Risk Assessment and Management Plan (RMP)

A risk is an event or condition that, if it occurs, could have a positive or negative effect on a project's objectives. Risk Management is the process of identifying, assessing, responding to, monitoring, and reporting risks. This Risk Management Plan defines how risks associated with the Condo Management System project will be identified, analyzed, and managed. It outlines how risk management activities will be performed, recorded, and monitored throughout the lifecycle of the project and provides templates and practices for recording and prioritizing risks.

The Risk Management Plan is created by the project manager in the Planning Phase of the CDC Unified Process and is monitored and updated throughout the project. The intended audience of this document is the project team, project sponsor and management.

Risk identification will involve the project team, appropriate stakeholders, and will include an evaluation of environmental factors, organizational culture and the project management plan including the project scope. Careful attention will be given to the project deliverables, assumptions, constraints, WBS, cost/effort estimates, resource plan, and other key project documents.

A Risk Management Log will be generated and updated as needed and will be stored electronically in the project library located at https://drive.google.com/drive/u/0/folders/1Yaso52WHZf5TxmD2KLVr0bEh4Nu_fUrg

List of risks across user stories:

Sprint - 1

US-1: Public User Sign-Up

Data security: Storing user details in MongoDB poses a risk of data breaches if proper security measures are not implemented, in which case sensitive user information could be compromised.

API vulnerability: Developing a sign-up API opens up the system to potential security vulnerabilities such as injection attacks, parameter tampering, or unauthorized access. Without proper input validation and testing, attackers could exploit weaknesses in the API to gain unauthorized access to user accounts or inject malicious code.

Front-end vulnerability: Implementing the front-end React component for the sign-up form introduces the risk of malicious scripts injected through the form that could be executed within users' browsers.

Validation failure: Client-side validation for the sign-up form inputs may not be sufficient to prevent all types of incomplete or improper data submission, which can result in malformed data being sent to the server, leading to errors or inconsistencies in the user database.

US-2: Public User Login

Authentication vulnerabilities: Risk of brute force attacks, session fixation, or token hijacking which can potentially grant unauthorized access to user accounts.

Front-end vulnerability: Implementing the front-end React component for the sign-up form introduces the risk of malicious scripts injected through the form that could be executed within users' browsers.

JWT security: Issues such as insecure token storage, insufficient token expiration policies, or improper validation of tokens could lead to security breaches, including unauthorized access or session hijacking.

Password Security: If passwords are not properly encrypted using a strong cryptographic algorithm, they could be vulnerable to password cracking techniques, exposing sensitive user information.

US-3: Signed in Public User Create Profile

Data security: Expanding the user schema in MongoDB to include profile details increases the amount of personal information stored in the system. If proper security measures are not implemented, sensitive user information could be compromised.

API vulnerability: Adding API endpoints for retrieving and updating user profiles exposes the system to security risks such as injection attacks, unauthorized access, or data manipulation. Attackers could exploit weaknesses in the API to gain unauthorized access to user accounts or inject malicious code.

Front-end vulnerability: Implementing a front-end React component for designing the profile management page introduces the risk of malicious scripts injected through the form to be executed within users' browsers or Cross-Site Request Forgery (CSRF)
Insecure file upload: Without proper validation and sanitization of uploaded files, attackers could upload malicious files to the server, leading to security breaches and compromising the system

Validation failure: Client-side validation for the required profile details may not be sufficient to prevent all types of incomplete or improper data submission, which can result in malformed data being sent to the server, leading to errors or inconsistencies in the user database or injection attacks.

US-4: Enter Registration Key to Assign User Roles

Registration key security: Keys may not be securely generated, transmitted, and validated. Weaknesses in key generation algorithms or improper handling of keys during transmission could lead to guessing attacks or unauthorized access to restricted data.

Role assignment vulnerabilities: If role assignment logic is not implemented securely, attackers could manipulate the registration key or exploit vulnerabilities in the role assignment process to gain elevated privileges or access unintended features or data.

Data security: Risks of updating the database schema include unauthorized modification or access to user roles if proper access controls and encryption mechanisms are not implemented. Insecure database configurations or vulnerabilities in the schema update process could lead to data breaches or integrity issues.

UX impact: Risks include user frustration or abandonment if the registration key input process is confusing or cumbersome. Poorly designed registration key interfaces or inadequate user guidance could lead to usability issues and dissatisfaction among users.

Impact Probability	Low	Medium	High
Low	Validation failure Insecure file upload Role assignment vulnerability	API vulnerability Front-end vulnerability Validation failure Registration key security	Data security
Medium	JWT security	UX impact	Password security
High	Insufficient testing		Authentication vulnerabilities

Table [1]: Risk management chart (Sprint - 1)

Risk ID	Risk Type and Description	Risk Score	Resolved in Sprint	Strategy and Effectiveness
US-1.0	Technical Management External Budget Schedule Etc.	Low Medium High	Sprint 1	Mitigate Accept Avoid Transfer
US-1.1	Technical risk Data security	Medium	Sprint 1	Mitigate
US-1.2	External risk API Vulnerability	Low	Sprint 1	Mitigate
US-1.3	External risk Front-end vulnerability	Low	Sprint 1	Avoid
US-1.4	Technical risk Validation failure	Low	Sprint 1	Mitigate
US-1.5	Technical risk Insufficient testing	Medium	Sprint 1	Mitigate
US-2.1	External risk Authentication vulnerability	High	Sprint 1	Mitigate
US-2.2	External risk Front-end vulnerability	Low	Sprint 1	Avoid
US-2.3	External risk JWT security	Low	Sprint 1	Mitigate
US-2.4	Technical risk Password security	High	Sprint 1	Mitigate
US-2.5	Technical risk	Medium	Sprint 1	Mitigate

