Software Risk Management

Syllabus

Unit	Contents	Lectures
3.	• **Software Risk Management** → Introduction to software risk → Types of Risk → Nature of Risk → Software Risk Management → Risk Mitigation Management • **Software Reliability**	**10**

Introduction to Software Risk

- Software Risk is a measure of the probability of its occurrence and the loss due to its exposure.
- The Software Risk affects the process of development, project development and the software product itself.
- The Software Risk is possible in software process, project and product management.
- Software Risk arises due to uncertainties in management and the ineffectiveness of technical procedures.

Types of Software Risk

- Software Process Risk
- Software Project Risk
- Software Product Risk

Software Process Risk

- Includes managerial and technical procedures required to be undertaken for software development.
- Managerial processes includes activities like planning, staffing, monitoring, quality assurance and control.
- Technical procedures include software engineering activities like requirement analysis, design, code and test.
- Process Risk occurs due to uncertainties involved in assessing, estimating various inputs to the software process, resource availability, confirmed quality specifications from customer.

Software Process Risk …

- In technical procedures, uncertainty may be on account of the customer not being able to confirm in precise terms the software requirement specifications or uncertainty about platform, its capability and configuration.
- These uncertainty affect quality, efforts, cost and schedule enhancing business risk.

Software Project Risk

- Arises on account of operational, organizational and contractual software development factors.
- Occurs due to conditions and constraints about resources, relationship with vendors and contractors, unreliable vendors and lack of organizational support.
- Occurs due to internal budgeting constraints and unreliable customer payments.

Software Product Risk

- Concern the quality characteristics of software product.
- Originates from the conditions like unstable requirement specifications, not being able to meet the design specifications affecting software performance and uncertain test specifications.
- There is a risk of losing the business and facing strained customer relations.

Nature of Software Risk

- Technology Risk
- People Risk
- Organizational Risk
- Requirement Risk
- Estimation Risk

Technology Risk

- These risks fall in the domain of hardware, software and network communication technology, which are subject to continuous improvement and may lead to obsolescence.

People Risk

- These are the risks associated with persons in the teams and risk concerns availability, capability, skills, maturity and so on.

Organizational Risk

- These are in the area of development organization and customer organization.
- The environment in both the organization is a matter of concern.

