk management and configuration control in software projects.
- Identify, analyze, and prioritize risks using structured approaches.
- Describe the configuration management process and its role in maintaining system integrity.

RESOURCES NEEDED

For this lesson, you would need the following resources:

- PPT/Module
- Pencil and Paper

DISCUSSION:

INTRODUCTION TO RISK MANAGEMENT

Every decision we make in business or projects carries a degree of uncertainty. Whether it's launching a new product, investing in new technology, or hiring new staff, there is always the chance that events may turn out better or worse than expected. This uncertainty is what we call **risk**, and **Risk Management** is the discipline that helps us deal with it effectively.

Introduction to Risk

Risk is the possibility that an **event or condition** will occur and **affect the achievement of objectives**, positively or negatively.

- **Key Factors**:
  a. **Probability** – The chance that the event will occur.
  b. **Impact** – The effect on objectives if the event does occur.

Examples:

- **Negative Risks***: Cyberattack, equipment breakdown, budget overrun.*
- **Positive Risks***: New market opening, technological breakthrough.*

Risk Management is a **systematic process** of identifying, analyzing, and responding to project or organizational risks.

It involves:

- *Recognizing what could go wrong or right.*
- *Assessing how likely it is to happen.*
- *Planning how to minimize threats and maximize opportunities.*
- *Continuously monitoring for new or changing risks.*

Importance of Risk Management

1. **Prevents losses** by anticipating problems.
2. **Improves decision-making** by providing a structured approach.
3. **Protects resources** such as time, money, and human capital.
4. **Increases the chance of success** by preparing for uncertainties.
5. Ensures **compliance** with legal, safety, and industry standards.

Risk Management Principles

The principles of risk management provide the foundation for making **effective, consistent**, and **informed decisions** in the face of uncertainty.

These principles are widely recognized in standards such as **ISO 31000:2018** and can be applied to businesses, projects, and even personal decision-making.

1. **Proactive, not reactive** – anticipate issues before they happen.
2. **Continuous process** – monitor risks throughout the project lifecycle.
3. **Integrated approach** – consider risks in all aspects (technical, financial, operational).
4. **Stakeholder involvement** – include all relevant parties in risk discussions.

↳ The Risk Management Process

Risk management is not just about avoiding problems—it's about **systematically handling uncertainty** to protect objectives and take advantage of opportunities. The **Risk Management Process** is a step-by-step approach used to identify, assess, respond to, and monitor risks.

Standards like **ISO 31000** and the **PMBOK Guide** outline similar processes, which can be adapted for any organization or project.

➢ Standard Steps

a. **Risk Identification** – *Recognizing potential threats or opportunities*.
   - **Goal**: Recognize potential events or situations that may affect objectives.
   - **Methods**: Brainstorming, checklists, historical data, expert judgment, SWOT analysis.

   Example:
   - *A software company identifies risks such as data breaches, server downtime, and regulatory changes.*

b. **Risk Analysis** – *Assessing the likelihood and impact*.
   - **Goal**: Understand the nature of the risk, its cause, and its possible effects.

   Example:
   - *Assigning a 70% probability to server downtime with an estimated ₱500,000 impact.*

c. **Risk Prioritization** – *Ranking risks based on severity*.
   - **Goal**: Compare the level of risk against **risk criteria** (tolerance or appetite).
   - **Action**: Determine which risks are acceptable and which require action.

   Example:
   - *Accepting small cost overruns but acting on risks that may cause project delays.*

d. **Risk Response Planning** – *Choosing strategies to mitigate, avoid, transfer, or accept risks.*
   - **Goal**: Decide and implement actions to address each risk.

e. **Risk Monitoring and Review** – Tracking risks and adjusting plans as necessary.
   - **Goal**: Continuously track identified risks and scan for new ones.
   - **Includes**: Updating risk registers, reassessing likelihood/impact, and reviewing the effectiveness of responses.

   Example:
   - *Monthly review meetings to check if cybersecurity controls are still effective.*

↳ Types of Risk

Risks come in many forms, depending on the source, nature, and area of impact. Understanding the **different types of risk** helps organizations plan the right strategies to manage them.

In risk management, risks are often grouped into **categories** so they can be analyzed and addressed more effectively.