	Insufficient testing			
US-3.1	Technical risk Data security	Medium	Sprint 1	Mitigate
US-3.2	External risk API Vulnerability	Low	Sprint 1	Mitigate
US-3.3	External risk Front-end vulnerability	Low	Sprint 1	Avoid
US-3.4	Technical risk Insecure file upload	Low	Sprint 1	Mitigate
US-3.5	Technical risk Validation failure	Low	Sprint 1	Mitigate
US-4.1	Technical risk Registration key security	Low	Sprint 1	Mitigate
US-4.2	Technical risk Role assignment vulnerability	Low	Sprint 1	Mitigate
US-4.3	External risk Data security	Medium	Sprint 1	Mitigate
US-4.4	Technical risk Insufficient testing	Medium	Sprint 1	Mitigate
US-4.5	External risk UX-Impact	Medium	Sprint 1	Mitigate

Table [2]: List of identified risks (Sprint - 1)

Sprint - 2

US-5: Create Owner’s Property Dashboard

Data privacy: Displaying property details on the dashboard may pose risks to data privacy if sensitive information such as property addresses, ownership status, or financial data is exposed to unauthorized users.

Authentication vulnerabilities: Risks of unauthorized access or data manipulation exist if authentication mechanisms for accessing the dashboard are not implemented securely. Weaknesses in authentication processes could lead to unauthorized users gaining access to sensitive property information.

Front-end vulnerability: Implementing the front-end React components for the dashboard introduces the risk of code injection or Cross-Site Scripting (XSS) attacks if proper input validation and sanitization measures are not implemented. Attackers could exploit vulnerabilities in the front-end code to execute malicious scripts within users' browsers.

Data integrity: Risks include data inconsistencies or inaccuracies on the dashboard if data validation and verification processes are not robust. Inaccurate property details or outdated information could impact the decision-making process for property owners and users accessing the dashboard.

Insufficient testing: Risks include incomplete coverage of test scenarios, which may result in undiscovered bugs or vulnerabilities in the frontend and backend components. Failure to adequately test the components could lead to errors, inconsistencies, or unexpected behavior in the application, impacting user experience and system reliability

US-6: Create Property Profile by Condo Company Manager

Data security: Risks arise from storing property profile details in the system, including sensitive information such as property addresses, unit numbers, and owner contact details. Without proper security measures, such as encryption and access controls, there's a risk of unauthorized access or data breaches.

Authorization vulnerabilities: Risks of unauthorized access to property profile creation functionalities if access control mechanisms are not implemented effectively. Weaknesses in authorization logic could allow unauthorized users to create or modify property profiles, leading to data manipulation or integrity issues.

Front-end vulnerability: Implementing the front-end React components for property profile creation introduces the risk of code injection or Cross-Site Scripting (XSS) attacks if proper input validation and sanitization measures are not implemented. Attackers could exploit vulnerabilities in the front-end code to execute malicious scripts within users' browsers.

Data validation failure: Risks of data inconsistency or inaccuracy in property profiles if validation processes for input data are not robust. Incomplete or improper data submission could lead to errors or inconsistencies in property details, impacting the reliability of the information stored in the system.

Insufficient testing: Risks include incomplete coverage of test scenarios, which may result in undiscovered bugs or vulnerabilities in the frontend and backend components. Failure to adequately test the components could lead to errors, inconsistencies, or unexpected behavior in the application, impacting user experience and system reliability

US-8: Condo Manager Enter Details For Every Component in the Property

Data integrity: Risks arise from entering and managing details for every component in the property, including fixtures, utilities, and amenities. Without robust data validation and verification processes, there's a risk of data inconsistencies or inaccuracies, impacting the reliability of property information stored in the system.

Authorization vulnerabilities: Risks of unauthorized access to component details entry functionalities if access control mechanisms are not implemented effectively. Weaknesses in authorization logic could allow unauthorized users to view or modify component details, leading to data manipulation or integrity issues.

Front-end vulnerability: Implementing the front-end React components for entering component details introduces the risk of code injection or Cross-Site Scripting (XSS) attacks if proper input validation and sanitization measures are not implemented. Attackers could exploit vulnerabilities in the front-end code to execute malicious scripts within users' browsers.

Data security: Risks of unauthorized access or data breaches if sensitive component details, such as maintenance schedules, inspection records, or warranty information, are not adequately protected. Proper security measures, such as encryption and access controls, are essential to prevent unauthorized access to sensitive property information.

Insufficient testing: Risks include incomplete coverage of test scenarios, which may result in undiscovered bugs or vulnerabilities in the frontend and backend components. Failure to adequately test the components could lead to errors, inconsistencies, or unexpected behavior in the application, impacting user experience and system reliability

US-9: Implement Registration Key Distribution From Condo Managers to Public Users

Security of registration keys: Risks arise from the generation, distribution, and validation of registration keys, including risks of key guessing attacks, unauthorized access, or data breaches if keys are not securely generated, transmitted, and validated. Weaknesses in key generation algorithms or improper handling of keys during distribution could lead to unauthorized access to the system or guessing attacks.

Role assignment vulnerabilities: Risks of unauthorized access or privilege escalation if role assignment logic for registration keys is not implemented securely. Attackers could manipulate registration keys or exploit vulnerabilities in the role assignment process to gain elevated privileges or access unintended features or data.

Data security: Risks associated with updating the database schema to include registration key details, including risks of unauthorized modification or access to key data. Insecure database configurations or vulnerabilities in the schema update process could lead to data breaches or integrity issues if proper access controls and encryption mechanisms are not implemented.

