

# Functional Specification:

**Risk Assessment Tool That Calculates The Type, Cost And Likelihood of Breaches.**

Institute of Technology Carlow

Department of Computing & Networking

Student Name: Eimhin Lane

Student Number: C00240680

## Table of Contents:

- Introduction: ..... 2
- 1. Application Overview: ..... 2
  - 1.1 Application Purpose – ..... 2
  - 1.2 Project Goals – ..... 2
- 2. Application Target Group:..... 2
  - 2.1 Organisations – ..... 2
- 3. Use Diagrams: ..... 3
  - 3.1 Tool Map – ..... 3
- 4. FURPS:..... 3
  - 4.1 Functionality – ..... 4
  - 4.2 Usability – ..... 4
  - 4.3 Reliability – ..... 4
  - 4.4 Performance – ..... 4
  - 4.5 Supportability – ..... 4
- 5. Design Diagrams: ..... 4
  - 5.1 Dashboard Function – ..... 4
  - 5.2 Assessment Information – ..... 5
  - 5.3 Assessment Results – ..... 5
  - 5.4 Creating a New Session – ..... 6
  - 5.5 Upload/Download Sessions – ..... 6
  - 5.6 Information Screen – ..... 7
  - 5.6 Dashboard Interface Blueprint – ..... 8
- 6. Identifying Key Aspects: ..... 8
  - 6.1 The Threats – ..... 8
  - 6.2 The Cost – ..... 9
  - 6.3 The Likelihood – ..... 9
- 7. Machine Learning ..... 9
  - 7.1 Supervised Learning Regression – ..... 9
  - 7.2 Decision Trees – ..... 10
- 8. Programming Languages..... 10
  - 8.1 Python– ..... 10
  - 8.2 Visual Basic– ..... 10

## Introduction:

This functional specification will provide a breakdown on the design philosophy of the tool alongside a detailed description on key aspects of the tool including its primary purpose, user group and how the tool will function. Descriptions on how this risk assessment tool will perform the tasks necessary for satisfactory results are vital to defining a working program that meets an expected level of quality.

## 1. Application Overview:

### 1.1 Application Purpose –

This application is to be a Quantitative Risk Assessment tool, these are tools used by companies in various industries to help identify weaknesses in their systems and possible threats that could capitalise on them. This particular tool will be aimed at cyber security issues, offering an easy-to-use alternative to spreadsheet approaches and their various limitations. Many tools exist, most of which are developed internally by companies, but others are purpose built to be openly available to anyone who needs the tool.

### 1.2 Project Goals –

This specific tool will quantify the potential cost, the type and the likelihood of a breach. The cost of a breach will be defined as financial loss and asset loss that a company will endure during the breach. The type of attack will be described and a common method of preventing of the threat will be provided. The likelihood will be described in two different ways firstly in a percentage based on inputted information and secondly in the method described in Section 1.1 of the Research Report, where in it is ranked as no threat, minimum threat, and maximum threat.

The project will ultimately provide a well-rounded description of what is wrong with your system and how to fix it in a simple and efficient manner for those that may not understand the more technically inclined side of their services. Through this ease of use it may encourage a deeper investment in cyber security from the company who use it.

## 2. Application Target Group:

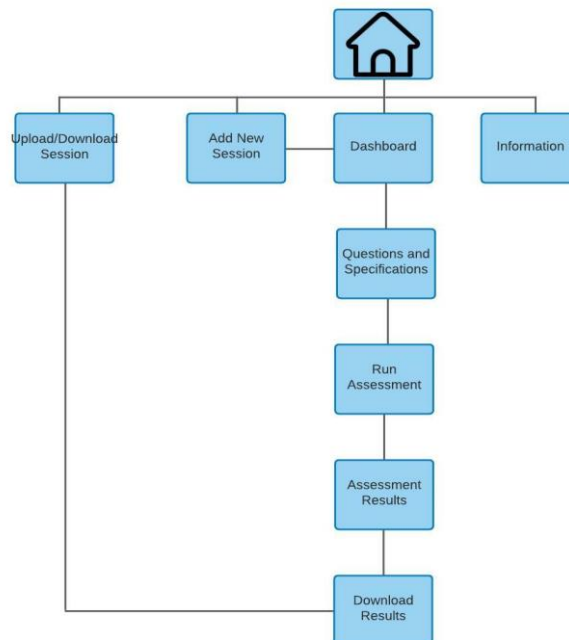
### 2.1 Organisations –

The primary group that this tool is designed with in mind is companies who wish to invest further in their cybersecurity. The tool should be effective no matter the size of an organisation, whether they are large scale organisation or a small start-up the tool will adapt based off the information they

