Assignment-1

Topic: Risk Management Framework
Course: SE 612

Submitted By:
Mehedi Hasan Sun (BSSE 1025)
Abdullah-Al-Jahid (BSSE 1030)

Submitted To:
Dr. Mohammed Shafiul Alam Khan
Associate Professor, IIT
University of Dhaka

Date: 6 January, 2021

Risk Management Framework: InDez

To apply RMF, we have chosen our SPL-2 project which is 'InDez'. The 5 stages of RMF based on 'InDez' are given below.

1. Understanding The Business Context

InDez is an android mobile application that focuses on helping people to decorate rooms using augmented reality. One general purpose is that anyone can use this application to see how his/her rooms will look like after decoration. This is an augmented reality-based android application that will be used for interior designing and decorating. Our application will provide users the option to drag and drop augmented furniture in their room which they are able to see using their phone's camera. Then users can select the color and texture of furniture and wall, change room lighting.

Goals:

1. On-Time Delivery: InDez must be up and running before the final project presentation
2. Accuracy: All data related to furniture and specially the size and the position of a furniture must be 100% accurate
3. Scalability: Though InDez has a small number of users now, it should be scalable for a huge number of users.
4. Functioning: InDez should be able to run smoothly without any system failure.
5. AR-Experience: Allowing people around the globe to experience 3D virtual models of their furniture.

Priorities:

1. Accuracy is the main concern of our application. The more accuracy we can gain, the more successful will be our project.

2. Identifying The Business & Technical Risks

Table 1: InDez's Prioritized Business Goals

Rank	Business Goal	Description
H	On-Time Delivery	Due to covid-19 situation, the project deadline has not been fixed yet, but to be on the safe side, InDez should be completed developing by April, 2021
H	Accuracy	Since having misinformation can have major consequences, all the data must be absolutely accurate.
M	Scalability	As the number of users may increase in future, InDez should be robust.
H	Functioning	InDez should be able to run smoothly without any system failure.
H	AR-Experience	Allowing people around the globe to experience 3D virtual models of their furniture.

Table 2: InDez's Business Risks

Business Risk	**Description**
Requirements have not been fulfilled before deadline	There are some mandatory requirements for InDez that need to be fulfilled like save, versioning, light etc. Launching the product without checking them can seriously have negative impacts
Fails to perform actions accurately.	The failure of the system to perform critical operational functions will Negative consequences. This type of risks threatens the utility of the system, thus reducing people's will to the usage of the app
Unable to handle bulk data	As we will store users information along with workspaces and object lists, our application has to handle a huge amount of data.
System failure	Successfully performed security attacks can have a major negative impact on the system.Processing multiple objects concurrently can lead to system crash. If not anything, having major security flaws within the system will discourage the people from using it.
Poor user experience	Unable to place virtual objects in real world locations. This can create negative impacts on users' minds.

Table 3: InDez's Business Risk Indicators and likelihood of Occurrence

Business Risk	**Business Risk Indicators**	**Likelihood of Occurrence**
Requirements have not been fulfilled before deadline	• Number of unfinished requirements • Effort required to fix critical and important errors • Non-robust implementation of the requirements	H
Fails to perform actions accurately.	• Number of incorrect critical operations performed • Efforts required to fix the errors that cause the failures • Number of users lost • Number of wrong placement of objects. • Number of unstable objects • Number of failure while loading saved workspace	M
Unable to handle bulk data	• Non-robust response of the requests • Number of missed requests	L
System failure	• Number of security vulnerabilities identified • Effort required to secure the vulnerabilities • Number of users lost	L
Poor user experience	• Number of wrong placement of objects. • Number of unstable objects • Number of failure while loading saved workspace	M

Table 4: InDez's Technical Risks

ID	Technical Risk
TR1	Unable to access QA tools for unit testing
TR2	QA tests do not fully evaluate requirements.
TR3	Testing does not cover fault tolerance. System failures are likely
TR4	System is susceptible to denial-of-service attacks.
TR5	Processing multiple objects concurrently can lead to system crash
TR6	System does not require good passwords. Attackers can get in more easily and cause unpredictable behavior.
TR7	Inefficient detection of surface
TR8	Unable to place virtual objects in real time world location
TR9	System may not work properly under heavy traffic

Table 5: IIT360's Categorized Technical Risks and Likelihood of Occurrence

ID	Technical Risk	Technical Risk Indicators	Likelihood
TR1	Unable to access QA tools for unit testing	Number of development phase bugs reported	H
TR2	QA tests do not fully evaluate requirements.	Number of requirements-phase bugs reported post-implementation	H
TR3	Testing does not cover fault tolerance. System failures are likely	Number of faults reported	H

TR4	System is susceptible to denial-of-service attacks.	Number of suspicious amount of traffic generated by a single IP	L
TR5	Processing multiple objects concurrently can lead to system crash	Number of object placement in a single workspace	L
TR6	System does not require good passwords. Attackers can get in more easily and cause unpredictable behavior.	Number of unauthorized logins and accesses Number of IDS anomalies	M
TR7	Inefficient detection of surface	Insufficient amount of light. Minimal amount texture difference.	M
TR8	Unable to place virtual objects in real time world location	Number of shaky objects	L
TR9	System may not work properly under heavy traffic	Mean availability of bulk data	L

3.Synthesizing and Ranking the Risks

To better understand and manage risks, we will establish a relationship between business goals, business risks, technical risks and subsequently prioritize them.