Insufficient testing: Risks include incomplete coverage of test scenarios, which may result in undiscovered bugs or vulnerabilities in the frontend and backend components. Failure to adequately test the components could lead to errors, inconsistencies, or unexpected behavior in the application, impacting user experience and system reliability

Impact Probability	Low	Medium	High
Low	● Authentication Vulnerabilities	● Front-end vulnerability	● Security of registration keys
Medium	● Role assignment vulnerabilities	● Data validation failure	● Data security ● Authorization vulnerabilities ● Data integrity ● Data privacy
High	● Insufficient testing		

Table [3]: Risk management chart (Sprint - 2)

Risk ID	Risk Type and Description	Risk Score	Resolved in Sprint	Strategy and Effectiveness
US-5.1 #56	Data Integrity Data Privacy	High	TBD	Mitigate
US-5.2 #57	Front-End Vulnerability Data Privacy	Medium	TBD	Mitigate
US-5.3 #58	Front-End Vulnerability Data Privacy	Medium	TBD	Mitigate
US-5.4 #59	Authentication Vulnerabilities Data Security	High	TBD	Mitigate
US-5.5 #60	Authentication Vulnerabilities Front-End Vulnerability	Low	TBD	Avoid
US-5.6 #62	Authentication Vulnerabilities Data Privacy	High	TBD	Mitigate
US-5.7 #63	Insufficient testing	Low	TBD	Avoid
US-6.1 #64	Data Security Data Validation Failure	Medium	TBD	Mitigate
US-6.2 #65	Authorization Vulnerabilities Data Validation Failure	Low	TBD	Mitigate
US-6.3 #66	Front-End Vulnerability Data Validation Failure	Medium	TBD	Mitigate
US-6.4 #67	Front-End Vulnerability Data Validation Failure	Medium	TBD	Mitigate
US-6.5 #68	Data Validation Failure	Medium	TBD	Mitigate
US-6.6 #69	Insufficient testing	Low	TBD	Avoid
US-8.1 #70	Data Integrity Authorization Vulnerabilities Front-End Vulnerabilities	High	TBD	Mitigate
US-8.2 #71	Data Integrity Authorization Vulnerabilities Front-End Vulnerabilities	High	TBD	Mitigate
US-8.3 #72	Data Integrity Authorization Vulnerabilities Front-End Vulnerabilities	High	TBD	Mitigate
US-8.4 #73	Front-End Vulnerabilities Data Integrity	Medium	TBD	Mitigate
US-8.5 #74	Data integrity	Low	TBD	Accept
US-8.6 #75	Insufficient Testing	Low	TBD	Avoid
US-9.1	Security of Registration	Low	TBD	Mitigate

#76	Role Assignment Vulnerabilities			
US-9.2#77	Security of Registration	Low	TBD	Mitigate
US-9.3 #78	Data security Role assignment vulnerabilities	Medium	TBD	Mitigate
US-9.4 #79	Data Security	Medium	TBD	Mitigate
US-9.5 #80	Insufficient Testing	Low	TBD	Avoid

Table [4]: List of identified risks (Sprint - 2)

Sprint - 3

US-7: Condo Manager Upload File for Each Property

File integrity: Risks arise from uploading and managing files for each property, including risks of data corruption, loss, or unauthorized access if proper file integrity checks and access controls are not implemented. Without robust file validation mechanisms, there's a risk of uploading corrupted or malicious files, compromising the integrity of property data stored in the system.

Authorization vulnerabilities: Risks of unauthorized access to file upload functionalities if access control mechanisms are not implemented effectively. Weaknesses in authorization logic could allow unauthorized users to upload or access files, leading to data manipulation or security breaches.

Front-end vulnerability: Implementing the front-end React components for file upload introduces the risk of code injection or Cross-Site Scripting (XSS) attacks if proper input validation and sanitization measures are not implemented. Attackers could exploit vulnerabilities in the front-end code to execute malicious scripts within users' browsers.

Data security: Risks of unauthorized access or data breaches if sensitive files, such as property documents, contracts, or inspection reports, are not adequately protected. Proper security measures, such as encryption and access controls, are essential to prevent unauthorized access to sensitive property information stored in uploaded files.

Insufficient testing: Risks include incomplete coverage of test scenarios, which may result in undiscovered bugs or vulnerabilities in the frontend and backend components. Failure to adequately test the components could lead to errors, inconsistencies, or unexpected behavior in the application, impacting user experience and system reliability

US-10: Implement Condo Fee Rate Entry

Data accuracy: Risks arise from entering and managing condo fee rates, including risks of data entry errors, inconsistencies, or inaccuracies if proper validation and verification processes are not implemented. Without adequate controls, there's a risk of entering incorrect fee rates, leading to financial discrepancies or incorrect billing for condo owners.

Authorization vulnerabilities: Risks of unauthorized access to fee rate entry functionalities if access control mechanisms are not implemented effectively. Weaknesses in authorization logic could allow unauthorized users to modify fee rates, leading to financial manipulation or disputes.

Front-end vulnerability: Implementing the front-end React components for fee rate entry introduces the risk of code injection or Cross-Site Scripting (XSS) attacks if proper input validation and sanitization measures are not implemented. Attackers could exploit vulnerabilities in the front-end code to execute malicious scripts within users' browsers.

Data security: Risks of unauthorized access or data breaches if fee rate data is not adequately protected. Proper security measures, such as encryption and access controls, are essential to prevent unauthorized access to sensitive financial information related to condo fee rates.