provide. These organisations may not be able to research or create their own tool and as such this project is intended to provide this functionality to them. This tool will bring awareness to the various threats that they face and should encourage a greater understanding of cybersecurity within these corporations.

### 3. Use Diagrams:

#### 3.1 Tool Map –



### 4. FURPS:

FURPS is a model, designed by Robert Grady, that provides a context to the requirements of a project. These requirements can be both functional and non-functional. FURPS is an acronym of the various headings that make it up, these being;

- Functionality
- Usability
- Reliability
- Performance
- Supportability

Judging a system on these headings can help in classifying the software's attributes and is widely used in the software industry. There is an additional section of FURPS which is referred to as FURPS+ that is used to emphasize multiple attributes.

#### 4.1 Functionality –

Functionality of the assessment tool is described in greater detail in Section 5.

#### 4.2 Usability –

The average user should be guided along the usage of the tool through key buttons and visually that will be familiar to them through other established software, such as home buttons, run buttons, text prompts and more. The user should not require an in-depth knowledge of their technologies just of their purpose for answering the assessments questions.

#### 4.3 Reliability –

The system should maintain functionality in the event of unentered information adapting to the information that has been answered to still provide necessary results.

#### 4.4 Performance –

The tool should be responsive loading in as little time as possible. When performing tasks that may take extended periods of time such as running the assessment, we can inform the user through a processing icon.

#### 4.5 Supportability –

Utilising the docx format in Microsoft word we can upload and download assessments with little issue. Doing so in program will help mitigate time taken to communicate with cloudmersive for the assessment files.

## 5. Design Diagrams:

### 5.1 Dashboard Function –

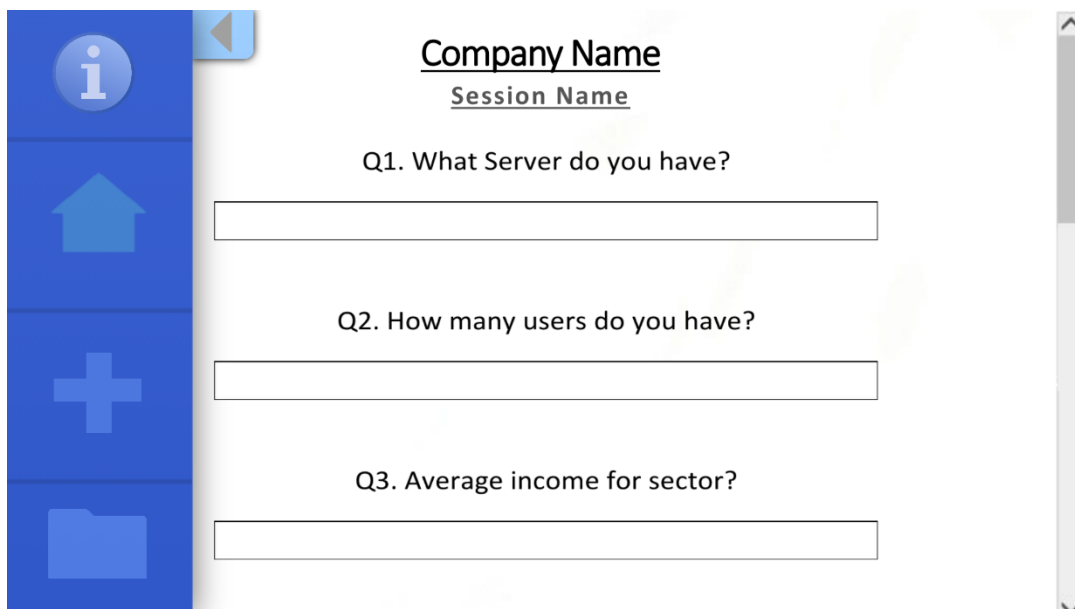
Upon starting up you will be brought to a dashboard; this will effectively act as our hub for all the functionalities the tool provides. From here you can select a variety of options, an information button for a description on how to use the tool, a home button to return to the dashboard, a new session button to start a new assessment and an upload/download button to save your current

assessment or upload a previous one. This side-bar menu will be collapsible if you wish to see the centre of the dashboard more prominently.

