Risk Management Report

Commerce Bank Web Application

March 14th, 2021

Team Members

Zach Gharst

William Keke

Benaiah Kilen

Atticus Parris

Andrew Poitras

Document Control

Change History

Revision	Change Date	Description of changes
V1.0	3/14/2021	Initial release

Document Storage

This document is stored in the project’s Git repository at: https://github.com/UMKC-CS451R-Spring-2021/semester-project-group-3-commerce.

Document Owner

William Keke is responsible for developing and maintaining this document.

Identified Risks

Rank	Risk	Probability of Loss	Size of Loss	Risk Exposure
1	WebApp does not consistently connect to the database.	Moderate	Catastrophic	Extreme Risk
2	Password fails to encrypt before entering the database.	Unlikely	Major	High Risk
3	Developers need to practice more with ASP.NET than initially expected.	Almost Certain	Minor	High Risk
4	Documented hours of effort expected for tasks are inaccurate.	Likely	Minor	High Risk
5	Forget to encrypt/hide connection string.	Unlikely	Major	High Risk
6	Accidentally pushing an unfinished/fundamentally flawed build to master.	Rare	Major	High Risk
7	Not enough budget or time to deliver a finished product.	Rare	Major	High Risk
8	Product fails to meet the expectations of the customer.	Rare	Catastrophic	High Risk
9	Requirements change too often and delay development.	Unlikely	Moderate	Moderate Risk
10	More web-pages are needed than initially expected.	Unlikely	Moderate	Moderate Risk
11	Differing naming, styling, or scripting conventions among web-pages.	Almost Certain	Negligible	Moderate Risk
12	Application front-end isn’t properly tested on all device viewports resulting in unwanted visual artifacts.	Moderate	Negligible	Low Risk
13	Project team approaches problems with an anti-pattern response.	Unlikely	Negligible	Low Risk

Risk Response Plan

Risk ID: 1	**Title:** *Improper database connection*	**Origination Date:** *3/13/2021*
Status: *Contingent*		**Originator:** *Benaiah Kilen*
Description: *This risk refers to the probability that the web application will improperly connect to the database. The consequences of this risk include: failure to connect to the database and its contents, an inability to carry out tasks within the application (logging in, notifying users, etc.), and failure to deliver a functioning product.*		**Assessment:** *Qualitative*
		Probability: *Moderate*
		Consequences: *Catastrophic*
		Risk Exposure: *Extreme Risk*
Owner: *Zach Gharst, Benaiah Kilen*		
Risk Response Alternatives: *Extensive testing to ensure the connection string is properly defined and the database's server is open to connect to. Would require us to re-analyze how we connect to the database, and at worst would require us to re-analyze most of our code.* *Integrating the required tables in a different way than we had used initially. Requires effort to research and implement a new method, and we are at risk of the new method not working/being compatible.*		
Risk Response Plan (Activities & Milestones)		
Date	**Actions**	**Responsibilities**
3/13/2021	*Run tests on project to ensure that database is connected. Make adjustments if not.*	*Tester - Runs tests to check if database is connected.* *Project Manager - calls emergency meeting if needed* *Database Administrator & Developers - Make any needed adjustments to fix issues*
End of each iteration	*Recheck that database still connects to frontend of application. Immediately address if not.*	*Tester - Runs tests to check if database is connected.* *Project Manager - calls emergency meeting if needed* *Database Administrator & Developers - Make any needed adjustments to fix issues*
Plan Status		
Date	**Status**	
3/13/2021	*Currently no issues with database connectio*n	
Resources: *Project team*		

Risk ID: 2	**Title:** *Password fails to encrypt before entering the database.*	**Origination Date:** *03/13/2021*
Status: *Identified*		**Originator:** *Atticus Parris*
Description: *User's password fails to encrypt before entering database. Causes user privacy to become vulnerable. Puts user at risk of having personal information stolen.*		**Assessment:** *Qualitative*
		Probability: *Unlikely*
		Consequences: *Major*
		Risk Exposure: *High Risk*
Owner: *Zach Gharst, Benaiah Kilen*		
Risk Response Alternatives: *Monitor database contents. Create tests to ensure password encryption.*		
Risk Response Plan (Activities & Milestones)		
Date	**Actions**	**Responsibilities**
03/13/2021	*On implementation of passwords being hashed into the database, tests are performed to ensure that the process works as intended.*	*Database Administrator - properly implement password hashing* *Tester - run tests to ensure password hashing works properly*
Plan Status:		
Date	**Status**	
3/13/2021	*Password hashing has not been implemented yet*	
Resources: *Database Administrator, Tester*		