1. **Strategic Risks**

- Long-term business decisions (e.g., entering a new market).
- Risks that affect an organization's long-term goals, plans, and overall direction.
- **Impact**: Can threaten business growth or sustainability.

Examples:
- *Entering a new market without sufficient research.*
- *Competitors introducing superior products.*

2. **Operational Risks**
   - Day-to-day business activities (e.g., equipment breakdown).
   - Risks arising from day-to-day business operations.
   - **Impact**: May disrupt productivity and increase costs.

   Examples:
   - *Machine breakdowns.*
   - *Inefficient processes.*
   - *Human errors in routine tasks.*
3. **Financial Risks**
   - Related to funding, cash flow, and investments.
   - Risks related to money management, funding, and economic conditions.
   - **Impact**: Can affect profitability and cash flow.

   Examples:
   - *Currency exchange rate fluctuations.*
   - *Credit defaults.*
   - *Unexpected inflation.*
4. **Compliance Risks**
   - Violations of laws or regulations.
   - Risks from violating laws, regulations, or contracts.
   - **Impact**: May lead to legal penalties, fines, or reputational damage.

   Examples:
   - *Non-compliance with data privacy laws.*
   - *Breach of industry-specific regulations.*
5. **Environmental Risks**
   - Natural disasters or climate-related issues.
   - Risks arising from environmental factors and sustainability issues.
   - Impact: Can disrupt operations and supply chains.

   Examples:
   - *Natural disasters (floods, earthquakes).*
   - *Climate change effects.*
6. **Reputational Risk**
   - Risks that damage the organization's image and stakeholder trust.
   - **Impact**: Can lead to loss of customers and revenue.

   Examples:
   - *Negative publicity on social media.*
   - *Product recalls.*
7. **Security and Safety Risk**
   - Risks to the safety of people, assets, or information.
   - Impact: May cause injury, data loss, or service interruption.

   Examples:
   - *Cybersecurity attacks.*
   - *Workplace accidents.*

Risk Register

A **Risk Register** is a tool used to document:

- **Risk ID:** Unique identifier for each risk.

- **Risk Description:** Clear statement of the risk event.
- **Category:** Type of risk (technical, financial, schedule, operational, etc.).
- **Probability:** How likely the risk is to occur (e.g., High/Medium/Low or % value)
- **Impact:** The potential effect if the risk occurs (on cost, schedule, quality, etc.).
- **Priority:** Derived from probability × impact (helps rank risks).
- **Response Strategies:** Actions planned to reduce or eliminate the risk.
- **Risk Owner**: Person responsible for managing the risk.
- **Status:** Current state (Open, In Progress, Closed).

Example :

Risk ID	Risk Description	Category	Likelihood	Impact	Priority	Mitigation/Response	Owner	Status
R1	Supplier delay in hardware delivery	Schedule	High	High	Critical	Identify backup suppliers; negotiate buffer stock	Project Manager	Open
R2	Cybersecurity breach	Technical	Medium	Very High	Critical	Install firewalls, conduct penetration testing	IT Security Lead	In Progress
R3	Budget overrun due to scope creep	Financial	Medium	High	High	Strict change control; periodic budget reviews	Finance Lead	Open
R4	Key staff resignation	Resource	Low	Medium	Moderate	Cross-train staff; maintain knowledge repository	HR Manager	Open
R5	Regulatory compliance issue	Compliance	Low	Very High	High	Regular compliance audits; legal consultation	Compliance Officer	Closed

RISK IDENTIFICATION AND ANALYSIS

Risk identification and analysis are the foundation of effective risk management. Before an organization can **respond** to risks, it must first **find them** and **understand their potential impact**. This process ensures that no significant threats or opportunities are overlooked.

Risk Identification

Risk identification is the process of **detecting and describing potential risks** that could affect objectives.

- **Goals**
  a. Recognize **all possible risks**, both internal and external.
  b. Create a **risk register** for documentation.
  c. Prepare for risk assessment and response planning.
- **Common Risk Sources:**
  1. **Technical Risks:** system failures, software bugs
  2. **Management Risks:** poor communication, unclear objectives
  3. **External Risks:** legal changes, natural disasters
  4. **Operational Risks:** process inefficiencies, resource shortages
- **Common Risk Identification Techniques**
  1. **Brainstorming**
     - Gathering ideas from team members about possible risks.
     - A group discussion where team members freely suggest potential risks.
     - **Advantage:** Encourages creativity, diverse perspectives.

