

**Project Title - Distributed Computing for E-Post Office**

**Project Phase - Risk Impact and Analysis Document**

**Course Name - Software Engineering**

**Course Code - CSE1005**

**Lab Slot - L37-L38**

**Group Members:**

**1. Raghu Kiran R – 21BCE7706**

**2. Ramith Yadav S – 21BCE7731**

**3. P. Pavan Kumar Reddy – 21BCE7118**

**4. Dumpa Deva Harsha – 21BCE8911**

**5. K. Sai Akhil – 21BCE7353**

**Risk Impacts and Analysis Table for E Post Office**

**Risk Impact Table:**

|  |  |  |
| --- | --- | --- |
| **S.no** | **Functional Requirements** | **Risk Impact** |
| 1. | User Management | High |
| 2. | Compliance management | Low |
| 3. | Integration Management | High |
| 4. | Operation and Performance | Medium |
| 5. | Technical management | High |
| 6. | Security Management | High |

**Analysis:**

**1. User Management:** Risk Impact will be High.

**Risks involved:**

1. Unauthorized access to the user account (data breach) thus compromising sensitive information to unauthorised individuals.

2. Loss of user data (personal information).

**Solutions:**

1. Unauthorized access to the user account (data breach): Implementation of Multifactor Authentication or two step verification.

2. Loss of user data (personal information): Implement data encryption, backup user data regularly and establish access controls and user permissions.

3. Have roles and authentications specified like the admin has the power to login and view, delete or update info in the database, etc..,

**2. Compliance Management:** Risk Impact will be Low.

Risks involved:

1. Violation of data protection regulations are any stage causing customer dissatisfaction.

2. Violation of any of terms mentioned in SLA (Service Level Agreement) with the customer.

Solutions:

1. Regularly audit/ review to ensure regulatory requirements are met.

2. Keep note of the terms and conditions agreed upon as per the SLA and ensure the software meets the agreed standards or protocols.

**3. Integration Management:** Risk Impact will be High.

Risks Involved:

1. Inaccurate details/ Data corruption impacting the reliability.

2. Increased Downtime due to no proper backup mechanism.

Solutions:

1. Implementing data redundancy to store important data in more than one location so as to recover it easily in case of downtime or failure.

2. Implementing data validation to ensure accuracy of data before processing.

**4. Operation and Performance Management:** Risk Impact will be Medium.

Risk Involved:

1. Hard for user to understand the environment i.e.., not being user friendly.

2. No proper documentation thus leading to

Solutions:

1. Provide user training session to make them familiar with the software and make available a technical support to reach out to them in case they face any difficulty.

2. Develop and maintain a detailed documentation right from the start of the software implementation so as to fix any troubles and functionality failures quickly.

**5. Technical Management:** Risk Impact will be High.

Risks Involved:

1. Not compatible on certain software’s like able to execute hassle free on one software and not able to execute well on some other software.

2. Slow response time can not be tolerated by the customer thus making their reliability on software dent.

3. Software errors and bugs due to minor errors in code.

Solutions:

1. Assessing and quickly changing so as to develop a compatible software.

2. Reaching optimised stage in every cycle of development to ensure capacity planning and smoother performance.

3. Regularly test the software to identify errors / bugs and fix them quickly by taking guide of the documentation and understanding what went wrong.

**6. Security Management:** Risk Impact will be High.

Risks Involved:

1. Software service interruptions caused due to external factors.

2. Loss of customer trust in case of cyber attacks or security breaches as E Post Office deals with personal information.

Solutions:

1. Implementing strict access controls like multifactor authentication.

2. Encrypting sensitive data stored in the database.

3. Keeping the application up to date with the latest software by conducting regular security audits.