# AI-Powered Chatbot Development for Customer Support Automation

Risk management is a structured approach to identifying, assessing, and responding to potential threats and opportunities that may affect the AI-Powered Chatbot for Customer Support Automation project. This project involves building, training, and deploying an AI chatbot integrated with multiple platforms which can introduce technical, security, and regulatory risks. Proactive risk management ensures the chatbot is reliable, secure, and compliant with industry standards.

**Risk Assessment and Management Plan**

**Risk Identification Methods**

• Brainstorming with developers, security teams, and business stakeholders to identify chatbot-specific risks.  
• SWOT Analysis to assess internal and external factors affecting the chatbot deployment phase.  
• Historical data review from similar AI projects to predict common integration failures or performance risks.

**SWOT Summary – Chatbot Project**

|  |  |
| --- | --- |
| **Strengths**  • Skilled development and AI team • Strong IT infrastructure | **Weaknesses**  • Limited prior experience in chatbot fine-tuning • Limited language training data for all use cases |
| **Opportunities**  • Automation of customer support 24/7 • Integration with multiple platforms | **Threats**  • Data privacy breaches / hallucinations • Regulatory non-compliance (e.g., GDPR/Privacy Act) |

**Risk Register (Qualitative)**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Risk ID | Risk Description | Category | Source | Probability | Impact | Priority |
| R1 | Chatbot provides inaccurate or hallucinated answers | AI Quality | Poor prompt design / insufficient training | High | High | Critical |
| R2 | Leakage of personal data through chatbot logs | Security | Unmasked PII or weak access controls | High | High | Critical |
| R3 | Integration failures with CRM/ticketing system | Technical | API mismatch or downtime | Medium | High | High |
| R4 | Model bias or offensive content | Ethical | Unbalanced training data | Medium | High | High |
| R5 | High latency or service downtime | Infrastructure | Overload or hosting issues | Medium | Medium | Medium |
| R6 | Vendor API cost spikes | Financial | Increased usage or limits | Medium | Medium | Medium |
| R7 | Regulatory changes or non-compliance | Regulatory | Privacy regulations updates | Low | High | Medium |
| R8 | Knowledge base not updated | Operational | Manual updates missed | Medium | Medium | Medium |

## Quantitative Risk Analysis

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Risk ID | Probability | Impact | Risk Score | Rating |
| R1 | 5 | 5 | 25 | Extreme |
| R2 | 5 | 5 | 25 | Extreme |
| R3 | 4 | 4 | 16 | High |
| R4 | 3 | 4 | 12 | High |
| R5 | 3 | 3 | 9 | Medium |
| R6 | 3 | 3 | 9 | Medium |
| R7 | 2 | 4 | 8 | Medium |
| R8 | 3 | 3 | 9 | Medium |

## Risk Response Plan

|  |  |  |
| --- | --- | --- |
| Risk ID | Strategy | Mitigation Actions |
| R1 | Mitigate | Use prompt evaluation pipeline, add grounding knowledge base, apply guardrails and fallback replies |
| R2 | Avoid | Mask PII in logs, DLP checks, encryption, RBAC, audit trail |
| R3 | Mitigate | Use pre-production testing, failover API routing, retry mechanisms |
| R4 | Mitigate | Bias testing, diverse training dataset, implement refusal policies |
| R5 | Transfer | Use cloud autoscaling, CDNs, and SLAs with hosting provider |
| R6 | Accept | Monitor usage, implement caching and prompt optimization |
| R7 | Mitigate | Compliance checks, legal reviews, configuration changes as required |
| R8 | Mitigate | Automate KB sync; assign clear update owners |

**Risk Monitoring and Control**

• Maintain Risk Register throughout development and operations.  
• Weekly project meetings to review risk status and mitigation effectiveness.  
• Configure alerts for major events.  
• Use tools like Microsoft Project or Jira to link risks to tasks and deadlines.  
• Critical and High risks must be resolved or accepted before Go-Live.

**Change Request Management Process**

# Workflow

1. Submit CR – Stakeholder or team member submits a change request.

2. Log & Screen – Change Manager logs and screens for completeness.

3. Impact Analysis – Assess effect on cost, schedule, resources, risks.

4. Recommendation – Approve, Defer, Reject, or request clarification.

5. Approval – PM or CCB (Change Control Board) approves high-impact CRs.

6. Implementation – Update project plan, risk register, and schedule.

7. Verify & Close – Confirm deployment and communicate to stakeholders.

**Sample Change Log**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| CR ID | Title | Impact (S/C/$) | Decision | Dependencies | Owner | Status |
| CR-07 | Add Sinhala Language | High / Cost↑ / Time↑ | Approved | UAT → Launch | Tech Lead | In Build |
| CR-09 | WhatsApp Channel Integration | High / Time↑ | Deferred | Post Go-Live Phase | PM | Deferred |
| CR-11 | Add GDPR Logging | Medium / Cost↑ | Approved | API Config →Legal Review | Security | Approved |