RiskED User Guide

1. Overview

The RiskED – Cyber Risk Identification & Assessment Tool is a proof of concept (PoC) designed to demonstrate risk modelling concepts without requiring complex installations or technical expertise. The tool provides a left-shift methodology for understanding your system, offering an intuitive interface for entering key parameters and generating actionable risk insights. Although built for complex systems such as Industrial Control Systems (ICS), Oil & Gas, Manufacturing, and Transportation, it can also model less complex subsystems.

2. What the Tool Does

• Build System Model: Constructs a dependency model based on user-supplied dependency information and the probability of each leaf node.

• Risk Assessment: Calculates risk scores from user-provided inputs.

• Scenario Analysis: Allows users to explore different risk scenarios by adjusting parameters.

• Visualisation: Displays results in easy-to-understand graphs, charts, and tables.

• Export Options: Enables downloading of results for further analysis.

3. Module Description

Following the alphabetical sequence in the left sidebar, you will provide the following information:

(A) Cyber Risk Profile: Collects your responses to 15 cybersecurity risk profile statements, analyses them to generate category-based risk coefficients, and displays a summary of your cyber risk profile.

(B) Cyber Risk Profile Report: Depends on the information provided in (A). Generates a comprehensive cybersecurity risk profile report using your responses mapped to industry standards, analysed via the API key you provided. Outputs are available as downloadable Word documents.

(C) Model Mapping: The most critical part of the tool. Lets users build, edit, and visualise a system dependency model as a directed graph—allowing the definition of nodes and dependencies, assignment of probabilities to leaf nodes, and the ability to download the resulting model as a PNG image. The PoC is limited to 15 nodes.

(D) Model Analysis: Depends on the information provided in (A) and (C). Performs statistical analysis by building a Bayesian Network from system dependency data, conducting probabilistic inference and sensitivity analysis (both single-node and multi-node), computing posterior probabilities for each node, and visualising how changes in components affect overall system risk. Results are saved for further reporting.

(E) Risk Analysis Reports: Depends on the outcomes of (D). Generates a comprehensive Cyber Risk and Resiliency Report for the system under analysis by sending the results of prior sensitivity and Bayesian analysis to an external AI model. Displays and allows download of a formatted report tailored for senior leadership, including an executive summary, risk analysis, sensitivity outcomes, and actionable recommendations.

4. Prerequisite

API Key: This PoC relies on the Llama3 LLM (open source) to interpret the results of the analytics performed by RiskED. You will need a free API key to use the demo.

To obtain a free key:

1. Navigate to https://console.groq.com/login and sign up.

2. Once signed in, go to the API Keys page from the left-side navigation panel.

3. Click 'Create API Key' and give it a name.

4. Click 'Submit'.

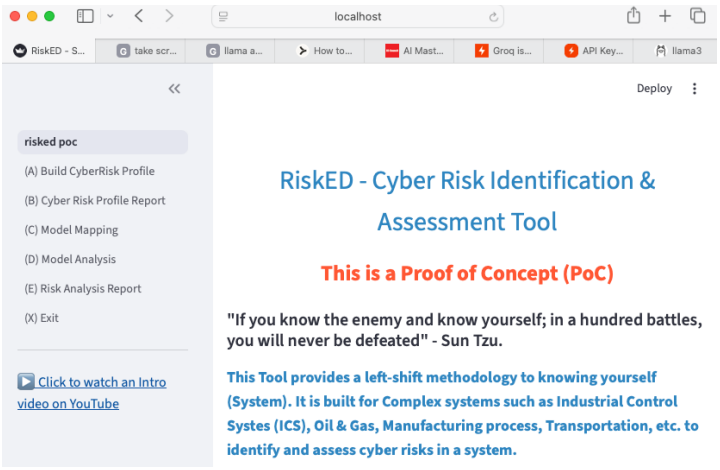
5. Copy the generated key to your clipboard or a document and save it for future use.

5. How to Use the Application

Step 1: Access the App

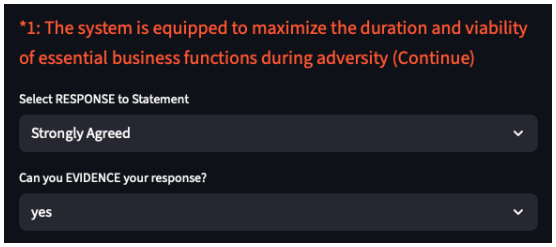
Open the app in your browser: https://risked-poc.streamlit.app/ . No installation is required; the app runs entirely online.