Insufficient testing: Risks include incomplete coverage of test scenarios, which may result in undiscovered bugs or vulnerabilities in the frontend and backend components. Failure to adequately test the components could lead to errors, inconsistencies, or unexpected behavior in the application, impacting user experience and system reliability

US-11: Calculate and Present Condo Fees

Accuracy of calculations: Risks arise from calculating condo fees, including the potential for errors or discrepancies in fee calculations if the underlying algorithms or formulas are not implemented correctly. Incorrect fee calculations could lead to financial inaccuracies, billing discrepancies, or dissatisfaction among condo owners.

Data integrity: Risks of data corruption or loss if proper data validation and error handling mechanisms are not implemented during fee calculation processes. Without adequate safeguards, there's a risk of processing invalid or incomplete data, leading to incorrect fee calculations or system failures.

Performance issues: Risks of performance degradation or system overload during fee calculation processes, especially if dealing with large datasets or complex calculations. Inefficient algorithms or resource-intensive calculations could lead to system slowdowns, timeouts, or unresponsive behavior, impacting user experience and system reliability.

Transparency and auditability: Risks of insufficient transparency or auditability in fee calculation processes, which could lead to mistrust or disputes among condo owners. Clear documentation and logging of fee calculation steps are essential to ensure accountability and facilitate auditing and reconciliation processes.

Insufficient testing: Risks include incomplete coverage of test scenarios, which may result in undiscovered bugs or vulnerabilities in the frontend and backend components. Failure to adequately test the components could lead to errors, inconsistencies, or unexpected behavior in the application, impacting user experience and system reliability

US-12: Record Operational Budget and Costs

Data accuracy and completeness: Risks arise from recording operational budgets and costs, including the potential for inaccuracies or omissions if proper validation and verification processes are not in place. Without adequate controls, there's a risk of recording incorrect budget figures or missing essential cost data, leading to financial discrepancies or mismanagement of funds.

Security of financial data: Risks of unauthorized access or data breaches if operational budget and cost records are not adequately protected. Proper security measures, such as encryption, access controls, and regular security audits, are essential to prevent unauthorized access to sensitive financial information.

Compliance with regulations: Risks of non-compliance with financial regulations or reporting standards if budget and cost recording processes do not adhere to legal requirements. Failure to comply with regulations could lead to penalties, fines, or legal liabilities for the organization.

Integration with accounting systems: Risks associated with integrating budget and cost records with accounting systems or financial software. Incompatible formats, data discrepancies, or errors during data transfer could lead to synchronization issues or inconsistencies between systems, impacting financial reporting and analysis.

Insufficient documentation and audit trail: Risks of inadequate documentation or audit trail for budget and cost recording processes, which could hinder transparency, accountability, and auditability. Clear documentation of recording procedures, approvals, and changes is essential to ensure traceability and facilitate financial audits and reviews.

US-13: Generate Annual Financial Reports

Data accuracy and completeness: Risks arise from generating annual financial reports, including the potential for inaccuracies or missing data if proper validation and verification processes are not in place. Without adequate controls, there's a risk of including incorrect financial figures or omitting essential information, leading to unreliable reports and misinformed decision-making.

Timeliness of reporting: Risks of delays or missed deadlines in generating annual financial reports, especially if the reporting process is manual or reliant on inefficient workflows. Delays in reporting could impact stakeholders' ability to make informed decisions or comply with regulatory requirements, leading to reputational damage or legal consequences.

Compliance with reporting standards: Risks of non-compliance with financial reporting standards or regulatory requirements if annual financial reports do not adhere to prescribed formats or guidelines. Failure to comply with reporting standards could result in penalties, fines, or legal liabilities for the organization.

Data security and confidentiality: Risks of unauthorized access or disclosure of sensitive financial information contained in annual reports. Proper security measures, such as encryption, access controls, and data anonymization, are essential to protect confidential financial data from unauthorized disclosure or misuse.

Auditability and transparency: Risks of insufficient auditability or transparency in the generation process of annual financial reports, which could hinder accountability and scrutiny. Clear documentation of reporting procedures, data sources, and assumptions is necessary to facilitate financial audits and reviews, ensuring the integrity and reliability of the reports.

Impact Probability	Low	Medium	High
Low	● Performance Issues	● Front-end Vulnerability ● Transparency and Auditability	● Data Integrity ● Timeliness of Reporting
Medium	● Insufficient Testing ● Integration with Accounting Systems	● File Integrity ● Compliance with Regulations	● Authorization Vulnerabilities ● Data Accuracy ● Data Accuracy and Completeness ● Compliance with Reporting Standards
High	● Accuracy of Calculations	● Insufficient Documentation and Audit Trail ● Auditability and Transparency	● Data Security ● Security of Financial Data ● Data Security and Confidentiality

Table [5]: Risk management chart (Sprint - 3)

Risk ID	Risk Type and Description	Risk Score	Resolved in Sprint	Strategy and Effectiveness
US-7.1 #	File integrity	Medium	TBD	Mitigate
US-7.2 #	Authorization vulnerabilities	High	TBD	Mitigate
US-7.3 #	Front-end vulnerability	Medium	TBD	Mitigate
US-7.4 #	Data security	High	TBD	Mitigate
US-7.5 #	Insufficient testing	Low	TBD	Avoid
US-10.1 #	Data accuracy	Medium	TBD	Mitigate
US-10.2 #	Authorization vulnerabilities	High	TBD	Mitigate
US-10.3 #	Front-end vulnerability	Medium	TBD	Mitigate
US-10.4 #	Data security	High	TBD	Mitigate
US-10.5 #	Insufficient testing	Low	TBD	Avoid
US-11.1 #	Accuracy of calculations	High	TBD	Mitigate
US-11.2 #	Data integrity	High	TBD	Mitigate
US-11.3 #	Performance issues	Low	TBD	Avoid
US-11.4 #	Transparency and auditability	Medium	TBD	Mitigate
US-11.5 #	Insufficient testing	Low	TBD	Avoid
US-12.1 #	Security of financial data	High	TBD	Mitigate
US-12.2 #	Data accuracy and completeness	Medium	TBD	Mitigate
US-12.3 #	Compliance with regulations	Low	TBD	Mitigate
US-12.4 #	Integration with accounting systems	Medium	TBD	Mitigate
US-12.5 #	Insufficient documentation and audit trail	Medium	TBD	Avoid
US-13.1 #	Timeliness of reporting	Low	TBD	Accept
US-13.2 #	Data accuracy and completeness	Medium	TBD	Accept

