Risk assessment for Umi

Low-Risk Issues

1. **User Interface Bugs (Low Risk)**
    - **Risk:** Minor bugs in the interface can cause minor display issues.
    - **Mitigation:** Conduct regular usability tests and quality assurance sessions during development to catch bugs early. Prioritize user feedback for UI improvements.
2. **API Integration Challenges (Low Risk)**
    - **Risk:** Minor inconsistencies when integrating Notion and Spotify APIs.
    - **Mitigation:** Allocate buffer time in the schedule to debug and test each API feature. Maintain thorough documentation on API behaviors and limitations.
3. **Data Loss in Task Management (Low Risk)**
    - **Risk:** Users may experience data loss if not saved correctly.
    - **Mitigation:** Implement autosave functionality and backups. Provide users with a prompt to confirm task completion or exit without saving to avoid accidental data loss.
4. **Calendar Sync Errors (Low Risk)**
    - **Risk:** Synchronization delays between Umi's calendar and Google Calendar.
    - **Mitigation:** Set up automatic syncing at regular intervals and provide users with a manual sync option.
5. **Mascot Design Overload (Low Risk)**
    - **Risk:** Mascot animations or interactions could be distracting.
    - **Mitigation:** Test mascot engagement with target users and allow users to turn off or limit mascot interactions if preferred.

Medium-Risk Issues

6. **Scalability of Server Resources (Medium Risk)**
    - **Risk:** Increased user load may slow down the application.
    - **Mitigation:** Monitor server capacity and set up scalable infrastructure on cloud services, allowing for auto-scaling if the application gains more users.
7. **Compatibility with Different Browsers/Devices (Medium Risk)**
    - **Risk:** UI may not render consistently across devices and browsers.
    - **Mitigation:** Conduct cross-browser testing and prioritize responsive design using media queries for common devices and browsers, ensuring accessibility and usability on various platforms.
8. **User Data Privacy (Medium Risk)**
    - **Risk:** Sensitive user data could be mishandled or exposed.
    - **Mitigation:** Use encryption for data storage and transmission, and clearly communicate privacy policies. Regularly audit code and systems for security compliance.

High-Risk Issues

9. **API Downtime or Service Changes (High Risk)**
    - **Risk:** Reliance on Notion and Spotify APIs makes the application vulnerable to changes or outages.

- **Mitigation:** Implement fallback functions for key features, like local task management or offline music playlists, to ensure core functionalities are accessible even if APIs are down.

10. **Project Scope Creep (High Risk)**
    - **Risk:** Adding too many features could delay the project timeline.
    - **Mitigation:** Maintain a clear project scope and establish regular checkpoints to assess progress. If new features are suggested, evaluate and prioritize them based on impact and feasibility, considering deferring extras to later versions.