Example:

- *A software development team is brainstorming possible delays, bugs, or security flaws.*

2. **Interviews**
   - Consulting experts or stakeholders
   - One-on-one or group interviews with experts, stakeholders, or project members.
   - **Advantage:** Provides deep insights from experienced individuals.

Example:

- *Interviewing a cybersecurity expert to identify potential data breach threats.*

3. **Checklists**
   - Using industry-specific lists of known risks.
   - Using predefined lists of known risks from similar projects or industry standards.
   - **Advantage:** Prevents missing common risks.

Example:

- *Construction safety checklist covering equipment, weather, and legal compliance.*

4. **SWOT Analysis**
   - Identifying risks through Strengths, Weaknesses, Opportunities, Threats.
   - Analyzing **Strengths, Weaknesses, Opportunities, Threats** to spot internal and external risks.
   - **Advantage:** Balances risk identification with opportunity spotting.

Example:

- *Identifying "weak supplier relationships" as a threat in a supply chain project.*

5. **Historical Data Review**
   - Studying past projects and incidents.
   - Reviewing records of past projects, incident reports, and lessons learned.
   - **Advantage:** Learns from real experiences to avoid repeating mistakes.

Example:

- *Analyzing previous IT outages to predict possible system failures.*

6. **Delphi Technique**
   - Gathering opinions from a panel of experts anonymously over multiple rounds until consensus is reached.
   - **Advantage:** Reduces bias, promotes honest input.

Example:

- *Risk forecasting for a new product launch with multiple industry experts.*

7. **Process Mapping / Flowcharting**
   - Spotting risks in each step of a process.
   - Visualizing the workflow to identify possible points of failure or bottlenecks.
   - **Advantage:** Makes hidden risks visible in complex processes.

Example:

- *Flowcharting a manufacturing process to identify quality control gaps.*

8. **Cause-and-Effect Analysis (Fishbone Diagram)**
   - Identifying root causes of potential risks by categorizing contributing factors.
   - **Advantage:** Prevents focusing only on symptoms.

Example:

- *Identifying causes of potential shipment delays: weather, transport issues, and customs.*

Risk Analysis

Risk Analysis is the process of examining identified risks to understand their **nature, causes, likelihood, and potential impact** on a project, system, or organization.

It helps decision-makers determine:

- *Which risks are most critical?*
- *How they should be prioritized.*
- *What responses or controls should be applied?*

➢ Types of Risk Analysis

1. **Qualitative Risk Analysis**

- It is the process of **evaluating and prioritizing risks** using **descriptive (non-numerical) methods**.
- It assesses risks based on their **probability of occurrence** and **impact** on project objectives (cost, time, scope, quality).
- Focuses on **probability and impact scales** (e.g., High/Medium/Low).

☑ Techniques

a. **Risk Probability-Impact Matrix**

- Risks are rated based on probability (likelihood) and impact (severity).
- The matrix helps classify risks as **High, Medium, or Low priority**.

b. **Risk Categorization**

- Group risks by source (technical, financial, operational, compliance).
- Helps identify **recurring risk patterns**.

c. **Risk Urgency Assessment**

- Evaluates how quickly a response is needed.

Example:

- *Risk of regulatory deadline missed = urgent; staff turnover risk = less urgent.*

d. **Expert Judgment**

- Input from subject matter experts or experienced project managers.

Example:

- *Evaluating that supplier delay has a High probability and Medium impact.*
- *Entry in Risk Register*

RISK ID	DESCRIPTION	PROBABILITY	IMPACT	PRIORITY	CATEGORY	NOTES
R-01	Key team member quits	High	High	Critical	HR	Requires a mitigation plan
R-02	Minor spec change	Medium	Low	Low	Scope	Acceptable risk
R-03	New tool integration	Low	High	Medium	Technical	Monitor during implementation

2. **Quantitative Risk Analysis**

- Uses **numerical and statistical methods**.
- Measures risk in terms of **cost, time, or performance impacts**.
- Involves techniques like:
  - *Expected Monetary Value (EMV) Analysis*
  - *Monte Carlo Simulation*
  - *Decision Tree Analysis*