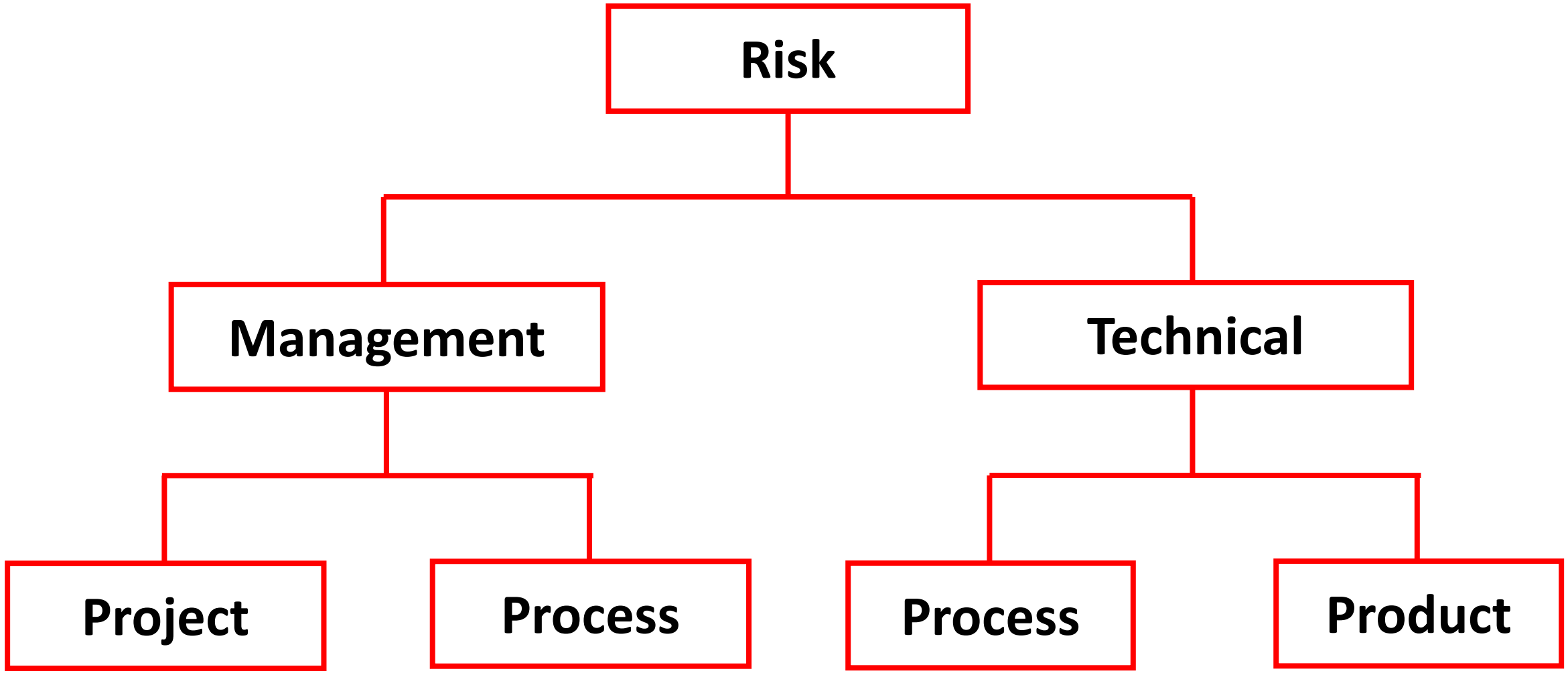
Requirement Risk

- This is about clarity, completeness and confirmation of the requirement by the end users and customer.
- It is about the volatility of the requirement.

Estimation Risk

- Not being able to judge in precise terms the component of the software, reusability and system characteristics affecting the size, effort and schedule.

Risk Hierarchy



Risk Management

- Risk Management is a scientific process based on the application of game theory, decision theory, probability theory and utility theory.
- Risk Management is a process made up of following steps.
  - Risk Identification
  - Risk Analysis
  - Risk Assessment
  - Risk Planning for Resolution
  - Risk Monitoring
  - Risk Mitigation

Risk Identification

- Identifies and enumerates the risk.

Risk Analysis

- Enables an understanding of the occurrence, impact and timing of occurrence of risk.

Risk Assessment

- Quantified in terms of the probability of occurrence, loss on occurrence and the risk exposure.

Risk Planning for Resolution

- Provides approach in terms of effective steps in dealing with risk in terms of strategies and execution.

Risk Monitoring

- Helps to identify and measure the occurrence, impact and implications of risk till it is resolved satisfactorily.

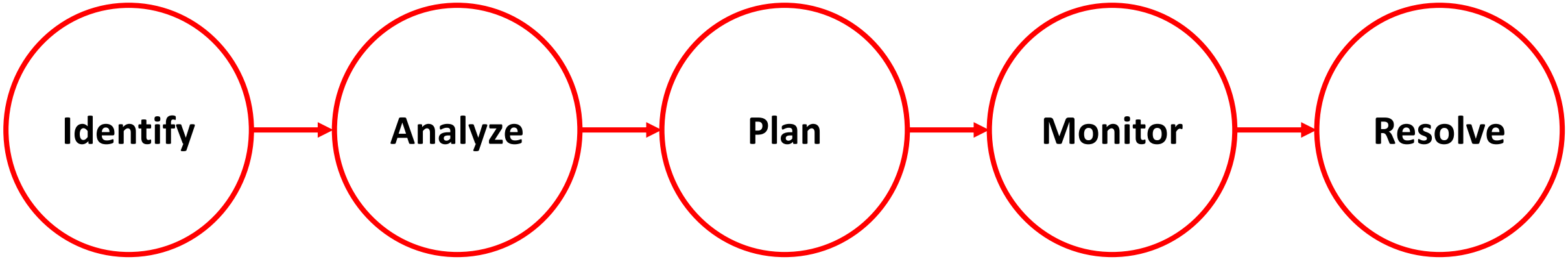
Risk Mitigation

- Helps to meet the challenges or risk occurrence in effective implementation of specific plan of risk management.

Software Risk Management

- Software Risk Management process is done using following steps
  - Identify
  - Analyze
  - Plan
  - Track
  - Resolve

Software Risk Management …



Software Risk Management : Identify Risks

- Risk identification is a process to handle certain inputs that produce a set of outputs i.e. a list of risks, their types and its importance in the context of the software proposed to be developed.
- The inputs are the degree of uncertainty on a number of features like requirements, technology, people allocation, insufficient domain and application knowledge, concerns about lack of skills and knowledge, and issues regarding the technical and commercial aspects of the software development.

Software Risk Management : Identify Risks …

- The above inputs help to identify the risks and their nature. In order to ensure that risk identification is complete, organizations develop checklists that are used to identify the risks.
- The organizations also maintain risk database provided they have handled small or large software development projects.
- The checklist, risk database and risk assessment forms are the facilitation in the risk identification process.