## 5.2 Assessment Information –

Much of your activity will take place in the central portion of the dashboard which is where all current assessment information is entered. At the top of the screen, you will be able to put the company name and session name. By default, the company and session name will be titled “Company Name” and “Session Name” to let the user know what the two fields are. The names entered will be used to automatically generate a file name when saving the session.

Beneath the name you will be asked a variety of questions where in you will enter the proper information for your organisation. These questions are used to determine the various assessment criteria of likelihood, breach type and cost. Financial questions and user questions are used to decide which areas are at most threat to be attacked for their value of information or monetary gain. Technical questions will be used in determining the type of attacks you are likely to endure and how to solve them. When satisfied you can hit the run assessment button to get your results.



**Company Name**  
**Session Name**

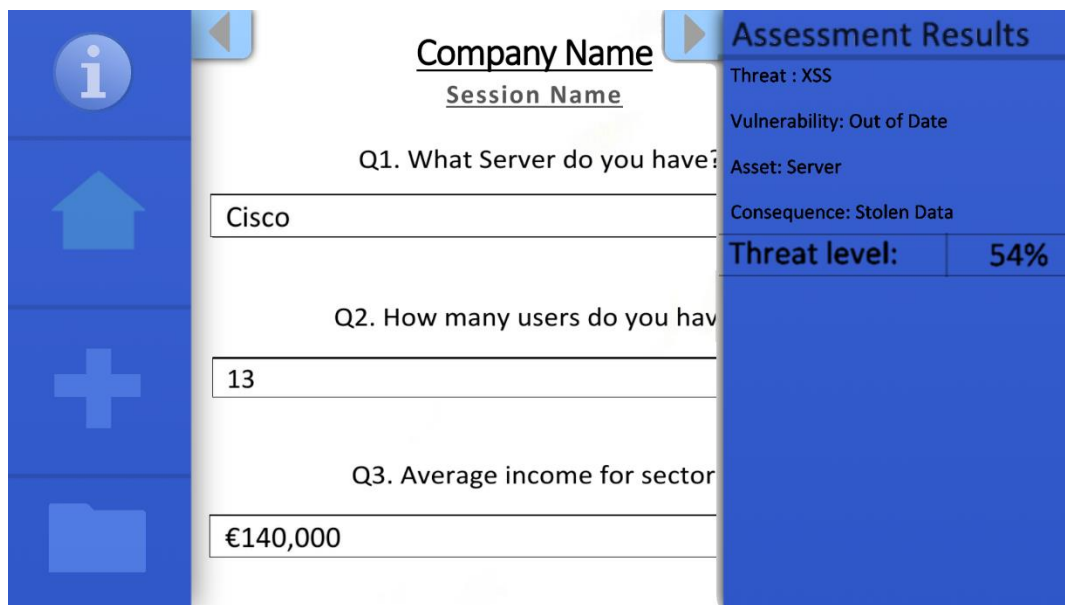
Q1. What Server do you have?

Q2. How many users do you have?

Q3. Average income for sector?

## 5.3 Assessment Results –

Upon hitting the run assessment button, you will be provided the assessment results on a new toolbar which will come in on the right side of the screen as opposed to the menu on the left. This menu is divided up amongst the various threats, likelihood, assets and consequence of a breach. The assessment will be listed in descending order starting with the most likely attacks and running down the list. At the bottom of this menu is a section to change the generated file name if you are to save the assessment results.

