Semester	T.E. Semester V – Computer Engineering
Subject	Software Engineering
Subject Professor In-charge	Dr. Sachin Bojewar
Assisting Teachers	Prof. Sneha Annappanavar
Laboratory	M313B

Student Name	Deep Salunkhe
Roll Number	21102A0014
TE Division	A

Title: Risk Management

Explanation:

1)What is Risk and Risk Management:

- Risk: Risk refers to the potential for loss or harm that can arise from various factors or events. It involves uncertainty and the possibility of unfavorable outcomes that can affect an individual, organization, project, or any other entity. Risks can come from a variety of sources, including financial, operational, strategic, compliance, environmental, and more.

- Risk Management: Risk management is a systematic process of identifying, assessing, prioritizing, and mitigating risks to minimize the potential negative impacts on an organization or individual. The goal of risk management is to make informed decisions that balance risk and reward, ensuring that risks are either avoided, reduced, shared, or accepted with appropriate strategies and measures in place.

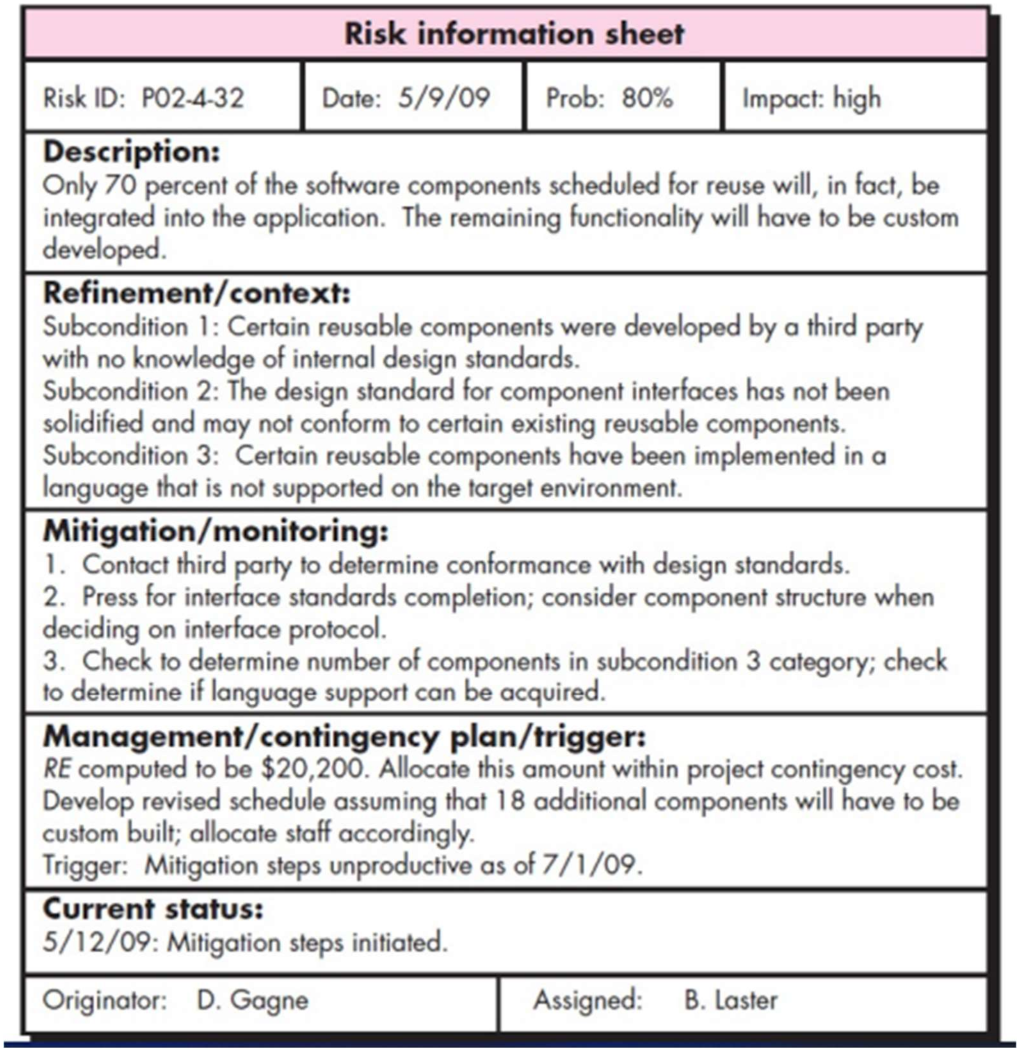
2) Types of Risk:

a) Known Risks: These are risks that are recognized and can be anticipated based on historical data or prior experience. Known risks are generally easier to assess and manage because there is existing information to work with. Examples include market fluctuations, regulatory changes, and known operational issues.

b) Unknown Risks: These are risks that are not readily identifiable or have not been encountered before. Unknown risks can be challenging to anticipate and plan for because they lack historical data or a clear understanding. They often emerge unexpectedly and can have a significant impact. Examples include natural disasters, emerging technologies, and unforeseen market disruptions.

c) Predicted Risks: Predicted risks fall between known and unknown risks. These are risks that may not have been encountered directly, but there is enough information and analysis available to predict their likelihood and potential impact. Predicted risks are managed by developing strategies and contingency plans based on informed predictions. Examples include potential economic recessions, political events, and cybersecurity threats based on trends and analysis.

3)Formate and Discription:



Risk information sheet

Risk ID: P02-4-32	Date: 5/9/09	Prob: 80%	Impact: high

Description:
Only 70 percent of the software components scheduled for reuse will, in fact, be integrated into the application. The remaining functionality will have to be custom developed.

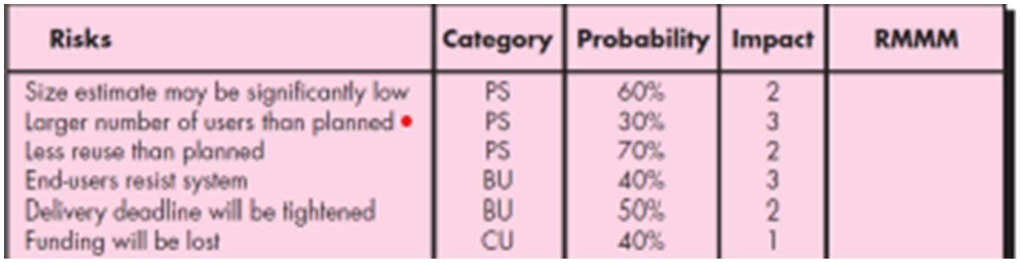
Refinement/context:
Subcondition 1: Certain reusable components were developed by a third party with no knowledge of internal design standards.
Subcondition 2: The design standard for component interfaces has not been solidified and may not conform to certain existing reusable components.
Subcondition 3: Certain reusable components have been implemented in a language that is not supported on the target environment.

Mitigation/monitoring:
1. Contact third party to determine conformance with design standards.
2. Press for interface standards completion; consider component structure when deciding on interface protocol.
3. Check to determine number of components in subcondition 3 category; check to determine if language support can be acquired.

Management/contingency plan/trigger:
RE computed to be $20,200. Allocate this amount within project contingency cost. Develop revised schedule assuming that 18 additional components will have to be custom built; allocate staff accordingly.
Trigger: Mitigation steps unproductive as of 7/1/09.

Current status:
5/12/09: Mitigation steps initiated.

Originator: D. Gagne	Assigned: B. Laster



Risks	Category	Probability	Impact	RMMM
Size estimate may be significantly low	PS	60%	2	
Larger number of users than planned •	PS	30%	3	
Less reuse than planned	PS	70%	2	
End-users resist system	BU	40%	3	
Delivery deadline will be tightened	BU	50%	2	
Funding will be lost	CU	40%	1	

Implementation:

1. **Known Risks:**

   - **System Downtime:** This is a well-known risk in software engineering. Known risks could include server outages, software bugs, or infrastructure failures that may lead to system downtime, causing delays in order processing.