Software Risk Management : Identify Risks …

- The risk identification process begins with an assessment using the check list.
- The assessment is best done when it is conducted as a participatory activity.
- The risk analyst conducts interviews with experienced personnel who have worked earlier in similar software projects.
- Periodic meetings are conducted with persons with persons to identify the risk.

Software Risk Management : Identify Risks …

- It should be noted that risk identification is not a one time exercise that is undertaken at the beginning of the life cycle; in fact it is an exercise that continues till the software is delivered satisfactorily
- Once the risk is identified, its attributes i.e. the probability of occurrence and the loss arising out of risk are determined.
- Both these attributes are based on the subjective judgement of the people concerned. The judgement may be supported by risk database and the experience of people in the field.

Software Risk Management : Identify Risks …

- The loss may not be monetary, but could emerge in the form of adverse effect on the quality of the software which include features like flexibility, maintainability, portability, reliability, reusability etc.

Software Risk Management : Analyse and Assess Risks

- Risk Analysis is the process that defines activities and methods to estimate and evaluate risk.
- During the risk estimation, the probability of occurrence and consequences of the risk is estimated.
- During the risk evaluation process, the risk options against certain predefined criteria are discussed.
- The Risk Analysis process begins with list of risks obtained from the previous process of risk identification. Each risk from the list is taken for estimation and evaluation.

Software Risk Management : Analyse and Assess Risks …

- To act on this step, the organization needs an evaluation criteria and the risk database.
- First the probability and consequence is estimated and then risk exposure is determined.
- **Risk Exposure = Probability X Loss**.
- At the end of the risk analysis, we will get a prioritized risk list with probability, risk exposure and risk severity.
- This forms the basis for constructing a risk action plan for resolution.

Software Risk Management : Risk Plan

- The risk plan proposes various actions to deal with the risks identified and analyzed.
- The output of the process is the Risk Action Plan i.e. RAP.
- RAP takes as input the Prioritized Risk List based on risk severity and determines resolution strategies for each risk present on the risk list.
- The risk resolution strategies as suggested by Ellan Hall are
  - Risk Acceptance
  - Risk Avoidance

Software Risk Management : Risk Plan …

- Risk Protection
- Risk Reduction
- Risk Research
- Risk reverses
- Risk Transfer

Risk Strategy :Risk Acceptance

- This strategy is chosen when we have no choice but to live with the risk and face the consequences.

Risk Strategy :Risk Avoidance

- This strategy is chosen to eliminate risk altogether or bypass the risk altogether.
- This strategy is chosen when we are in the situation of lose – lose.

Risk Strategy :Risk Protection

- This strategy is chosen when there is a possibility to reduce the probability of occurrence of risk and the consequential loss

Risk Strategy :Risk Reduction

- This strategy is chosen over and above the risk protection.
- Based on cost benefit analysis, the organization may take actions to reduce the incidence of the risk, thus giving rise to major reduction in the consequential loss.

Risk Strategy :Risk Research

- This strategy is chosen to reduce the risk by seeking more information about the risk for better evaluation and to deal with risk more effectively.
- We can conduct a proof of concept exercise or experiments to reduce the volatility of the requirement specifications.
- The organization may seek information from genuine resources on new product or introduction of new technology.

Risk Strategy :Risk Reserves

- This strategy is chosen when the risk severity is low but the risk acceptance is not possible.
- We can build a contingency plan to deal with this risk in case of the occurrence of the risk.
- We may provide extra slack in schedule, keep a reserve on the call.
- Reserve funds for the emergency.

Risk Strategy :Risk Transfer

- This strategy is used when it is possible to transfer the risk to someone else.
- Outsourcing, sub – Contracting , buying a resource or tool as a risk transfer strategy

Tracking Risk

- The risk tracking process monitors risk occurrence, consequences and exposure and provides triggers to act to resolve the risk.
- The tracking process provides methods to keep watch on the various activities that are likely to be affected by the risk. These methods provide feedback on occurrence and impact and trigger the predetermined action.
- The tracking process will have a threshold norm for each risk beyond which the trigger will generate action to resolve the risk by changing strategy or executing the proposed plan of action.

Tracking Risk …

- The risk tracking process has an input on risk status from the project team and from different MIS reports on software development addressing the issue of schedule, cost, delivery and quality. The output of the risk tracking system process is evaluation of exposure, severity and triggers to act where necessary.

Tracking Risk …

- The threshold could be risk exposure or risk severity.
- The risk occurrence is a possibility at any time. The original estimates and forecasts on occurrence, exposure, timing may change during the life cycle and tracking risk becomes an essential activity in risk management system and has to be made or integrated activity in software development plan.