US-13.3 #	Compliance with reporting standards	High	TBD	Mitigate
US-13.4 #	Data security and confidentiality	High	TBD	Mitigate
US-13.5 #	Auditability and transparency	Medium	TBD	Avoid

Table [6]: List of identified risks (Sprint - 3)

Sprint - 4

US-14: Set Up Common Facilities Management

Infrastructure readiness: Risks associated with setting up common facilities management include the readiness of infrastructure such as physical spaces, equipment, and utilities. Delays or deficiencies in infrastructure preparation could hinder the effective management of common facilities, leading to operational disruptions or inefficiencies.

Resource allocation: Risks related to allocating sufficient resources, including personnel, budget, and technology, for managing common facilities. Inadequate resources may result in suboptimal facility management practices, compromising the quality of service provided to occupants or users of the facilities.

Compliance with regulations: Risks of non-compliance with regulatory requirements or building codes in the setup of common facilities management. Failure to adhere to regulations could result in fines, penalties, or legal liabilities for the organization, as well as safety or health hazards for occupants.

Integration with existing systems: Risks associated with integrating common facilities management systems with existing property management or operational systems.

Compatibility issues, data discrepancies, or technical challenges during integration could disrupt facility management processes or data flow, affecting service delivery and decision-making.

User training and adoption: Risks of insufficient user training or resistance to adopting new facility management processes or technologies. Inadequate training programs or lack of user engagement may impede the effective utilization of common facilities management systems, limiting their potential benefits and efficiency gains.

US-15: Calender-Like Interface for Facility Reservation

User interface design: Risks associated with the design and implementation of a calendar-like interface for facility reservation. Poor user interface design may lead to usability issues, such as difficulty in navigating the calendar, confusion in booking facilities, or inconsistencies in displaying reservation information, resulting in user dissatisfaction and decreased adoption.

Concurrency and conflicts: Risks of managing concurrent reservation requests and resolving conflicts in booking facilities. Without proper concurrency control mechanisms, multiple users may attempt to reserve the same facility simultaneously, leading to conflicts or overbooking situations that could disrupt scheduling and cause frustration among users.

Data integrity and security: Risks related to ensuring the integrity and security of reservation data in the calendar interface. Vulnerabilities such as data corruption, unauthorized access, or data loss could compromise the accuracy and confidentiality of reservation information, impacting the reliability and trustworthiness of the system.

Integration with backend systems: Risks associated with integrating the calendar interface with backend systems for facility management and reservation tracking. Compatibility issues, data synchronization errors, or communication failures between the frontend interface and backend databases may result in inconsistencies or inaccuracies in reservation data, affecting the overall functionality and usability of the system.

Scalability and performance: Risks of scalability and performance bottlenecks in handling large volumes of reservation requests or concurrent user interactions. Inadequate system scalability or inefficient resource utilization may lead to slow response times, system crashes, or degraded performance during peak usage periods, negatively impacting user experience and satisfaction.

US-16: Display Real-Time Availability in Reservation System

Data synchronization: Risks associated with ensuring real-time synchronization of availability data across the reservation system. Inaccurate or delayed updates to availability status may lead to conflicts or inconsistencies in reservation requests, resulting in double bookings or missed opportunities for users to reserve facilities, ultimately impacting user satisfaction and system reliability.

Concurrency control: Risks of managing concurrent access to availability information by multiple users. Without proper concurrency control mechanisms, simultaneous reservation requests may lead to conflicts or race conditions, where users may inadvertently book the same facility or encounter errors due to inconsistent data states, leading to frustration and confusion.

Performance optimization: Risks related to optimizing system performance for real-time availability updates. Processing and propagating availability changes in a timely manner require efficient algorithms and resource utilization to minimize latency and ensure responsiveness, especially during periods of high user activity or frequent reservation updates.

User interface responsiveness: Risks associated with displaying real-time availability information to users in the reservation system interface. Ensuring that availability status updates are promptly reflected in the user interface without perceptible delays or inconsistencies is crucial for providing a seamless and intuitive booking experience, as any lag or inaccuracies may undermine user trust and satisfaction.

Data integrity and security: Risks of maintaining the integrity and security of availability data in the reservation system. Vulnerabilities such as unauthorized access, data tampering, or system breaches could compromise the accuracy and confidentiality of availability information, leading to unauthorized bookings, data loss, or privacy violations, posing significant risks to system reliability and user trust.

US-17: Manage Reservations on a First-Come-First-Serve Basis

Fairness and equity: Risks associated with ensuring fair and equitable treatment of users in the reservation process. Implementing a first-come-first-serve (FCFS) policy may lead to challenges in prioritizing reservation requests based on their submission time, potentially resulting in dissatisfaction or disputes among users who perceive the allocation of facilities as unfair or biased.