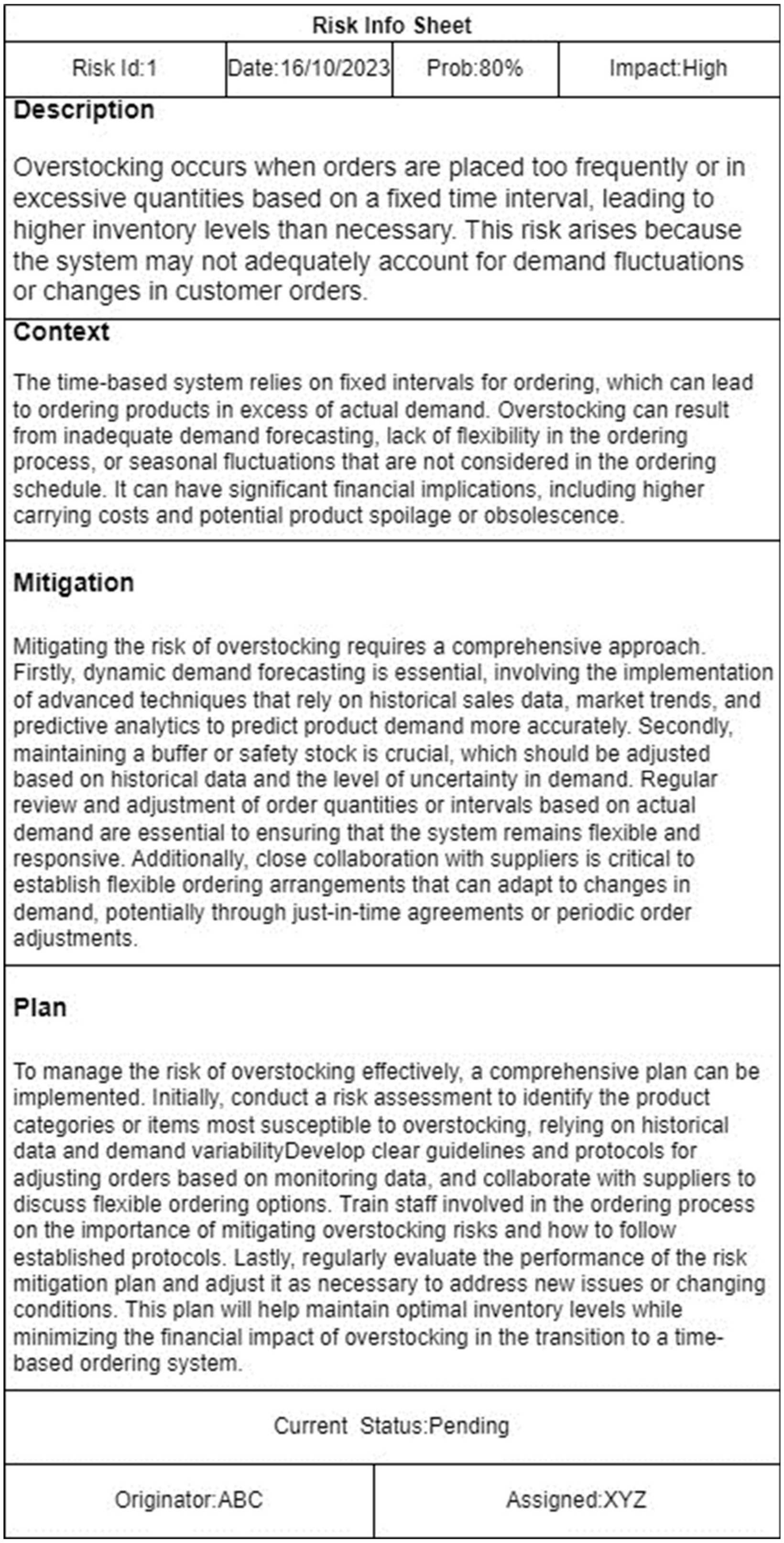
- **Supplier Delays:** Known risks can involve delays from suppliers or vendors who may not meet their promised delivery schedules, affecting the order system's reliability.
- **Inventory Management:** Issues like overstock or inventory shortages are known risks. Software should be able to manage and notify users about these inventory issues.