- *Sensitivity Analysis*

☑ **Techniques**

a. **Expected Monetary Value (EMV) Analysis**

- Expected Monetary Value (EMV) is a quantitative risk analysis technique used to calculate the average outcome of uncertain events in terms of money or cost.
- It considers both:
  - *The probability of a risk occurring.*
  - *The monetary impact (cost or benefit) if the risk occurs.*

→ **Formula:**

$$\text{EMV} = \text{Probability of Event} \times \text{Impact (Cost or Benefit)}$$

→ **Steps in EMV Analysis**

1. **Identify risks** (from the risk register).
2. **Assign probabilities** to each risk (0–1 or 0%–100%).
3. **Estimate impact** (in cost, schedule, or resources).
4. **Calculate EMV** for each risk.
5. **Sum EMVs** across all risks to determine **overall risk exposure**.

Example

- **Scenario***: A software project may face these risks:*

Risk	Probability	Impact (Cost)	EMV (Probability × Impact)
R1: Supplier delay	0.3 (30%)	–$50,000	–$15,000
R2: Scope creep	0.2 (20%)	–$80,000	–$16,000
R3: Server upgrade reduces downtime	0.4 (40%)	+$30,000 (benefit)	+$12,000

- **Total EMV = –$15,000 + (–$16,000) + $12,000 = –$19,000**
  - *This means the project should allocate $19,000 as a contingency reserve to cover potential losses.*

- *If the probability of a server crash is 20% and it would cost $10,000, then:*

EMV = 0.2 x 10,000 = **$2,000**

b. **Monte Carlo Simulation**

- Monte Carlo Simulation is a quantitative risk analysis technique that uses repeated random sampling to model the probability of different outcomes in a project.
- It helps answer:
  - *What is the probability of finishing on time?*
  - *What is the probability of staying within budget?*
- Instead of a single estimate, it produces a range of possible outcomes with probabilities.

Example:

- **Scenario:** *A project manager estimates an activity duration as*
  - ✓ *Optimistic (O): 8 days*
  - ✓ *Most Likely (M): 10 days*
  - ✓ *Pessimistic (P): 14 days*
- **Using Monte Carlo Simulation:**
  - ✓ *The model randomly samples thousands of times between 8–14 days.*

- ✓ *Results may show:*
  - 70% probability that the task finishes in 10 days or less.
  - 90% probability that the task finishes in 12 days or less.

c. **Sensitivity Analysis**

- Sensitivity Analysis is a quantitative risk analysis technique used to determine which risks or variables have the greatest impact on project objectives (cost, schedule, performance).
- It helps answer the question:
  - *"Which risk matters the most?"*

→ **How It Works**

1. List project risks or uncertain variables (e.g., cost of materials, task duration).
2. Change one variable at a time while keeping others constant.
3. Observe the effect on the project objective (cost, time, quality).
4. Rank risks based on their level of impact.

Example:

Risk / Variable	Impact on Project Duration (days)
Supplier delivery delay	±20 days
Software development errors	±15 days
Testing & QA issues	±10 days
Minor staff turnover	±5 days

d. **Decision Tree Analysis**

- A decision tree maps decisions and uncertain events in a tree diagram so you can compute the Expected Monetary Value (EMV) of each decision path and pick the best option under uncertainty.
- Elements:
  - **Decision nodes (□)** — choices you control.
  - **Chance nodes (○)** — uncertain events with probabilities.
  - **Branches** — actions or outcomes.
  - **Payoffs** — values (costs or benefits) at the ends.
  - **Probabilities** — assigned to chance branches (sum = 1 at each chance node).

→ **Steps To Use A Decision Tree**

1. Draw the tree: start with a decision node, then branches for alternatives.
2. For each uncertain event, draw chance branches and assign probabilities.
3. Attach payoffs (monetary values) at terminal nodes.
4. Calculate EMV at each chance node:

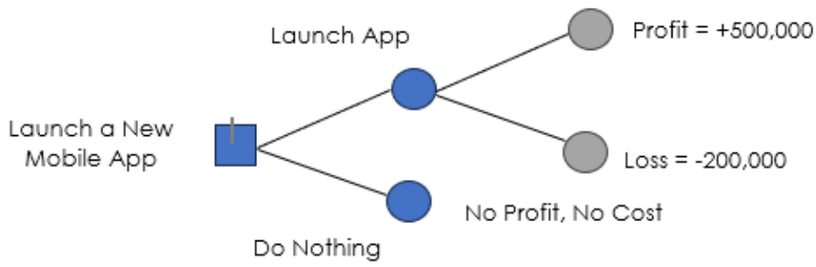
$$\mathbf{EMV=\sum(probability \times payoff)}$$