Your landing page will look like this:

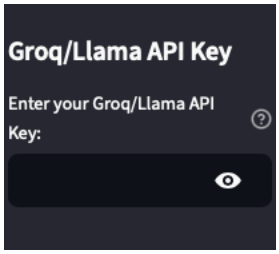


Step 2: Provide Information (Data)

Module (A): Provide responses to cyber risk statements from a drop-down menu, as shown below:



Module (B): To generate this report, copy and paste your Groq/Llama API key into the space provided and press Enter. The module will not run if an invalid API key is provided.



Module (C): The input process is as follows:

• Root Node Selection: Select a root node (e.g., 'People', 'Technology', 'Process') from a dropdown list. This list includes default nodes and any previously added nodes that can act as parents.

• Child Node Input: Enter the name of the child node in the text input field. Each child node must have a unique name.

• Dependants Selection: Specify whether the child node has dependants using a radio button ('Yes' or 'No'). 'Yes' means the node is an internal node; 'No' means it is a leaf node.

• Probability Assignment: Probability is only assigned to leaf nodes. Use a slider to set a probability value between 0.00 and 1.00.

• Saving and Editing: When you submit the form, the node is added to the model and saved in a CSV file. You can also edit or delete nodes (except for protected default nodes).

Example Workflow:

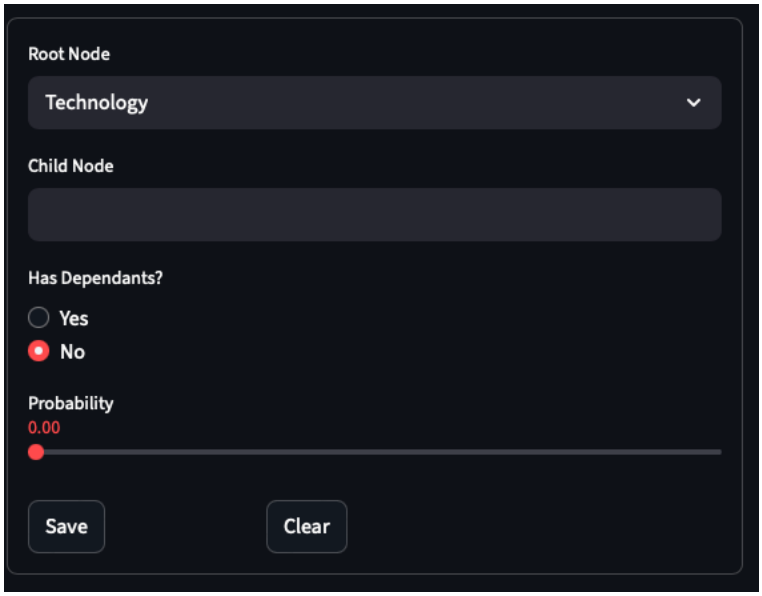
1. Select Root Node: 'Technology'

2. Enter Child Node: 'Firewall'

3. Has Dependants? 'No'

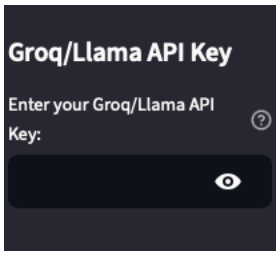
4. Set Probability: 0.85

5. Save: The relationship 'Technology → Firewall' with probability 0.85 is added.



Module (D): This module runs automatically as soon as it is selected; no user input is required.

Module (E): To generate this report, copy and paste your Groq/Llama API key into the space provided and press Enter. The module will not run if an invalid API key is provided.



6. Outputs You Will See

• **Risk Score Summary:** A table showing calculated risk scores for each factor.

• **Scenario Comparison**: If multiple scenarios are entered, the app compares them side by side.

• **Downloadable Report**: Export results as a PNG (the model tree) or DOC (reports) for offline use.

7. Key Features

• **Interactive Controls**: Adjust sliders and dropdowns to refine your analysis.

• **Real-Time Updates:** Charts and tables refresh dynamically as you change inputs.

• **User-Friendly Design**: Clear navigation and responsive layout for desktop and mobile.

• Data is not stored in this tool.

8. Support

For questions or feedback, please contact the development team at info@crsmethods.com