Resolving Risk

- Risk Resolution Process s defined where risk action plan forms the basis for resolving the risk using resolution tools and techniques and risk database.
- The objective of the process is to reduce the risk to the level of acceptable risk.
- The output of the risk resolution process is the list of acceptable risk(s), reduced rework and corrective measures with respect to each risk.

Resolving Risk …

- The Risk Resolution activities are : -
  - Act on Triggers
  - Execute The Risk Acton Plan
  - Monitor The Action Plan and Assess The New Risk Scenario
  - Control The Risk Exposure Through Action and / or Action on Deviation
- The skills required to resolve risk are creativity and collaboration.
- Effective implementation of risk action plan calls for generation of new and innovative ideas.

Resolving Risk …

- This calls for the creativity in the project team.
- The risk action plan implementation is not straight forward. It is a collaborative process and cannot be implemented in isolation.
- The fundamental risk resolution strategy is to reduce uncertainty, gain additional knowledge and draw upon the experience of others from internal and external sources.
- The risk resolution process is not a structured process, in fact it is a process where creativity and collaboration among team members are the key of success.

Resolving Risk …

Process Steps	Inputs	Outputs
Identify Risk	• Uncertainty • Lack of Knowledge • Lack of Concerns • Lack of Issues • Risk Database	**List of Risk by** • Category • Class • Type • Context
Analyze Risk and Assess Risk	• List of Risk • Risk Database	**Risk List with** • Probability • Loss • Exposure • Severity • Priority

Resolving Risk …

Process Steps	Inputs	Outputs
Plan Risk for Resolution	• Prioritized Risk List determining resolution strategies and implementation	• Risk Action Plan i.e. Conversion of strategy into concrete steps for action
Track Risk	• Risk Status Through MIS • Risk Threshold	**Emergence of** • Threshold • Deviation • Triggers to act • Measures and Metrics onto update Risk Database

Resolving Risk …

Process Steps	Inputs	Outputs
Resolve Risk	• Risk Action Plan • Use of Tools and Technologies	**Changing Risk Scenario into** • Acceptable Risk • Reduce Risk Exposure

Risk Mitigation Through RMMM Plan

- Risk Mitigation Planning
- Risk Mitigating i.e. Risk Reducing the impact of risk is done through RMMM Plan.
- RMMM stands for Risk Mitigation, Monitoring and Management.
- RMMM Plan deals with Risk Migration, Monitoring and Management of risks in a systematic manner.
- The steps involved in RMMM Plan are : -
  - Prepare a Prioritized Risk List base on Risk Exposure and Risk Severity Index.

Risk Mitigation Through RMMM Plan …

- Determine Risk Resolution Strategy for Each Risk.
- Design an Acton Plan based on Resolution Strategy to deal with Risk.
- Institute a Monitoring Plan through systematic review and MIS report on risks integrated into software development MIS report.
- Take Corrective Measure to Control the Impact.

Risk Mitigation Through RMMM Plan …

Risk Particulars				RMMM Plan	
Provisional Risk Name	**Risk ID**	**Severity Impact Index**	**Strategy**	**Plan Details**	**Reviews**
Volatility of Requirement Specification due to End Users	6	6	Prevention	• Prototype • Proof of Concept Experimentation	• Prototype implantation • Proof of concept Confirmation

Risk Mitigation Through RMMM Plan …

Risk Particulars				RMMM Plan	
Provisional Risk Name	**Risk ID**	**Severity Impact Index**	**Strategy**	**Plan Details**	**Reviews**
Inexperience and Lack of Skill	22	4	Prevention	• Seminar on Domain Knowledge • Training on Skills	• End of Seminar and Training Courses and revisiting RMP

Risk Mitigation Through RMMM Plan …

Risk Particulars				RMMM Plan	
Provisional Risk Name	**Risk ID**	**Severity Impact Index**	**Strategy**	**Plan Details**	**Reviews**
Staff Turnover	9	9	Acceptance	• No Plan of Action	
Application Knowledge Absent	3	6	Transfer	• Outsource the development	• Periodical

RMMM Plan Document

- (Mature) Software Development Organization prepares an RMMM plan document for each software project and updates the risk database on
  - Risk Type
  - Estimated Impact of Risk
  - Risk Strategy
  - Risk Exposure
  - Estimated Risk
  - Actual Impact of Risk

RMMM Plan Document : Structure

- Software Project Name | ID | Details
- Project Scope Details
- Software Details
  - Customer Wise
  - End User Wise
  - Development Environment Wise
- Risk Statement with Context

