RISK CHECK LIST

◾ Product size (PS) — risks associated with the overall size of the software to be built or modified

◾ Business impact (BU) — risks associated with constraints imposed by management or the marketplace

◾ Customer characteristics (CU) — risks associated with the sophistication of the customer and the

developer's ability to communicate with the customer in a timely manner

◾ Process definition (PR) — risks associated with the degree to which the software process has been

defined and is followed by the development organization

◾ Development environment (DE) — risks associated with the availability and quality of the tools to be

used to build the product [resource allocation plan]

◾ Technology to be built (TE) — risks associated with the complexity of the system to be built and the

"newness" of the technology that is packaged by the system

◾ Staff size and experience (ST) — risks associated with the overall technical and project experience of

the software engineers who will do the work

**Risk Table - Online Hospital Management and Service Booking System**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Risks** | **Category** | **Probability** | **Impact** | **RMMM** |
| **System complexity may be significantly high** | **PS** | **60%** | **3** | **Build incrementally, modular design** |
| **Database design will be complex** | **PS** | **50%** | **3** | **Use proven patterns, test early** |
| **Healthcare regulations not followed** | **BU** | **70%** | **4** | **Legal consultation, encrypt data** |
| **Hospital partnerships will fail** | **BU** | **60%** | **3** | **flexible APIs** |
| **End-users resist system adoption** | **CU** | **50%** | **2** | **Simple interface, local language support** |
| **Payment integration will fail** | **TE** | **40%** | **3** | **Multiple gateways, test thoroughly** |
| **Real-time features won't work** | **TE** | **30%** | **2** | **Use reliable technology, load testing** |
| **Team lacks healthcare knowledge** | **ST** | **70%** | **3** | **Hire domain expert, train team** |
| **Staff size insufficient for scope** | **ST** | **50%** | **3** | **Plan resources, consider outsourcing** |
| **Security vulnerabilities will exist** | **DE** | **60%** | **4** | **Encryption, access control, audit logs** |
| **Home service delivery will fail** | **Operational** | **60%** | **2** | **Partner with logistics, GPS tracking** |
| **System downtime during emergencies** | **Operational** | **40%** | **4** | **Backup servers, 24/7 monitoring** |

**Impact Values:**

* **1 — negligible**
* **2 — marginal**
* **3 — critical**
* **4 — catastrophic**

***The work product is called a Risk Mitigation, Monitoring, and Management Plan (RMMM)***