2. **Unknown Risks:**

    - **Emerging Technology Disruption:** New technologies or disruptive innovations in the industry, such as blockchain for supply chain management, could pose unforeseen challenges that the software engineering team may not be prepared for.
    - **Regulatory Changes:** Changes in international trade regulations or taxation laws affecting cross-border shipments might be unknown risks that can impact the order system.
    - **Market Shifts:** Unexpected changes in consumer preferences, like a sudden surge in demand for eco-friendly products, may introduce unknown risks to the system.

3. **Predicted Risks:**

    - **Cybersecurity Threats:** Predicted risks could include an expected increase in cybersecurity threats such as DDoS attacks or data breaches targeting the order processing system. Software engineers can proactively enhance security measures.
    - **Shipping Cost Fluctuations:** Anticipated fluctuations in shipping costs, perhaps due to fuel price changes or geopolitical events, can be predicted risks that impact the software's cost estimation and optimization algorithms.
    - **Supply Chain Disruptions:** Predicted risks might include labor strikes, natural disasters, or geopolitical instability affecting the supply chain. Software engineers can prepare for these by building in contingencies.



Risk Info Sheet

Risk Id:1	Date:16/10/2023	Prob:80%	Impact:High

Description

Overstocking occurs when orders are placed too frequently or in excessive quantities based on a fixed time interval, leading to higher inventory levels than necessary. This risk arises because the system may not adequately account for demand fluctuations or changes in customer orders.

Context

The time-based system relies on fixed intervals for ordering, which can lead to ordering products in excess of actual demand. Overstocking can result from inadequate demand forecasting, lack of flexibility in the ordering process, or seasonal fluctuations that are not considered in the ordering schedule. It can have significant financial implications, including higher carrying costs and potential product spoilage or obsolescence.

Mitigation

Mitigating the risk of overstocking requires a comprehensive approach. Firstly, dynamic demand forecasting is essential, involving the implementation of advanced techniques that rely on historical sales data, market trends, and predictive analytics to predict product demand more accurately. Secondly, maintaining a buffer or safety stock is crucial, which should be adjusted based on historical data and the level of uncertainty in demand. Regular review and adjustment of order quantities or intervals based on actual demand are essential to ensuring that the system remains flexible and responsive. Additionally, close collaboration with suppliers is critical to establish flexible ordering arrangements that can adapt to changes in demand, potentially through just-in-time agreements or periodic order adjustments.

Plan

To manage the risk of overstocking effectively, a comprehensive plan can be implemented. Initially, conduct a risk assessment to identify the product categories or items most susceptible to overstocking, relying on historical data and demand variabilityDevelop clear guidelines and protocols for adjusting orders based on monitoring data, and collaborate with suppliers to discuss flexible ordering options. Train staff involved in the ordering process on the importance of mitigating overstocking risks and how to follow established protocols. Lastly, regularly evaluate the performance of the risk mitigation plan and adjust it as necessary to address new issues or changing conditions. This plan will help maintain optimal inventory levels while minimizing the financial impact of overstocking in the transition to a time-based ordering system.

Current Status:Pending

Originator:ABC	Assigned:XYZ

.

Conclusion:

In conclusion, risk management and analysis in software engineering are integral processes that play a crucial role in the successful development and deployment of software systems. By identifying, assessing, and mitigating potential risks, software teams can proactively address issues before they become critical, ultimately leading to more efficient and reliable software projects. These practices help in delivering high-quality software that meets user requirements, stays within budget, and adheres to timelines. Furthermore, as the software development landscape evolves with emerging technologies and changing user needs, the importance of robust risk management and analysis continues to grow, ensuring adaptability and resilience in the face of uncertainty. It is imperative for software engineering teams to embrace and prioritize these practices, as they ultimately contribute to the overall success and competitiveness of software projects.