Concurrency and contention: Risks of managing concurrent reservation requests and potential contention for limited resources. In scenarios where multiple users submit reservation requests simultaneously for the same facility or time slot, conflicts may arise, requiring robust concurrency control mechanisms to prevent double bookings, race conditions, or inconsistent outcomes, which could undermine user trust and system reliability.

System scalability: Risks related to the scalability of the reservation system to handle increasing demand and workload. As the number of reservation requests grows, the system must efficiently process and manage incoming requests while maintaining responsiveness and performance, without experiencing bottlenecks, degradation, or service disruptions that could impact user experience and satisfaction.

Feedback and communication: Risks associated with providing timely feedback and communication to users regarding the status of their reservation requests. Ensuring clear and transparent communication channels for notifying users about the outcome of their reservation attempts, including confirmations, rejections, or waitlist notifications, is essential for managing user expectations and fostering trust in the reservation process.

Compliance and regulations: Risks of compliance with relevant policies, regulations, or contractual obligations governing reservation management. Adhering to legal requirements, organizational policies, or contractual agreements regarding reservation procedures, data privacy, or accessibility standards is critical for mitigating legal liabilities, reputational risks, and potential sanctions or penalties that could arise from non-compliance.

US-18: Design Role-Based Access Control System

Complexity in role definition: Risks associated with defining and managing roles within the access control system. Designing a role-based access control (RBAC) system requires careful consideration of user roles, permissions, and hierarchical structures to ensure that access rights are properly assigned and enforced. Inadequate role definition or misalignment between roles and organizational responsibilities may lead to access inconsistencies, security vulnerabilities, or administrative overhead, impacting system integrity and usability.

Granularity and flexibility: Risks related to achieving the right balance between granularity and flexibility in access control policies. Striking a balance between fine-grained access control to enforce least privilege principles and flexible role assignment to accommodate dynamic user roles and evolving organizational needs is challenging. Overly restrictive access policies may hinder user productivity, while overly permissive policies may increase the risk of unauthorized access, data breaches, or privilege escalation, necessitating careful policy design and review.

Access control enforcement: Risks associated with the effective enforcement of access control policies across the system. Implementing robust mechanisms for access validation, authorization, and audit logging is essential for preventing unauthorized access attempts, privilege abuse, or security breaches. Failure to properly enforce access controls may result in data exposure, unauthorized modifications, or unauthorized actions by malicious insiders or external attackers, compromising system confidentiality, integrity, and availability.

Integration and interoperability: Risks of integrating the RBAC system with existing infrastructure, applications, and identity management solutions. Ensuring seamless interoperability and compatibility with diverse platforms, protocols, and authentication mechanisms requires thorough integration testing, validation, and configuration management. Incompatibilities, misconfigurations, or interoperability issues may disrupt access control operations, user authentication, or provisioning workflows, leading to service disruptions, user frustration, or security vulnerabilities.

Compliance and governance: Risks related to compliance with regulatory requirements, industry standards, or organizational policies governing access control practices. Adhering to data protection regulations, privacy laws, or industry-specific mandates regarding access rights, user consent, and data handling is crucial for mitigating legal risks, reputational damage, or financial penalties associated with non-compliance. Implementing effective access controls, audit trails, and governance frameworks is essential for demonstrating compliance, accountability, and risk management practices to stakeholders and regulatory authorities.

US-19: Predefined Roles and Permissions Setup

Role definition accuracy: Risks associated with accurately defining predefined roles and permissions to align with the needs and responsibilities of different user groups within the system. The definition of roles must be comprehensive, clear, and reflective of organizational requirements to ensure that users are assigned appropriate access rights and privileges. Risks include ambiguities in role definitions, inconsistencies in permission assignments, or inadequate consideration of user roles' functional requirements, which could lead to unauthorized access, data breaches, or operational inefficiencies.

Permission granularity and control: Risks related to the granularity and control of permissions assigned to predefined roles within the system. The permission model must support fine-grained access control to restrict users' actions and privileges based on their roles and responsibilities. Risks include overly permissive permissions, insufficient segregation of duties, or lack of controls to enforce least privilege principles, resulting in elevated security risks, data exposure, or regulatory non-compliance.

Role-based access control (RBAC) implementation: Risks associated with the implementation of role-based access control mechanisms to enforce predefined roles and permissions effectively. The RBAC system must be robust, scalable, and configurable to accommodate changes in user roles, organizational structures, and access requirements over time. Risks include implementation flaws, vulnerabilities in access control logic, or misconfigurations that could result in access violations, privilege escalation, or unauthorized actions by users, compromising system security and integrity.

User role mapping and assignment: Risks related to accurately mapping user identities to predefined roles and managing role assignments dynamically. The role assignment process must be automated, auditable, and consistent to ensure that users are granted the appropriate level of access based on their roles, responsibilities, and organizational affiliations. Risks include errors in role mapping, manual oversight, or inconsistencies in access provisioning, leading to unauthorized access, data leaks, or compliance violations.

Role evolution and maintenance: Risks associated with the evolution and maintenance of predefined roles and permissions over time. The role definition process must be iterative, adaptive, and responsive to changing organizational needs, regulatory requirements, and security threats. Risks include role proliferation, role creep, or lack of governance mechanisms to review, update, and deprecate roles periodically, resulting in role redundancy, confusion, or inefficiencies in access management and enforcement. Regular audits, role lifecycle management, and role-based training programs can help mitigate these risks and ensure the continued effectiveness of the role-based access control system.