RMMM Plan Document : Structure …

- Responsibilities by Risk Type and Assignment
  - Management
  - Operational
  - Technical
- Risk Table with Priorities and Strategies for Resolution
- Action Plan by Risk and Review Framework
- Expected Impact, Monitoring Steps and Stages
- RMMM Plan Review Schedule

RMMM Plan Document : Structure …

- Post–Implementation Risk database Updates
- Post – Implementation Comparative Analysis of Risk Impact on
  - Cost
  - Schedule
  - Effort
  - Scope
  - Quality

Risk Analysis and Management

- Risks are involved with Software Project
- The objective of risk analysis is to identify the risk and assess them to evolve the Risk Management Strategies
- We have to take care about Calculated Risk
- Calculated Risk can be
  - Guarded
  - Monitored
  - Controlled

Risk Analysis and Management …

- Risks are involved with Software Project
- The objective of risk analysis is to identify the risk and assess them to evolve the Risk Management Strategies
- We have to take care about Calculated Risk
- Calculated Risk can be
  - Guarded
  - Monitored
  - Controlled

Risk Analysis and Management Template

- The objective of Risk Analysis and Management is to Identify the Risks in various areas and asses the probability of occurrence and its impact on the project.
- To fix the probability of occurrence and take policy decision of developing

SEI Risk Management Taxonomy

Product Engineering	Development Engineering	Program Constraints
Requirements	**Development Process**	**Resources**
• Stability	• Formality	• Schedule
• Completeness	• Suitability	• Staff
• Clarity	• Process Control	• Budget
• Validity	• Familiarity	• Facilities
• Feasibility	• Product Control	
• Precedent		
• Scale		

SEI Risk Management Taxonomy …

Product Engineering	Development Engineering	Program Constraints
Design	**Development System**	**Contrast**
• Functionality	• Capacity	• Type of Contracts
• Difficulty	• Suitability	• Restrictions
• Interfaces	• Usability	• Dependencies
• Performance	• Familiarity	**Project Interfaces**
• Testability	• Reliability	• Customer
• Hardware Constraints	• System Support	• Associate Contractors
• Non Developmental S/W	• Deliverability	• Sub Contractors

SEI Risk Management Taxonomy …

Product Engineering	Development Engineering	Program Constraints
Code and Unit Test	**Management Process**	**Project Interfaces**
• Feasibility	• Planning	• Customer
• Unit Test	• Project Organization	• Associate Contractors
• Coding / Implementation	• Management Experience	• Sub Contractors
	• Project Interfaces	• Prime Contractors
		• Corporate Management
		• Vendors
		• Statutory Bodies

SEI Risk Management Taxonomy …

Product Engineering	Development Engineering	Program Constraints
Integration and Test	**Management Methods**	
• Environment	• Monitoring	
• Product	• Personal Management	
• System	• Quality Assurance	
	• Configuration Management	

SEI Risk Management Taxonomy …

Product Engineering	Development Engineering	Program Constraints
Engineering Specialties	**Work Environment**	
• Maintainability	• Quality Attitude	
• Reliability	• Co – Operation	
• Safety	• Communication	
• Security	• Morale	
• Human Factors		
• Specifications		
• Safety		