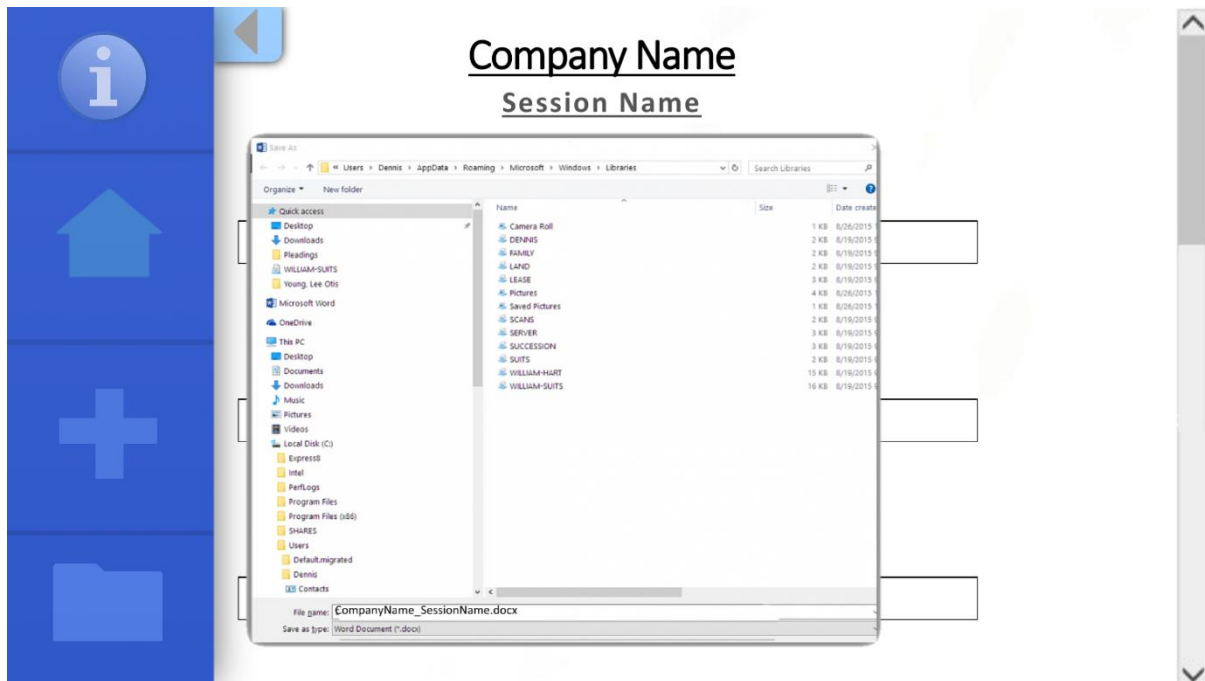


#### 5.4 Creating a New Session –

Upon hitting the new session button, you will be brought to a fresh screen without the dashboard information of whatever other session you had open. This allows you to work on multiple sessions at a time, or simply restart from scratch if you feel the information entered previously wasn't descriptive enough or accurate. From the bottom of the central screen, you can change between active sessions.

#### 5.5 Upload/Download Sessions –

If you wish to download a session you can save an in-progress session from the dashboard on the left or after running the assessment save a finished session including the assessment results. If you wish to resume progress or change information on a previous session that is no longer open, you can upload it if you have it saved to your device and resume from where you left off.



## 5.6 Information Screen –

When selecting the information screen, you will be provided a tutorial on the functions of the tool, describing the purpose of the tools various buttons, how to run an assessment and describing how the assessment results are formatted. If you wish to return to the dashboard you need to press the home button from there you can return to work on your assessment details from before. While the information screen is a non-core feature it can be extremely useful for those who need the help.

