Experiment No.: 6

Risk Analysis and Management

Batch: B2 **Roll No.:** 16010421059 **Experiment No.:** 6

Aim

To prepare a risk analysis and management plan document.

Resources needed

Internet Explorer, LaTeX Editor

Theory

Risk management is the identification, assessment, and prioritization of risks followed by coordinated and economical application of resources to minimize, monitor, and control the probability and/or impact of unfortunate events or to maximize the realization of opportunities. Risks can come from uncertainty in financial markets, threats from project failures (at any phase in design, development, production, or sustainment life-cycles), legal liabilities, credit risk, accidents, natural causes and disasters as well as deliberate attack from an adversary, or events of uncertain or unpredictable root-cause. Several risk management standards have been developed including the Project Management Institute, the National Institute of Standards and Technology, actuarial societies, and ISO standards. The strategies to manage threats (uncertainties with negative consequences) typically include transferring the threat to another party, avoiding the threat, reducing the negative effect or probability of the threat, or even accepting some or all of the potential or actual consequences of a particular threat, and the opposites for opportunities (uncertain future states with benefits). Risk Management's goal is to increase the impact and probability of positive risks and decrease them for negative risks. Thus, the understanding of risk management methodologies, tools and practices is extremely important for the future industry workforce to ensure better success of IT projects. Risk management includes six main processes. These are risk management planning,

risk identification, risk analysis, risk response planning, and risk monitoring and control.

IT Project Risk Management Processes

Risk Planning: In the Risk Management Planning process, it is decided how to execute the risk management activities of a project. The level of risk management is decided as it needs to be in line with the risk and importance of the project as a whole.

Risk Identification: Risk identification refers to the process of identifying dangerous or hazardous situations and trying to characterize it. The two main approaches to the identification of risks are the use of checklist and brainstorming.

Risk Analysis: A common problem with risk identification particularly for the more anxious is that a list of risk is potentially endless. Some way is therefore needed of distinguishing the more damaging and likely risk using the formula

$$Riskexposure = (potentialimpact) \times (probabilityofoccurrence)$$

Once risks have been identified, they must then be assessed as to their potential severity of impact (generally a negative impact, such as damage or loss) and to the probability of occurrence.

Risk Response Planning: Having identified the major risks and allocated priorities, the task is to decide how to deal with them. The project manager brainstorms and gathers all the positive and negative risks. It is important to note that this list of risks is not every possible thing that could happen, but rather the category of things that could happen. Consider, for example a project to build a house. Risks to consider would be on the order of slow progress, lack of material, lack of money, change of plans. Not run out of wood or the house catches fire. The purpose of risk planning is to have a plan on how to respond to a type of risk, not figure out all possible risks. So when a risk is realized and becomes an issue or problem, the team knows the steps to assess and respond. These risks would then be inputted into a report followed by the likelihood, impact, and rank of each risk.

Risk Monitoring and Control: The final input for Risk Management would be the control/treatment plans for each risk in case the risk unfolds into the project down the timeline. The Risk Monitoring and Control process is where the risks are diagnosed with treatment and control plans.

Activity

1. Identify a list of at least 10 risks using the given checklist, organizing a stakeholders brainstorming session.

2. Estimate the probability of occurrence of each risk on the scale of 1-10, risk impact on the scale of 1-10, and calculate risk exposure.

3. Develop a contingency plan of risk as per the given template in LaTeX.

Template

Risk Assessment and Risk Management Plan.

Risk #1:
Likelihood of risk: (on the scale of 1-10)
Potential impact on the project: (on the scale of 1-10)
Risk Exposure = (potential impact × Likelihood)
Ways to address this risk:

Risk #2.....
Risk #n.....

Risk Checklist: It is the first stage of risk management. It is a systematic attempt to specify possible threats to the project plan.