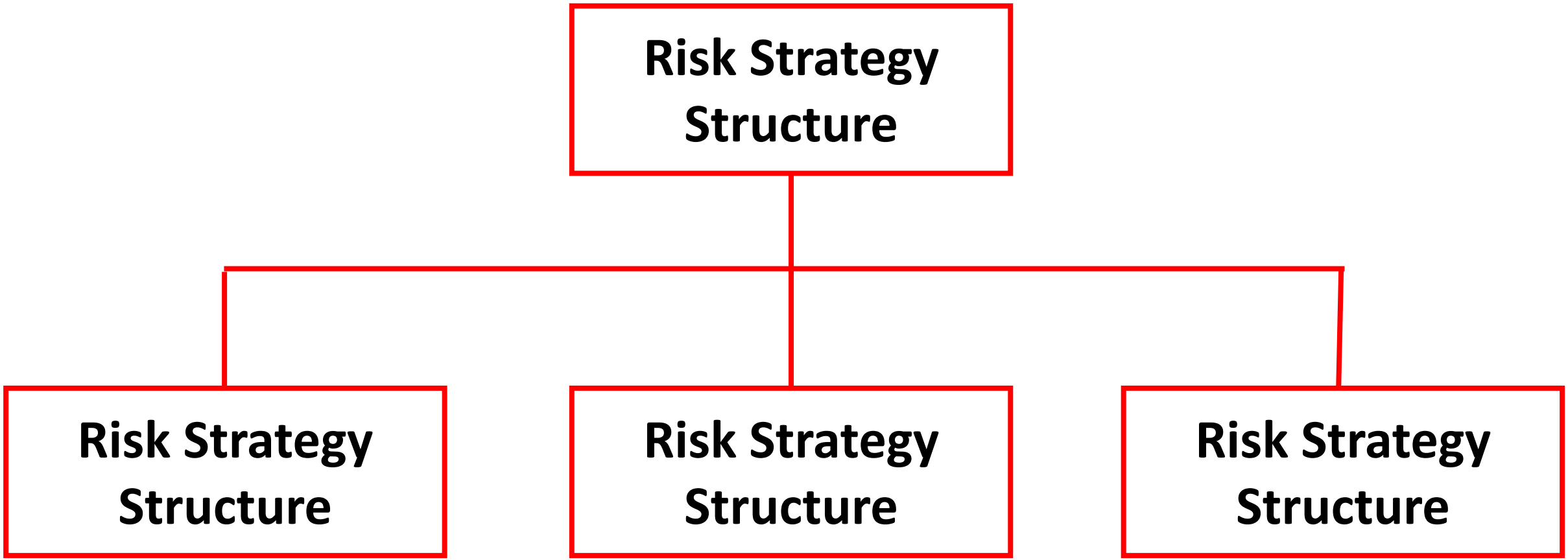
Plan Risk

- Risk plan proposes actions to deal with the risk identified and analyzed in earlier processes.
- The output of the process is the risk action plan.
- Risk Action Plan takes as input prioritized risk list based on severity and determines the resolution strategies for each risk present in the list.

Plan Risk …

- The Risk Goals are
  - Risk Acceptance
  - Risk Prevention
  - Risk Avoidance
  - Risk Protection
  - Risk Reduction
  - Risk Research
  - Risk Transfer
  - Risk Reverses

Plan Risk …


Risk Strategy Structure
Risk Strategy Structure
Risk Strategy Structure
Risk Strategy Structure

Risk Acceptance

- The strategy is chosen when we have no choice but to live with risk and face the consequences.

Risk Avoidance

- The strategy is chosen to eliminate risk altogether or bypass it altogether.
- The strategy is chosen when we are in lose – lose situation.
- We have to deal with the sources of risk avoidance or eliminate them by management actions.

Risk Protection

- The strategy is chosen when these is a possibility to reduce the probability of occurrence and the consequential loss.

Risk Reduction

- Depending upon the Cost – Benefit Analysis, the strategy is chosen over and above risk protection.
- The organization may take such actions that risk incidence is reduced, giving rise to major reduction in consequential loss.

Risk Research

- The strategy is chosen to reduce the risk by seeking more information about it for better evaluation and also to deal with it effectively.
- We have to conduct a proof of concept exercise or experiments to reduce to volatility of the requirement specification.
- We have to seek more information regarding new product or new technology.

Risk Reserves

- The strategy is chosen when the risk severity is low but risk acceptance is not possible.
- We have to build a contingency plan to deal with the risk.

Risk Resolution

- Risk resolution the process is defined where risk action plan forms the basis for resolving the risk using resolution tools and techniques and risk database.
- The main objective of the risk resolution process is to reduce the risk to the level of acceptable risk.
- The output of the risk resolution process is the list of acceptable risk, reduced rework and the corrective action.

Risk Resolution

- Risk resolution the process is defined where risk action plan forms the basis for resolving the risk using resolution tools and techniques and risk database.
- The main objective of the risk resolution process is to reduce the risk to the level of acceptable risk.
- The output of the risk resolution process is the list of acceptable risk, reduced rework and the corrective action.
- Risk resolution activities are
  - Act on the trigger
  - Execute the risk action

Risk Resolution …

- Monitor the action plan and assess the new risk scenario
- Control the risk resolution through action and / or action on deviation.

Risk Monitoring Mitigation Management Plan

- Prepare a prioritized risk list based on risk exposure and the corresponding severity index.
- Determine risk resolution strategy for each risk.
- Design an action plan based on resolution strategy to deal with risk.
- Institute a monitoring plan through systematic review and MIS report on risks integrated into software development MIS report.
- Take corrective measures to control the impact.

