## Risk plan

### Introduction

At present, people's demand for sports and fitness is increasing, and the application trend of health sports combined with high technology, online and big data is obvious.According to the Research report on China's Sports and Fitness Market in the third quarter of 2020, under the influence of the epidemic, residents' fitness and health issues have become a national social topic.So we decided to build a motion counting system to monitor our exercise.During the project development process, there may be some risks that require risk management and control.When it comes to projects or businesses, risks are unavoidable.Risk management is a systematic approach that can help identify, evaluate, and mitigate these risks to ensure the success of a project or business.Risk planning is a part of risk management that describes how to identify, evaluate, mitigate, and monitor risks in a project or business.Risk planning is an important tool that can help management teams predict potential problems and take measures to mitigate the impact of risks.

#### 1.1 O verview of major risks

Technical risk, safety risk, legal and ethical risk, demand change risk, poor communication risk, schedule risk and quality risk.

#### 1.2 Responsibilities

The responsibilities of the three members of the team include requirements analysis, design and architecture, coding and testing, and document writing.

### 2. Project risk table

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| classification | risk | r isk description | risk grade | Risk probability | Risk impact |
|  | The algorithm is inaccurate | The accuracy of the algorithm depends on the quality and quantity of the dataset, and it may be affected if the training dataset is either insufficient or less accurate. | Medium | 10%-30% | 0.6 |
|  | code error | If the code has an error, it may cause the program to crash or produce an incorrect output. | High | 20%-40% | 0.8 |
|  | Compatibility problem | The program may be incompatible with some hardware or software. | Medium | 15%-30% | 0.6 |
| Technical risk | security hole | If the program involves user data or sensitive information, security vulnerabilities may exist. | High | 10%-20% | 0.9 |
|  | Performance problems | Performance problems may arise when a program needs to process large amounts of data or perform complex calculations. | Medium | 10%-20% | 0.7 |
|  | Program scalability issues | If the program requires to extend or modify, scalability issues may arise. | High | 10%-20% | 0.6 |
|  | Data quality issues | If the program needs to process large amounts of data, data quality issues may arise. | Medium | 20%-30% | 0.7 |
|  | Program dependency issues | If a program depends on other software or libraries, dependency problems may arise. | Medium | 10%-30% | 0.5 |
|  | Quality risk | Users have high requirements for software quality, and if the project team members lack the development experience of the same type of projects, they need to pay close attention to the quality risk of the project. | Medium | 10%-15% | 0.6 |
|  | Data leakage | If the program involves user data or sensitive information, there may be a risk of data leakage. | High | 5%-20% | 0.8 |
| security risk | network attack | If the program communicates through the network, there may be a risk of a network attack. | High | Depends on the details of the project and the improvement of the safety measures | 0.9 |
|  | malicious software | If the program has a vulnerability or a security vulnerability, it may be attacked by malicious software. | Medium | Depends on the details of the project and the improvement of the safety measures | 0.6 |
|  | Code injection | If the program has a security vulnerability, it may be attacked by the code injection. | Medium | Depends on the details of the project and the improvement of the safety measures | 0.6 |
|  | privacy leak | If the program collects the user's personal health data, such as height, weight, heart rate, etc., then the data may be hacked or used improperly. | High | Depends on the details of the project and the improvement of the safety measures | 0.8 |
|  | data security | If the data is not properly stored or secure, then hackers may easily obtain the data, leading to personal privacy leakage of users. | High | Depends on the details of the project and the improvement of the safety measures | 0.9 |
| Legal and ethical risks | Liability and exemption clause | If the program fails to properly count the number of squats and push-ups, then the user may be harmed. In this case, the developer of the program may face legal action. | centre | 5% | 0.6 |
|  | ethical principle | Developers should follow ethical principles to ensure that their programs do not harm users or violate their personal privacy. | low | 5% | 0.3 |
|  | Abide by laws and regulations | Developers should comply with local laws and regulations to ensure that their procedures do not violate any laws and regulations. | low | 5% | 0.2 |
| Manage risk | Demand change risk | In the development process, there may be unclear definition of requirements, insufficient accuracy, or users do not really understand their needs, as well as various problems and technical support in the APP development process, which may cause the risk of demand change. | Medium | It ends on many factors, such as the size of the project, complexity, the effectiveness of demand management, the change of customer needs and so on. | 0.6 |
| Personnel risk | Poor risk of communication | Poor communication among members of the project is a very important factor affecting the smooth progress of the project. There may be differences in needs, development direction and technology leading to poor communication. | High | It depends on multiple factors, such as the background and cultural differences of the team members, the choice of communication methods and tools, the clarity and accuracy of the communication content, etc | 0.8 |
| Progress risk | Schedule delay | The project is demanding on the schedule, and the project schedule delay means the failed development. | High | 5%-10% | 0.8 |