Risk	**Risk Reduction Technique**
Personal shortfalls	Staffing with top talent; job matching; team building; training and career development; early scheduling of key personnel
Unrealistic time and cost estimates	Multiple estimation techniques; design to cost; incremental development; recording and analysis of past projects; standardization of methods
Developing the wrong software function	Improved software evaluation; formal specification methods; user surveys; prototyping; early user manuals
Developing the wrong user interface	Prototyping; task analysis; user involvement
Gold plating	Requirement scrubbing; cost benefit analysis; design to cost
Late changes to requirements	Change control procedure; incremental development
Shortfalls in externally supplied components	Quality assurance procedures; competitive design or prototyping; contract incentives
Real-time performance shortfalls	Simulation; benchmarking; prototyping; tuning; technical analysis
Development technically too difficult	Staff training and development; prototyping; technical analysis

Risk Assessment and Risk Management Plan

1. **Analysis of Assets**

- **Risk Identification:** Inadequate analysis of assets such as content, technology infrastructure, and human resources may result in insufficient resource allocation or ineffective project planning.
- **Risk Analysis:** Likelihood: 7, Potential Impact: 8, Risk Exposure = 7 * 8 = 56
- **Risk Planning:** Conduct a comprehensive analysis of assets including content quality, technological capabilities, and team expertise. Allocate sufficient time and resources for asset analysis during the project planning phase.
- **Risk Response:** Implement a structured approach for asset analysis, including stakeholder consultations and resource assessments. Develop contingency plans to address any gaps or deficiencies identified during asset analysis.
- **Risk Monitoring:** Regularly review and update asset analysis to ensure alignment with project objectives and requirements. Monitor resource utilization and adjust plans as needed to optimize asset allocation.

2. **Estimate or Computation of Threats and Risks in E-Learning**

- **Risk Identification:** Inaccurate estimation or computation of threats and risks in e-learning may lead to inadequate risk mitigation strategies or failure to address critical vulnerabilities.
- **Risk Analysis:** Likelihood: 6, Potential Impact: 9, Risk Exposure = 6 * 9 = 54
- **Risk Planning:** Utilize expert knowledge and available data to accurately estimate threats and risks in e-learning. Implement standardized risk assessment methodologies to ensure comprehensive coverage of potential vulnerabilities.
- **Risk Response:** Develop specific risk mitigation strategies tailored to the identified threats and risks in e-learning. Establish clear protocols for responding to and managing potential security incidents or breaches.
- **Risk Monitoring:** Monitor relevant metrics and indicators to track changes in the threat landscape and assess the effectiveness of risk mitigation measures. Conduct regular risk assessments to identify emerging risks and update mitigation strategies accordingly.

3. **Fixing Priorities**

- **Risk Identification:** Failure to accurately fix priorities may result in resource allocation inefficiencies, missed deadlines, or incomplete project deliverables.
- **Risk Analysis:** Likelihood: 8, Potential Impact: 7, Risk Exposure = 8 * 7 = 56

- **Risk Planning:** Establish clear criteria for prioritizing project tasks and objectives based on their strategic importance and potential impact on project success. Involve key stakeholders in the prioritization process to ensure alignment with organizational goals.
- **Risk Response:** Develop contingency plans to address changes in priorities or shifting project requirements. Implement agile project management methodologies to adapt to evolving priorities and stakeholder needs.
- **Risk Monitoring:** Regularly review and reassess project priorities in light of changing circumstances or new information. Maintain open communication channels with stakeholders to facilitate timely adjustments to project priorities as needed.

4. **Application of Controls as well as Countermeasures**
    - **Risk Identification:** Ineffective application of controls and countermeasures may leave the project vulnerable to security breaches, data loss, or other adverse events.
    - **Risk Analysis:** Likelihood: 7, Potential Impact: 8, Risk Exposure = 7 * 8 = 56
    - **Risk Planning:** Implement a multi-layered approach to security and risk management, including technical controls, administrative policies, and user awareness training. Regularly review and update control measures to address emerging threats and vulnerabilities.
    - **Risk Response:** Develop and document comprehensive security policies and procedures to guide the implementation of controls and countermeasures. Establish incident response protocols to facilitate rapid detection, containment, and recovery from security incidents.
    - **Risk Monitoring:** Conduct regular audits and assessments of control effectiveness to identify gaps or weaknesses in the security posture. Monitor relevant security metrics and indicators to track trends and patterns indicative of potential security threats or vulnerabilities.
5. **Supervising of Risks and Judging the Effectiveness of Counteractions**
    - **Risk Identification:** Inadequate supervision of risks and failure to assess the effectiveness of counteractions may result in prolonged exposure to threats or ineffective risk mitigation efforts.
    - **Risk Analysis:** Likelihood: 6, Potential Impact: 9, Risk Exposure = 6 * 9 = 54
    - **Risk Planning:** Establish clear roles and responsibilities for risk oversight and monitoring within the project team. Implement regular risk reviews and assessments to evaluate the effectiveness of existing counteractions and identify areas for improvement.