Table 6: Indez's Goal-to-Risk Relationship table

Business Goal	**Business Risk**	**ID**	**Technical Risk**
On-Time Delivery	Requirements have not been fulfilled before deadline	**TR1**	Unable to access QA tools for unit testing
		TR2	QA tests do not fully evaluate requirements.
		TR3	Testing does not cover fault tolerance. System failures are likely
Accuracy	Fails to perform actions accurately.	**TR7**	Inefficient detection of surface
		TR8	Unable to place virtual objects in real time world location
		TR5	Processing multiple objects concurrently can lead to system crash
Scalability	Unable to handle bulk data	**TR9**	System may not work properly under heavy traffic
Functioning	System failure	**TR4**	System is susceptible to denial-of-service attacks.
		TR5	Processing multiple objects concurrently can lead to system crash
		TR6	

			System does not require good passwords. Attackers can get in more easily and cause unpredictable behavior.
AR-Experience	Poor user experience	**TR7** **TR8**	Inefficient detection of surface Unable to place virtual objects in real time world location

Now we can chalk out the technical risk severity by business goals.

Table 7: InDez's Technical Risk Severity by Business Goals

ID	**Technical Risk**	**Business Risk**				
		On-Time Delivery	**Accuracy**	**Scalability**	**Functioning**	**AR-Experience**
TR1	Unable to access QA tools for unit testing	H	N/A	N/A	N/A	N/A
TR2	QA tests do not fully evaluate requirements.	H	N/A	N/A	N/A	N/A
TR3	Testing does not cover fault tolerance. System failures are likely	H	N/A	N/A	N/A	N/A

TR4	System is susceptible to denial-of-service attacks.	N/A	N/A	N/A	L	N/A
TR5	Processing multiple objects concurrently can lead to system crash	N/A	L	N/A	L	N/A
TR6	System does not require good passwords. Attackers can get in more easily and cause unpredictable behavior.	N/A	N/A	N/A	L	N/A
TR7	Inefficient detection of surface	N/A	M	N/A	N/A	M
TR8	Unable to place virtual objects in real time world location	N/A	L	N/A	N/A	L
TR9	System may not work properly under heavy traffic	N/A	L	N/A	N/A	N/A

4.Defining the Risk Mitigation Strategy

Now that we have identified all potential risks from both business and technical perspectives, we can now move ahead to plan how to mitigate these risks. Below are the methods that we will use for this job.

Business Risk	**Supporting Technical Risk**	**Risk Mitigation Method**		
		Improve QA in early SDLC phases	**Add testing Methods to QA**	**Add security measurements and testing to SDLC**
Requirements have not been fulfilled before deadline	**TR1**	**H**	**M**	
	TR2	**H**		**M**
	TR3	**M**	**H**	
Fails to perform actions accurately.	**TR5**	**H**	**M**	
	TR7	**M**	**H**	
	TR8	**M**	**H**	
Unable to handle bulk data	**TR9**	**H**	**H**	**M**
System failure	**TR4**		**M**	**H**
	TR5	**H**	**M**	
	TR6			**H**
Poor user experience	**TR7**	**M**	**H**	
	TR8	**M**	**H**	

5. Carrying Out Fixes and Validating

This stage involves execution of the risk mitigation strategy. Each strategic approach to risk mitigation will differ according to what sorts of risks were identified, what the business context is, and what methods were chosen to manage risk. Progress at this stage should be measured against the risk mitigation strategy. Good metrics include but are not limited to progress against risks, open risks remaining, and any artifact quality metrics previously identified. This stage involves application of those validation techniques identified earlier in order to give some confidence that risks have been properly mitigated through artifact improvement. In many respects, the validation plan is a test plan for risk mitigation assurance. Our project will have a unique validation plan that directly depends on the risks identified and the methods chosen to address them. Testing can be used to demonstrate and measure the effectiveness of various software assurance activities. The central concern at this stage is to validate that the artifacts and processes no longer carry unacceptable risks. This stage should define and leave in place a repeatable, measurable, verifiable validation process that the project can run from time to time to continually verify artifact quality