Risk MMM Plan Document

- Software Project ID/Name/Details
- Project Scope Details
- Software Details on Customer, End User(s) and the Development Environment
- Risk Statement with Context
- Responsibilities by Risk Type and Assignment
  - Management
  - Operational
  - Technical

Risk MMM Plan Document

- Risk Table with Priorities and Strategies for Risk Resolution
- Action Plans by Risk and Review Framework
- Expected Impact, Monitoring Steps and Stages
- RMMM Plan Review Schedule
- Post Implementation Risk Database Updates
- Post Implementation Comparative Analysis of Risk Impact on Cost, Schedule , Effect, Scope and Quality

Risk Monitor MM Plan Document (Format)

Plan							
PlanID	SystemID	RiskID	OrganizationID	ClientID	Low	Medium	High

Analysis of SEI Software Risk Taxonomy

- Requirement Risk
- Design Risk
- Code and Unit Test Risk
- Integration and Test
- Engineering Specific Risk
- Development Process Risk
- Development System Risk
- Management Process Risk
- Management Method Risk

Analysis of SEI Software Risk Taxonomy …

- Resources Risk
- Contract Risk
- Project Interfaces

Requirement Risks

- Requirement
- Completeness
- Clarity
- Validity
- Feasibility
- Precedent
- Scale

Requirement Risks : Requirement

- Is the requirement stable?
- Check with the end users and senior management for confirmation.
- Unstable requirement is a high – risk scenario.

Requirement Risks : Completeness

- Requirement may be stable, but does it completely solve the problem for which it is raised.
- Incomplete and stable requirement is also a high risk scenario.

Requirement Risks : Clarity

- Requirements are mainly the views of the end users. They may lack clarity, resulting in contradiction and inconsistencies in specifications.
- This happens mainly because users having different perception of problems and perspective on solution.
- Lack of clarity in the communication.

Requirement Risks : Validity

- Requirement specifications should be valid within itself and for solving the problem.
- A stable, complete and clear software requirement may not be valid for the goal of solving the specified business problem.

Requirement Risks : Feasibility

- Feasibility s to be assessed from the point of view of implementing requirement specification.
- It needs to be checked whether the collection and acquisition of necessary data and information is feasible. It not, it is virtually impossible to meet the requirement.

Requirement Risks : Precedent

- Ascertain the experience gained in other projects where similar scenario were handled and a similar requirement was met.

Requirement Risks : Scale

- The details, complexity and rigour of specifications are to be checked for necessity in the software solution.

Design Risks

- Functionality
- Difficulty
- Interface
- Performance
- Testability
- Hardware Constraints
- Non – Developmental Software

Design Risks : Functionality

- Is the design correct and complete to meet the functionality that is expected to deliver requirement specification?

Design Risks : Difficulty

- Is the design very complex so that it may not fulfil the design goals of delivering entire functionality

Design Risks : Interface

- Are interfaces chosen available, capable and appropriate as required in the design to meet the design goals?

Design Risks : Performance

- Is the design capable of giving desired performance on all functions, features and facilities specified in the requirement specifications?

Design Risks : Testability

- Is the design construct testable for all features?
- A good design claim is a total waste if it cannot be tested for all its features.

Design Risks : Hardware Constraints

- A good design needs corresponding hardware platform to function. If there are some constraints, technical or other, the design cannot be implemented effectively.

Design Risks : Non – Developmental Software

- Tools, Libraries and Components that have been considered in design need to be checked for suitability and availability.

Code and Unit Test Risks

- Feasibility Risk
- Unit Test Risk
- Implementation Risk

Code and Unit Test Risks : Feasibility Risk

- There as two aspects of feasibility. They are
  - Writing a code or generating a code
  - Successive testing of the code at the unit level

Code and Unit Test Risks : Unit Test Risk

- Refers to the testability of code at unit level

Code and Unit Test Risks : Implementation Risk

- This s from the point of view of integration into higher level system code.

Integration and Test Risks

- Environment
- Product
- System

Integration and Test Risks: Environment Risk

- The environments are the customer environment, use environment, hardware environment and software environment.
- Usually the above environments are such that the integration and testing becomes high risk proposition.
- The environment that is conducive for design and architecture facilitation, integration and testing highly required.

Integration and Test Risks: Product Risk

- If we want to integrate the product and features to deliver the requirement, then the product features has to match with software features and design.
- The above affects the integration and testing.
- The integration and testing is always a high risk proposition.

Integration and Test Risks: System Risk

- System integration is an issue when multiple platforms and software are in consideration.

Engineering Specific Risks

- Maintainability
- Reliability
- Safety
- Security
- Human factor

Engineering Specific Risks : Maintainability

- Ease of maintenance is an issue when software is large, complex and is configured on multiple platforms.
- In order to bring in high degree or mentainability to facilitate change requirements, upgradation and modification in the software.

Engineering Specific Risks : Reliability

- The reliability factor is looked for at the time of peak hour utilization of the system (resources).
- The extreme conditions like high volume of data handling, large number of users etc. are to be met for the reliability aspect.
- This aspect must be considered in large installations.
- The software is required to be tuned for such extreme conditions.

Engineering Specific Risks : Safety

- Is the system safe from the hackers and unauthorized persons?
- Sensitive and critical systems or software fail in these criteria and hence are major issue to be resolved.