5. Roll back values: at decision nodes, pick the branch with the **highest EMV** (if maximizing).
6. Choose the decision with the best overall EMV

Example:

- **Scenario:** *A company is deciding whether to launch a new mobile app or not.*
  - **Option A: Launch App**
    - *High Market Demand (prob = 0.4): Profit =* ***₱500,000***
    - *Low Market Demand (prob = 0.6): Loss =* ***₱200,000***

- **Option B: Do Nothing**
  - No cost, no profit → **₱0**



EMV (Launch App) = (0.4 x 500,000) + (0.6 x -200,00)

= 200,000 – 120,000 = **<u>₱80,000</u>**

Decision Node:

- Launch App = ₱80,000
- Do Nothing = ₱0

➢ **Steps in Risk Analysis**

1. **Identify Risks:** Collect risks from brainstorming, checklists, expert judgment, etc.
2. **Assess Probability:** Estimate how likely each risk is to occur.
3. **Assess Impact:** Determine the effect on cost, time, scope, or quality if the risk occurs.
4. **Prioritize Risks:** Rank risks using matrices, scoring, or simulations.
5. **Document in Risk Register:** Record results (probability, impact, ranking, and potential responses).

Example:

- **Scenario:** *Developing an e-commerce platform*.
  - **Risk Identified:** *Cybersecurity Breach.*
  - **Qualitative Analysis:**
    - *Probability: High*
    - *Impact: Very High (loss of customer trust, legal fines)*
  - **Quantitative Analysis:**
    - *30% chance of $500,000 financial impact from potential breach.*
  - **Action:** *Prioritize investment in advanced firewalls and penetration testing.*

<u>RISK RESPONSE PLANNING</u>

Risk Response Planning is the process of developing strategies and actions to address identified risks. It ensures that when a risk event occurs, the organization knows what to do, who will do it, and how to do it. This step follows Risk Analysis and is essential for minimizing threats and maximizing opportunities.

🡻 Risk Response Strategies

1. **Strategies for Negative Risks (Threats)**

a. **Avoidance:** Eliminate the risk by changing the plan.

Example:

- *Choosing a different supplier to avoid delays from a high-risk vendor.*

b. **Mitigation:** Reduce the likelihood or impact of the risk.

Example:

- *Conducting extra testing to reduce the chance of software bugs.*

c. **Transfer**: Shift the risk to a third party (often through contracts or insurance).

Example:

- *Purchasing insurance for shipment damage.*

d. **Acceptance**: Acknowledge the risk and decide to take no immediate action but monitor it.

Example:
- *Proceeding with an outdoor event despite possible light rain.*

2. **Strategies for Positive Risks (Opportunities)**

a. **Exploit**: Take actions to ensure the opportunity occurs.

Example:
- *Assigning your best team to a project to guarantee early completion.*

b. **Enhance**: Increase the probability or impact of the opportunity.

Example:
- *Offering staff incentives to boost productivity.*

c. **Share**: Partner with others to maximize the opportunity's benefits.

Example:
- *Co-developing a new product with another company.*

d. **Accept**

- Recognize the opportunity but take no action unless it occurs naturally.

Example:
- *Being open to unexpected positive market trends.*

Components of a Risk Response Plan

1. **Risk Description**
   - A clear and concise statement of the risk.
   - Should answer: *What is the risk?* and *Why is it a concern?*

   Example:
   - *"Supplier delays due to political unrest may postpone product launch."*

2. **Risk Category**
   - Groups the risk into a specific type (technical, financial, operational, environmental, etc.).
   - Helps in prioritizing and assigning to the right experts.

   Example:
   - *"Operational Risk – Supply Chain."*

3. **Risk Owner / Responsible Person**
   - The individual or team accountable for monitoring and managing the risk.
   - This ensures clear responsibility — no confusion over who should act.