- **Risk Response:** Develop mechanisms for capturing and reporting on risk-related data, including key risk indicators and performance metrics. Establish escalation procedures for addressing high-risk issues or incidents that require immediate attention.
- **Risk Monitoring:** Implement a robust risk monitoring and reporting framework to track changes in risk exposure over time. Conduct regular evaluations of risk management processes and practices to ensure alignment with industry best practices and regulatory requirements.

Risk Assessment and Risk Reduction Techniques

Risk	**Risk Reduction Technique**
Analysis of assets	Conduct thorough analysis of content, technology infrastructure, and human resources; allocate sufficient time and resources for asset analysis during project planning phase
Estimate or computation of threats and risks in e-learning	Utilize expert knowledge and available data to accurately estimate threats and risks; implement standardized risk assessment methodologies
Fixing priorities	Establish clear criteria for prioritizing project tasks and objectives; involve key stakeholders in the prioritization process
Application of controls as well as countermeasures	Implement a multi-layered approach to security and risk management; regularly review and update control measures
Supervising of risks and judging the effectiveness of counteractions	Establish clear roles and responsibilities for risk oversight and monitoring within the project team; implement a robust risk monitoring and reporting framework

Questions

Explanation of RMMM Plan

The RMMM plan, also known as the Risk Mitigation, Monitoring, and Management plan, is a comprehensive document that outlines strategies and procedures for identifying, assessing, mitigating, and monitoring risks throughout the lifecycle of a project. It serves as a roadmap for the project team to effectively manage risks and minimize their potential impact on project objectives. Here's an explanation of each component of the RMMM plan:

1. **Risk Identification:** This phase involves identifying potential risks that could affect the project. Risks can arise from various sources such as technical complexities, resource constraints, external dependencies, and changes in project scope. The RMMM plan outlines techniques and tools for systematically identifying risks and capturing them in a risk register.

2. **Risk Analysis:** Once risks are identified, they need to be analyzed to understand their potential impact and likelihood of occurrence. This analysis helps prioritize risks based on their severity and allows the project team to allocate resources effectively. The RMMM plan describes methodologies for assessing risks, such as qualitative and quantitative analysis, to determine their significance to the project.

3. **Risk Mitigation:** After analyzing risks, mitigation strategies are developed to reduce their likelihood or impact. These strategies may include implementing preventive measures, contingency plans, or transfer of risk to third parties. The RMMM plan details specific actions and resources required to implement mitigation strategies and assigns responsibilities to team members.

4. **Risk Monitoring:** Risk monitoring is an ongoing process throughout the project lifecycle to track the status of identified risks and assess the effectiveness of mitigation measures. The RMMM plan defines key performance indicators (KPIs) and triggers for monitoring risks and outlines procedures for regular risk reviews and updates. It also establishes communication channels for reporting and escalating risks as necessary.

5. **Contingency Planning:** In addition to mitigation strategies, the RMMM plan includes contingency plans to address risks that materialize despite mitigation efforts. Contingency plans outline predefined responses and actions to be taken in the event of a risk event, minimizing its impact on project objectives and ensuring continuity of project activities.

Outcomes:

CO2: Describe software planning and management

Conclusion:

Prepared the risk analysis document for our website Quirk IQ successfully

Grade

AA / AB / BB / BC / CC / CD / DD

Signature of faculty in-charge with date