

## Risk Assessment and Management Plan (RMP)

The purpose of this risk management plan is to identify, assess, and prioritize potential risks associated by developing a new condo management software system (CondoCare) that could impact the project, and to develop strategies for managing and mitigating those risks in order to ensure the safety and of the tenants, employees, and other stakeholders. This plan will provide a framework for proactively identifying and responding to risks, promoting effective decision-making, and minimizing negative impacts on the system's operations, reputation, and financial sustainability of CondoCare.

### **The benefits of risk assessment and management.**

Project success is significantly increased by the benefits of risk assessment and management plan because they mitigate risks and significantly improve the project's chances of success. Legal and compliance assurance is especially important when developing software systems, such as condo management systems, since it ensures that relevant laws and regulations are met, reducing legal risks. The plan reduces uncertainties by identifying potential risks early. By reducing uncertainties, the project can be planned and executed more accurately. Time and cost efficiency proactive risk management can save you significant amounts of money and time by reducing or preventing issues that may cause the project to stall.

Impact	Low	Medium	High
Probability			
Low	[1]Dependence on external system,,	Financial Risk,  Inaccurate estimation of costs  Lack of experience of project manager	Hardware suppliers, Technology, Lack of insurance or warranty
Medium	Poor Code Quality	Scope Creeping	System failure due to hardware malfunction/soft ware bugs.
High	Scheduled maintenance windows impacting usability.	Compromising Design	Recruiting the right Engineering and product management team

Figure [#]: Risk management chart

Risk ID	Risk Type and Description	Risk Score	Resolved in Sprint	Strategy and Effectiveness
	•	•		•
R1	<b>Technical:</b>  Our dependence on external systems gives us less control over the performance/uptime. (Service providers/database management)	Low	1	• Accept Existing services have a great track record.
R-6	<b>Upload and Sharing (US003)</b>  Risk of data breaches and unauthorized access when uploading and sharing files, especially sensitive or confidential information.	High	2	Avoid  Implement secure file transfer protocols, Enforce access controls and permissions, Educate users on secure sharing practices, Effectiveness: High with consistent implementation and user compliance.
R-7	<b>User Registration (US001)</b> Risk of unauthorized access, data breaches, and fraudulent registrations.	M	2	Accept Verify user identities, we need to use strong password policies and also implement CAPTCHA to prevent bots. Effectiveness: High with diligent implementation and regular updates.
R-8	<b>Reservation System (US006)</b>	M	2	Accept

	Risks involve unauthorized access to customer data, data corruption, system downtime, breaches of data laws, vulnerability to cyber-attacks, and data theft. System errors can cause overbooking and customer dissatisfaction			Enforce strict access controls. Conduct regular security audits. High when strategies are fully implemented, regularly updated, and maintained, with ongoing employee training and awareness
R-9	<b>Roles Management</b> (US008)  set up different roles (e.g., managers, finance personnel) for employees responsible for the same property.	M	2	Accept  Regular updates to access policies, continuous monitoring, and adapting to organizational changes are crucial for effectiveness. Integrating with broader security measures like multi-factor authentication, encryption, and incident response enhances overall security.
R-10	<b>Financial System</b> (US005) Vulnerability to cyber attacks (e.g., hacking, phishing), internal fraud, unauthorized transactions, data breaches, and compliance violations	H	2	Avoid  Implement robust cybersecurity measures, fraud detection systems, regular audits, employee training, and adhere to financial regulations  High, when consistently applied and updated to address evolving threats and regulatory changes.

Table [#]: List of identified risks