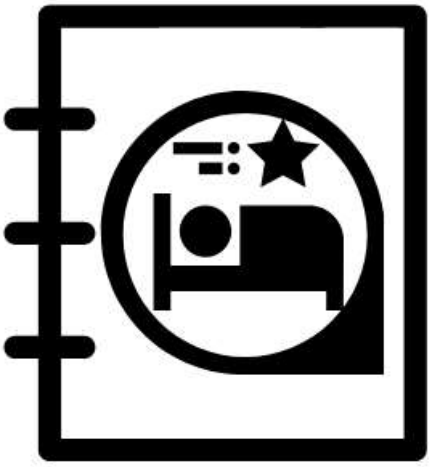
California State University Fullerton

CPSC 462

Object Oriented Software Design

Risk List & Risk Management Plan

for the



Hotel Reservation System

Josh Ibad
Chief Software Architecture
joshcibad@csu.fullerton.edu

Revision History:

Version	Date	Summary of Changes	Author
1.0	2021-10-18	• Initial Release	Josh Ibad
2.0	2021-11-15	• Changed role to Chief Software Architect • In description, bolded and separated If, then, result clauses into separate lines for ease of use and readability. • In risk mitigation approach, all mitigation approaches changed from suggestions and possibilities to definitive statement of mitigations that **will** be performed. • In risk mitigation approach for item 4 - Erroneous input, mitigation approach changed from UI design which is not a mitigation approach, into actions of administrator management and user training • In metrics, a specific measure has been identified along with a specific threshold. No new risks have been found in the current iteration. Risks will be further analyzed, reviewed, and refined in subsequent iterations.	Josh Ibad

Table of Contents

1 Risk Identification and Mitigation Plan

No.	Title	Description	Weight	Category	Mitigation Approach	Metrics
1.	System Crash	**If** the hotel reservation system crashes **then** the hotel will be unable to continue business **resulting** in losses in revenue surmounting to well above $1000 per day, depending on RevPAR and number of rooms still available.	1	Business	System backups will be performed which will cost around $3 per GB of data stored, and spinning up a cloud server to run the service will cost around $2+ per node per day.	System uptime in minutes. System should never be down for more than 5 minutes.
2	Security breach	**If** malicious actors find and exploit vulnerabilities in the public-facing interfaces of the system **then** they can hack the system- **resulting** in interruption of business operations. This can be tantamount to a crash, with losses surmounting well above $800 per day, depending on RevPAR and number of rooms still available.	2	Technical	Regular security assessments will be performed. A pentest will cost around $4k-$10k for systems of small scale.	Time taken for pentesters to find vulnerabilities, in days. System should be resistant to professional black-box penetration for a day at minimum.

No.	Title	Description	Weight	Category	Mitigation Approach	Metrics
3.	Slowdown under user load	**If** the hotel reservation system encounters large user load **then** the system can slow down- **resulting** in poor customer experience and thus losses in revenue. Can cost around $100 a day if high, and a steady decrease in customers if left unmanaged.	2	Resource	High spec servers will be used and load balancing will be utilized. This will cost well above $1k-$3k per month for each upgraded server.	Delays in units of milliseconds. System should not have delays over 5000 ms.
4.	Erroneous input	**If** the hotel manager inputs wrong information **then** users when they dont get what was expected **resulting** in losses in revenue. Lost business can cost $50 a day if not severe.	5	Business	System administrators and employees will respond to erroneous inputs and fix them manually. Training will be provided to employees and managers to minimize this risk.	How often erroneous input occurs, in count of errors per month. Successful erroneous inputs should occurs at most one per month.