### Risk Mitigation，Monitoring，Management

|  |  |  |  |
| --- | --- | --- | --- |
| R isk | Risk Mitigation | Risk Monitoring | Risk Management |
| The algorithm is inaccurate | Ensure the correctness of the algorithm, including theoretical proof, testing, etc.;  Optimize the algorithm to improve its accuracy and robustness;  Introduce the manual intervention mechanism to review and correct the algorithm results; | Monitor the output results of the algorithm, and find and correct the errors in time;  Monitor the operation of the algorithm, discover and solve the performance problems;  Monitor the use of the algorithm, collect user feedback and suggestions, and make timely improvement. | Establish a perfect algorithm development process, including demand analysis, design, development, testing, release and other links, to ensure the quality and stability of the algorithm |
| code error | Write high-quality code, follow best practices and standard specifications, and ensure code quality and readability.  Use automated test tools, such as unit testing, integration testing, and end-to-end testing, to ensure code correctness and stability. | Regular code review and testing to detect and fix potential errors. | Establish a management process for code errors and vulnerabilities to ensure timely detection and repair.  Establish a disaster recovery plan to respond to system failures and data loss caused by code errors. |
| Compatibility problem | During the design and development stages, consider compatibility issues across platforms and across browsers, ensuring that the code can be run in different environments. | Conduct compatibility tests to ensure that the application works properly in different environments. | Establish the management process of compatibility issues, and find and fix the problems in time. |
| security hole | Using security coding practices, such as input validation, error handling, and security configuration, can help reduce vulnerabilities in the code. | Scan for security vulnerabilities regularly, and take timely measures | Establish a security vulnerability management process to ensure the timely detection and repair of vulnerabilities. |
| Performance problems | During development, performance tests should be performed periodically to ensure that the system can meet the desired performance requirements. | Monitor the system performance, timely identify the performance problems and bottlenecks, and take measures in time | Establish performance problem management processes to ensure timely detection and resolution of performance issues. |
| Program scalability issues | A modular design and development approach enables individual parts of the system to be developed, tested, and deployed independently | Track the expansion requirements and changes of the system, and modify and optimize accordingly in time. | Establish scalability planning and strategies, including the system architecture, design, and development process, to ensure that the system can meet the future expansion requirements. |
| Data quality issues | Clean the data to remove duplicate, invalid or incorrect data to ensure the accuracy and completeness of the data. | Monitor data quality regularly, for example, through data quality reports or data monitoring tools, to timely detect data quality problems and take corresponding measures | Develop a data management plan, including data collection, data processing, data storage and other processes, clarify the responsibility and process of data management, and ensure the quality and safety of data |
| Program dependency issues | Management program dependency, including dependent version, dependent source, dependent update, etc., to ensure the reliability and stability of dependency. | Monitor dependent versions regularly, detect changes in dependent versions and take appropriate measures, such as upgrading or fallback dependent versions. | Develop a dependency management plan, including the choice of dependence, the management of dependence, dependency update, etc., to ensure the reliability and stability of dependence. |
| Quality risk | Develop detailed test plans and test cases to ensure the quality of the software | Establish a quality control mechanism to monitor and manage the quality in the software development process | Establish a quality management plan, define the quality objectives and quality standards, and formulate the corresponding quality control measures and quality assurance measures. |
| Data leakage | Encrypted storage and transmission of sensitive data to ensure the security of the data.  Establish an access control mechanism to limit and control the access to the data. | Establish a data monitoring mechanism to monitor and record the access and use of data. | Establish a data security management plan, clarify the data security goals and standards, and formulate the corresponding data security control measures and data security safeguard measures. |