   Example:
   - *The Procurement Manager is responsible for supplier-related risks.*

4. **Chosen Response Strategy**
   - The approach to address the risk, depending on whether it is:
     - Negative Risk (Threat): Avoid, Mitigate, Transfer, Accept.
     - Positive Risk (Opportunity): Exploit, Enhance, Share, Accept.

   Example:
   - *"Mitigation – arrange alternative suppliers."*

5. **Specific Actions**
   - Detailed steps to implement the chosen strategy.
   - Must be practical, measurable, and time-bound.

   Example:
   - *"Sign contracts with two backup suppliers within 30 days."*

6. **Timeline / Action Schedule**

- When each action should be completed.
- Helps ensure readiness before the risk event can occur.

Example:
- *"Backup suppliers to be contracted before September 15."*

7. **Contingency Plan**
   - A backup plan if the primary response fails.
   - Ensures operations can continue with minimal disruption.

   Example:
   - *"If all suppliers fail, shift production to in-house facilities."*
8. **Trigger Conditions**
   - Warning signs or indicators that the risk event is about to happen.
   - Allows for early activation of the plan.

   Example:
   - *"News reports of transport strikes lasting more than 3 days."*
9. **Required Resources**
   - Budget, personnel, and tools needed to execute the response.
   - Prevents delays caused by a lack of preparation.

   Example:
   - *"₱150,000 budget for expedited shipping."*
10. **Monitoring & Reporting Method**
    - How progress and effectiveness will be tracked and communicated.
    - Ensures the plan stays updated and relevant.

    Example:
    - *"Monthly risk review meeting with project team."*

RISK MONITORING AND CONTROL

Risk Monitoring and Control involves a set of ongoing activities to ensure risks are managed effectively throughout a project or operational process. It ensures that the risk management plan remains **relevant** and **effective** throughout the project or organizational operations.

Risk Monitoring and Control is the **continuous process** of:

- *Tracking identified risks*
- *Monitoring residual risks*
- *Identifying new risks*
- *Evaluating the effectiveness of risk responses*

↳ Activities in Risk Monitoring and Control

1. **Tracking Identified Risks**
   - Regularly reviewing previously identified risks to monitor their **status and trends**.
   - Comparing actual risk events with the predicted probability and impact.

   Example:
   - *Checking monthly if a supplier delay risk is still probable after backup suppliers were engaged.*
2. **Monitoring Residual Risks**
   - Observing and evaluating **leftover risks** after responses have been implemented.

- Ensuring these residual risks are at **acceptable levels**.

Example:

- *After cybersecurity upgrades, continue to monitor for phishing attacks.*

3. **Identifying New Risks**
   - Continuously scanning for risks that **emerge during the project** due to:
     - Market changes
     - Regulatory updates
     - Technology evolution

Example:

- *A sudden change in tax law introducing unexpected compliance requirements.*

4. **Evaluating Risk Response Effectiveness**
   - Assessing whether the chosen **risk response strategies** are working as intended.
   - Modifying plans if the risk persists or changes.

Example:

- *If dual-supplier arrangements still result in delays, consider local sourcing.*

5. **Updating the Risk Register**
   - Keeping the **risk register** current by:
     - Revising probability and impact ratings
     - Adding new risks
     - Closing risks that are no longer relevant

Example:

- *Moving a resolved risk to the "closed" section of the register.*

6. **Conducting Risk Audits and Reviews**
   - Performing **formal and informal reviews** of the entire risk management process.
   - Ensuring compliance with organizational policies and best practices.

Example:

- *Quarterly risk audits to verify mitigation steps were implemented.*

7. **Implementing Corrective and Preventive Actions**
   - Adjusting plans to:
     - Correct problems that have occurred
     - Prevent potential problems from becoming actual risks

Example:

- *Adding a backup server after detecting capacity shortages during peak load.*

8. **Communicating Risk Status**
   - Keeping **stakeholders informed** about current risks, changes, and response progress.
   - Using reports, dashboards, and meetings for transparency.

Example:

- *Weekly project update email containing the top 5 active risks.*

REFERENCES

- Pressman, Roger S, Software Engineering: A Practitioner's Approach, 9th Edition, Published by Mc Graw-Hill (2019)
- Sommerville, Ian, Software Engineering 10th Edition, Published by Pearson Education, Inc (2016)
- Bass, Len, Clements, Paul, & Kazman, Rick., Software Architecture in Practice (3rd Edition). Addison-Wesley, 2012