Impact Probability	Low	Medium	High
Low	● Infrastructure readiness ● Fairness and equity	● Resource allocation ● Feedback and communication	● Granularity and flexibility ● User role mapping and assignment
Medium	● Compliance with regulations ● Integration with backend systems ● Complexity in role definition	● User interface design ● Data synchronization ● System scalability ● Role evolution and maintenance	● Concurrency and conflicts ● Access control enforcement ● Role-based access control (RBAC) implementation
High	● Integration with existing systems ● User training and adoption ● User interface responsiveness	● Scalability and performance ● Integration and interoperability	● Data integrity and security

Table [7]: Risk management chart (Sprint - 4)

Risk ID	Risk Type and Description	Risk Score	Resolved in Sprint	Strategy and Effectiveness
US-14.1 #			TBD	
US-14.2 #			TBD	
US-14.3 #			TBD	
US-14.4 #			TBD	
US-14.5 #			TBD	
US-15.1 #			TBD	
US-15.2 #			TBD	
US-15.3 #			TBD	
US-15.4 #			TBD	
US-16.1 #			TBD	
US-16.2 #			TBD	
US-16.3 #			TBD	
US-16.4 #			TBD	
US-17.1 #			TBD	
US-17.2			TBD	

#				
US-17.3 #			TBD	
US-17.4 #			TBD	
US-18.1 #			TBD	
US-18.2 #			TBD	
US-18.3 #			TBD	
US-18.4 #			TBD	
US-19.1 #			TBD	
US-19.2 #			TBD	
US-19.3 #			TBD	
US-19.4 #			TBD	

Table [8]: List of identified risks (Sprint - 4)

Sprint - 5

US-20: Manage Employee Roles Interface

Role assignment errors: Risks associated with inaccuracies or inconsistencies in assigning roles to employees through the management interface. The interface for managing employee roles may be prone to user errors, such as selecting incorrect roles, assigning excessive permissions, or overlooking critical access requirements. These errors could result in unauthorized access, data breaches, or compliance violations, impacting system security and integrity.

Complexity in role management: Risks related to the complexity of managing employee roles effectively through the interface. As the organization grows or undergoes structural changes, the number of roles, permissions, and access requirements may increase, leading to greater complexity in role management. Without intuitive and efficient interfaces for role assignment, modification, or revocation, administrators may struggle to maintain accurate and up-to-date role assignments, increasing the risk of access control errors or inconsistencies.

Access control misconfigurations: Risks of misconfiguring access control settings or policies through the management interface. Administrators responsible for configuring employee roles may inadvertently misconfigure access control settings, such as granting excessive privileges, applying incorrect permissions, or overlooking security best practices. These misconfigurations could create security vulnerabilities, exploit opportunities, or compliance gaps, exposing the system to unauthorized access, data leakage, or malicious activities.

Auditability and accountability: Risks associated with the lack of auditability and accountability features in the role management interface. Without robust audit trails, logging mechanisms, or access control monitoring capabilities, it may be challenging to track changes to role assignments, identify unauthorized modifications, or detect suspicious activities. Inadequate auditability and accountability features could hinder incident response efforts, forensic investigations, or compliance audits, reducing the organization's ability to detect, mitigate, or prevent security incidents.

User training and awareness: Risks stemming from insufficient user training or awareness regarding role management practices and interface usage. Users responsible for managing employee roles may lack the necessary knowledge, skills, or awareness to perform their roles effectively, increasing the likelihood of errors, omissions, or misconfigurations in role assignments. Providing comprehensive training, documentation, or guidance on role management best practices and interface functionalities is essential for mitigating user-related risks and enhancing overall system security and compliance.

US-21: Secure and Scalable System

Security vulnerabilities: Risks associated with potential security vulnerabilities in the system architecture, design, or implementation. As the system scales to accommodate a larger user base or increased data processing requirements, it may become more susceptible to security threats, such as unauthorized access, data breaches, or denial-of-service attacks. Failure to address security vulnerabilities proactively through measures such as threat modeling, code reviews, or penetration testing could expose the system to exploitation, compromising sensitive data or disrupting system operations.

Data privacy and compliance: Risks related to maintaining data privacy and compliance with regulatory requirements as the system scales. Handling sensitive user data or processing personal information imposes legal and regulatory obligations regarding data protection, privacy, and security. Failure to implement robust data privacy controls, encryption mechanisms, or compliance monitoring measures could result in non-compliance penalties, legal liabilities, or reputational damage to the organization.

Performance bottlenecks: Risks of performance bottlenecks or degradation as the system scales to handle increased user traffic or data volume. Inadequate capacity planning, resource allocation, or system optimization strategies may lead to performance issues, such as slow response times, system downtime, or service interruptions. Mitigating performance risks requires careful monitoring, performance testing, and optimization efforts to ensure that the system can scale effectively while maintaining optimal performance levels.

Infrastructure dependencies: Risks associated with dependencies on external infrastructure or third-party services for system scalability. Relying on external providers for cloud hosting, storage, or other infrastructure components introduces dependencies that may impact system availability, reliability, or performance. Service outages, network disruptions, or changes in service-level agreements (SLAs) could affect the system's ability to scale seamlessly, requiring contingency plans, redundancy measures, or alternative deployment strategies to mitigate risks and ensure uninterrupted service delivery.

Cost management: Risks related to managing costs associated with system scalability and resource provisioning. Scaling infrastructure resources, such as compute instances, storage, or network bandwidth, to accommodate increased demand or workload fluctuations can incur additional costs. Failure to anticipate, monitor, or control scalability-related expenses could lead to budget overruns, financial constraints, or resource shortages, affecting the organization's ability to sustainably scale the system while managing operational costs effectively. Implementing cost optimization strategies, such as usage monitoring, resource allocation policies, or pricing negotiations with service providers, is essential for mitigating cost-related risks and ensuring long-term scalability and financial viability.