| network attack | Conduct regular vulnerability scanning and security assessment of the system, timely repair of vulnerabilities and strengthen security measures. | Conduct regular safety audit and safety assessment to find and solve safety problems in time | Formulate emergency plans and vulnerability repair plans to ensure that they can be timely addressed and solved when security problems occur. |
| malicious software | Install anti-virus software, firewall and other security software, timely upgrade and update, to ensure that it can timely detect and clear malicious software. | Regular anti-virus scanning and security inspection of the system, timely detect and remove malicious software. | Develop contingency plans and malware removal plans to ensure that security issues can be addressed in time. |
| Code injection | Use secure programming languages and frameworks to avoid using known vulnerabilities and insecure functions.  When writing code, avoid the way of dynamic code execution, such as eval () function | Monitor system logs and abnormal events, and find and handle abnormal requests and operations in time. | Regular security vulnerability scanning and security test on the system to find and fix vulnerabilities in time. |
| privacy leak | Take access control measures to limit access to sensitive information and ensure that only authorized persons have access. | Monitor system logs and abnormal events, and find and handle abnormal requests and operations in time. | Formulate privacy protection policies and privacy protection measures to ensure the security and confidentiality of sensitive personal information. |
| data security | Take data backup, access control, etc | Establish a monitoring mechanism to monitor the data storage, transmission and processing processes, and find and handle abnormal situations in time. | Establish a risk management mechanism for the comprehensive management and control of data security risks |
| Liability and exemption clause | Establish clear responsibilities and liability clauses to clarify the rights and obligations between developers and users | Establish a monitoring mechanism, monitor the developed products, timely find out the problems reported by users, and timely deal with and solve them. | Establish a risk management mechanism, and conduct a comprehensive management and control of the products |
| Demand change risk | Establish a clear demand change management mechanism, including the process of demand change, change application review and approval mechanism, etc., to ensure the rationality and feasibility of the demand change | Establish a demand change tracking mechanism, find and handle the demand change in time, and avoid the problems such as project delay caused by the demand change | Establish a risk management mechanism for the comprehensive management and control of demand changes |
| Poor risk of communication | Establish clear communication channels: ensure that team members can communicate and communicate smoothly, and establish a transparent, open and positive communication atmosphere.  Develop a clear communication plan: clarify the communication style, content and frequency of each stage, to ensure that everyone understands the communication plan, and can communicate according to the plan. | Evaluation the communication effect regularly, understand whether the communication achieves the expected effect, and timely find and correct the problems of bad communication. | Develop management plans for poor communication risks to ensure that poor communication risks are addressed in a timely and effective manner. |
| Schedule delay | Make a detailed project plan, including work content, workload, work time, work order, to ensure that everyone understands the project plan and can work according to the plan. | Monitor the progress implementation: to monitor and track the project progress regularly, find the progress deviation and problems in time, and take measures to adjust and correct them in time. | Develop a progress delay risk management plan to ensure the timely and effective response to the risk of progress delay. |

### 4． Summary

Risk planning is a key project management tool designed to help project teams identify, assess, and manage potential risks. By implementing the risk plan, the team can better control the project risk and ensure the project. In the risk plan, the team will first identify the risks that may affect the success of the project. These risks may include code errors, compatibility issues, security vulnerabilities, and data quality issues. The team will then assess these risks to determine the likelihood and extent of their impact. Next, the team will take appropriate risk management measures, including risk mitigation, risk monitoring, and risk management. The team will also communicate risk information with project stakeholders and stakeholders to ensure they understand the risk and are able to participate in risk management. Finally, the team will regularly update the risk plan and adjust to the project progress and new risks. By implementing the risk plan, the team can better manage and control the project risk, thus maximizing the successful completion of the project.