Risk Assessment Business Logic Document

1 Overview

The risk assessment module is a core component of the application, designed to allow users to evaluate risks associated with various processes or systems. It supports manual data entry and an embedded calculation mechanism for determining risk values.

2 Functional Requirements

2.1 User Authentication and Roles

2.1.1 Login Mechanism

Users can authenticate using:

- Email
  Password-based authentication.
- Two-Factor Authentication (2FA) with options:
  - SMS
  - Email
  - Authenticator App

2.1.2 User Roles

- **Standard User**: Can browse and enter risk data.
- **Owner (Admin)**: Has extended permissions for data management.

2.2 Risk Data Entry

Users access the risk assessment tool by selecting a relevant tile from the dashboard. The system allows manual entry of:

- Risk Name
- Threat Name
- Likelihood (L)
- Impact (I)

A predefined calculation mechanism will compute a Risk Score based on the formula:

$$Risk\ Score = f(L, I) \tag{1}$$

This formula is derived from the methodology provided in the Excel sheet. Users can edit previously entered risk entries. Data is stored in a database for future reference.

2.3 Risk Calculation Methodology

The risk assessment calculation follows a methodology extracted from the uploaded Excel document:

- Users enter Likelihood (L) and Impact (I) values manually.
- The system computes and displays the Risk Score automatically.

Risk categories based on the computed score:

- Low Risk: 1–3
- Medium Risk: 4–7
- High Risk: 8–10

2.4 Importing Risk Data

Users should be able to upload risk assessment data from structured files (e.g., Excel, CSV).

- One tab will include a predefined methodology for calculations (derived from the provided Excel file).
- The import feature ensures that risk values are validated before being stored.

3 Security Requirements

3.1 Database Protection

- The database must prevent unauthorized copying or downloading of data.
- Only authorized users can enter, edit, or export data.
- Recommended database: PostgreSQL or MySQL (avoiding Oracle Enterprise due to cost constraints).

3.2 Application Security Testing

- The application must pass a security scan performed using an automated vulnerability scanner.
- Security best practices, including encryption and secure authentication mechanisms, should be enforced.

4 Deployment and Environment

The system should be deployable both on-premises and in public cloud environments (e.g., Azure). It must support seamless data migration between environments.

5 UI Sketch

A UI wireframe will be designed to ensure that stakeholders approve the interface before development begins. The main dashboard will consist of 22 micro-modules (tabs/pages):

- Each tab will focus on a different risk-related function.
- One specific tab will handle risk score calculation, with simple input fields for manual entry.
- Another tab will provide a dictionary of definitions for reference.
- The UI will include an import option for structured risk data.