US-22: Owners can Submit Requests for Services from Employees

Service request processing: Risks associated with the processing and management of service requests submitted by owners to employees. As owners submit requests for various services, such as maintenance, repairs, or amenities, there is a risk of delays, miscommunication, or errors in processing these requests efficiently. Failure to establish clear procedures, workflows, or communication channels for handling service requests could result in delays in service delivery, dissatisfaction among owners, or disruptions in property management operations.

Data security and privacy: Risks related to the security and privacy of owner-submitted service requests and associated data. Service requests may contain sensitive information, such as personal details, property locations, or service preferences, which must be handled securely to prevent unauthorized access, data breaches, or privacy violations. Inadequate data encryption, access controls, or data handling practices could expose owner information to unauthorized parties, compromising confidentiality and trust in the system.

Resource allocation and scheduling: Risks of inefficient resource allocation and scheduling for fulfilling service requests submitted by owners. Property management teams must allocate resources, such as personnel, equipment, or materials, effectively to address service requests in a timely manner. Failure to optimize resource allocation, prioritize requests based on urgency or importance, or maintain accurate scheduling records could lead to inefficiencies, service delays, or conflicts in resource utilization, impacting owner satisfaction and property operations.

Communication breakdowns: Risks of communication breakdowns between owners, employees, and management teams involved in the service request process. Effective communication is essential for conveying service request details, status updates, or resolution actions between stakeholders, ensuring transparency, accountability, and responsiveness in service delivery. Lack of clear communication channels, protocols, or escalation procedures could result in misunderstandings, unresolved issues, or dissatisfaction among owners and employees, undermining trust and collaboration within the property management ecosystem.

Service quality and performance: Risks related to maintaining service quality and performance standards while fulfilling owner requests. Property management teams must ensure that service requests are addressed promptly, accurately, and satisfactorily to meet owner expectations and contractual obligations. Failure to deliver high-quality services, adhere to service level agreements (SLAs), or address owner feedback and complaints effectively could lead to reputational damage, loss of business, or legal liabilities for the property management company. Implementing robust quality assurance measures, performance metrics, and service improvement initiatives is crucial for mitigating risks and enhancing owner satisfaction and loyalty.

US-23: Employee (Paul) Accessing Assigned Request From Condo Owners

Data Security: There's a risk of unauthorized access to sensitive information if proper access controls are not implemented. If Paul can access requests beyond his assigned scope, it could lead to privacy breaches and data leaks.

Confidentiality Breach: If Paul can view requests from condo owners that are meant to be confidential or restricted to other employees or managers, it could result in a breach of confidentiality.

Data Integrity: If Paul has the ability to modify or tamper with requests that he shouldn't have access to, it could lead to data integrity issues and affect the accuracy and reliability of the information stored in the system.

Miscommunication: Allowing Paul to access requests from condo owners may result in miscommunication or misunderstandings if he acts on requests that are not within his assigned responsibilities or if he provides incorrect information.

US-24: Create User Notification Page or Updates

Notification delivery reliability: Risks associated with ensuring the reliable delivery of notifications to users regarding important updates, announcements, or events. The notification system must be robust enough to handle high volumes of notifications efficiently and deliver them to users in a timely manner. Risks include system failures, network issues, or software bugs that could result in delays, missed notifications, or inconsistent delivery, leading to user frustration and dissatisfaction with the platform.

Content accuracy and relevance: Risks of providing users with inaccurate, outdated, or irrelevant information through notifications. The content of notifications, including updates, alerts, or reminders, must be carefully curated and validated to ensure its accuracy, relevance, and usefulness to users. Risks include errors in content generation, inappropriate targeting or segmentation of notifications, or lack of mechanisms to verify the validity and currency of information, which could undermine user trust and confidence in the platform.

User privacy and data protection: Risks related to the privacy and security of user data and preferences used for delivering notifications. The notification system must comply with privacy regulations and industry standards to protect user information from unauthorized access, disclosure, or misuse. Risks include data breaches, unauthorized data sharing, or inadequate safeguards for storing and transmitting sensitive user data, leading to privacy violations, legal liabilities, or reputational damage for the platform.

Notification overload and fatigue: Risks of overwhelming users with excessive or intrusive notifications, leading to notification fatigue and disengagement. The frequency, timing, and relevance of notifications must be carefully managed to avoid overwhelming users with unnecessary or irrelevant information. Risks include overzealous notification strategies, lack of user control over notification settings, or failure to respect user preferences and boundaries, resulting in user dissatisfaction, decreased engagement, or even opt-out from the notification system.

Impact Probability	Low	Medium	High
Low	🟩	🟩	🟧
Medium	🟩	🟧	🟥
High	🟧	🟥	🟥

Table [9]: Risk management chart (Sprint - 5)

Risk ID	Risk Type and Description	Risk Score	Resolved in Sprint	Strategy and Effectiveness
US-20.1 #			TBD	
US-20.2 #			TBD	
US-20.3 #			TBD	
US-20.4 #			TBD	
US-21.1 #			TBD	
US-21.2 #			TBD	
US-21.3 #			TBD	
US-21.4 #			TBD	
US-22.1 #			TBD	
US-22.2 #			TBD	
US-22.3 #			TBD	
US-22.4 #			TBD	
US-22.5 #			TBD	
US-23.1 #			TBD	
US-23.2 #			TBD	
US-23.3 #			TBD	
US-23.4 #			TBD	
US-23.5 #			TBD	
US-24.1 #			TBD	
US-24.2 #			TBD	
US- 24.3 #			TBD	
US-24.4 #			TBD	

US-24.5 #			TBD	

Table [10]: List of identified risks (Sprint - 5)