Engineering Specific Risks : Security

- Is the system secure from power failures and protected from key process so that the risk of alter, delete or modification is not present?

Engineering Specific Risks : Human Factor

- Do the design, architecture and documentation require human considerations like ease of use, user friendly, easy to learn etc?
- Usually the (good) software fail on the above grounds because these are not considered properly.

Development Process Risks

- Formality
- Suitability
- Process Control
- Familiarity
- Product Control

Development Process Risks : Formality

- As we have six process models for the development of the system.
- In order to bring in the scientific approach in the development process, we have to use any one of the six process models.

Development Process Risks : Suitability

- The development model that has been chooses for the development of the system has to be suitable to meet the requirement(s) of the customer and the customer requirement specification.

Development Process Risks : Process COntrol

- Project MIS is used to by the project manager(s) to control the process(es).
- In case of the absence of the proper process control, there is high risk.

Development Process Risks : Familiarity

- In case the project development team is familiar with the development process the application of development process tools are going to be effective.

Development Process Risks : Product Control

- When the product is complex in nature, the development is a long term affair.
- Product control plays vital role at the time when the software is being developed in versions by different development teams and each team is responsible for one component of the main project.
- The proper product control helps the developer to deliver the entire scope.

Development System Risk

- Capacity
- Suitability
- Usability
- Familiarity
- Reliability
- System Support
- Deliverability

Development System Risk: Capacity

- The capacity of the development system is linked to the capacity of the project team and whether the organization has a development system in place or not.
- In case of absence of the development system in the organization, the project risk is inivitable.

Development System Risk: Suitability

- For any particular SRS, we can have multiple approaches to development like conventional, object oriented, waterfall model and so on.
- The SRS is going to be handled in best possible manner by any one of the aforesaid approaches.
- The risk is the selection of the appropriate approach.

Development System Risk: Usability

- Even in case of the selection of the appropriate approach is being done, then there is risk that the development system knowledge is adequate or not.

Development System Risk: Familiarity

- If the selection of the appropriate approach is being done and the development system knowledge is adequate then there is the risk that the development team is familiar with the development process or not.

Development System Risk: Reliability

- We cannot have an ideal or perfect development system.
- There is every chance that at the time of delivery of result is as per expectation or not.

Development System Risk: System Support

- In case of weak system support, there are chances that incorrect application or implementation may lead to the associated risk.

Development System Risk: Deliverability

- In case of the risk is perceived high or normal, then the risk is the inability to deliver the entire scope in all its dimensions.

Management Process Risks

- The project management is nothing but Software Project Management discipline.
- In case of the organization does not have a high degree of effective project management culture, discipline and practices, the project risk is going to be very high.

Management Methods Risks

- The management methods are
  - Monitoring
  - Personnel Management
  - Quality Assurance
  - Configuration Management

Management Methods Risks: Monitoring

- In case of SPM is not backed by proper monitoring of key result areas in the software then risk of process and product sets in.

Management Methods Risks: Personnel Management

- In case of the organization is not having the good or appropriate Personnel Management methods, there are going to be HR issues with the project team and are to be resolved at the earliest.
- If Personnel Management and HR policies and methods are not clear, then there is the risk of frequent turnover and low efficiency.

Management Methods Risks: Quality Assurance

- In case of the organization is not having the good or appropriate Quality Assurance Policy in place and in practice then product and process risk are bond to arrive.

Management Methods Risks: Configuration Management

- Configuration Management is nothing but the ensuring the availability of the hardware, software and tools as and when required by the development team to manage processes effectively and efficiently.
- In case of the management is having issues with respect to configuration management, the risk is very high.

Resources

- The resources are
  - Schedule
  - Staff
  - Budget
  - Facilities
- The above are critical resources and if planned resources are not likely to come through, then the organization faces risk with respect to product, process and project.

Contract

- The software development is usually undertaken with outside support. These supports are obtained by virtue of contracts.
- The contract bind the associated parties on a number of aspects. Improper and non monitored contracts pose adverse effect on the main project areas.
- If the contracts are not drafted properly, and further not monitored properly, then the risk of adverse effect on the main project arises.
- The contract also include the contract signed with hardware and software vendors that have specific delivery obligations.

Project Interfaces

- The software development process works through different interfaces.
- The interfaces are
  - Customer
  - Associate Contractors
  - Sub Contractors
  - Prime Contractors
  - Corporate Management
  - Vendors
  - Project Teams

Project Interfaces …

- These interfaces work effectively if and only if relations among them are managed properly.
- In case of the relationship management is poor, project and process risk is enhanced.