i

↑

+

📁

### System Information

**Description:**

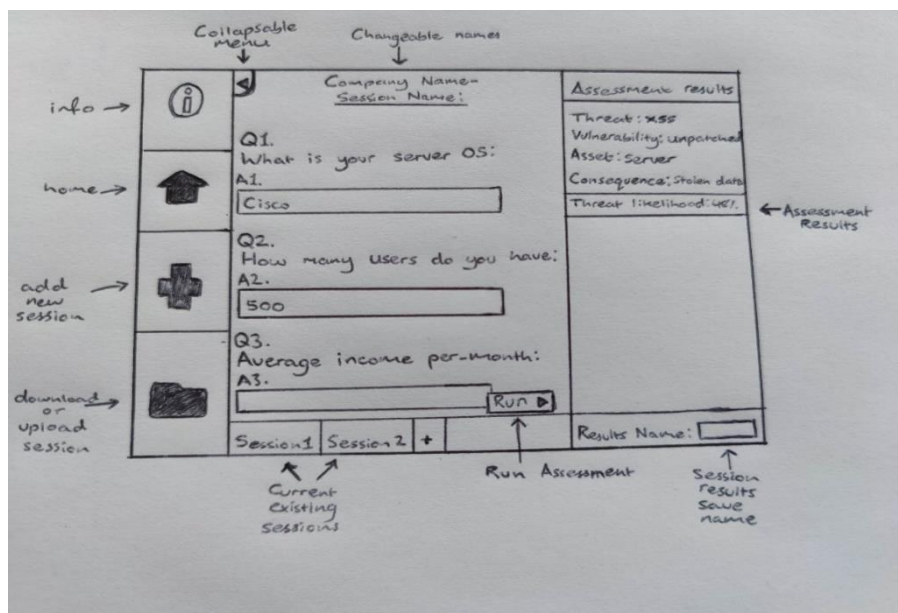
The purpose of this system is to offer an accessible and precise Risk Assessment for those need one. It is capable of rooting out any possible threats to security and confidentiality of your data. With this program you will be offered up solutions or descriptions on the various problems that may plague your system.

**Guide:**

Upon starting the program you will be prompted to enter your company name and be brought to the homescreen. After entering this name/company you will be brought to the homescreen with an empty assessment session. You can edit the name of the



### 5.6 Dashboard Interface Blueprint –



## 6. Identifying Key Aspects:

When the user enters information to run through an assessment it is important to understand what to do with that information. The tool will notify these key aspects in the information, and they are what are used to generate assessment results. These key aspects are known as the threat, the cost and the likelihood. This process needs to be automated efficiently in order to run a thorough assessment with as little down time as possible, as to not deter the users.

### 6.1 The Threats –

Maintaining a database of the various vulnerabilities and when a threat actor will utilise them is integral in the assessment process. We can identify what threat is usable based on information entered for hardware and software, such as if they are up to date. We can effectively use this style of cross-referencing information to identify what threats are capable of being used on the organisation.

## 6.2 The Cost –

Cost is calculated based on the amount of users, information or money being made and stored in software for an organisation. If this software is breached, we can determine if it is more costly than other areas based on the abundance assets stored on it.

## 6.3 The Likelihood –

Much the same as cost the asset quantity of certain areas will paint a larger target on its back, using the inputted information we will know if it is more likely for one part of the organisations set-up to be targeted than others.

# 7. Machine Learning

The process of determining what the likelihood of a breach is can be calculated via machine learning techniques. Machine learning can help when dealing with an immense amount of data that cannot be handled through conditional statements and loops without slowing down the program considerably. Analysing this data and making decisions based off that data is mostly handled by machine learning algorithms if handled properly.

Of the three primary forms of machine learning, supervised, unsupervised and reinforcement learning, I will be working with supervised learning. Supervised learning is further broken down into further tasks, the two most common being classification for predicting discrete values and regression for predicting a continuous response variable. Through this description it seems fit to utilise regression over classification when determining the likelihood of breaches in the risk assessment process.

## 7.1 Supervised Learning Regression –

As stated a supervised learning regression system is used to predict the value of a continuous response variable. Examples of regression problems include predicting the sales for new product, or the salary of a job based on the description. Regression can be further broken down into either a linear regression for determining a continuous dependent variable with any number of possible values or a logistic regression when the outcome only has a limited number of possible values.

It would be most apt to utilise the logistic regression, as the response variable is categorical in nature. Logistic regression is suited to model the chance of an event occurring.

One of the most renowned definitions of risk is that risk ( $R$ ) can be expressed by what can go wrong (scenario  $S$ ), what likelihood it will have (probability  $P$ ), and how severe consequences will be (consequence  $C$ ):

$$R = f(s, p, c)$$

## 7.2 Decision Trees –

Decision trees are non-linear and non-parametric models and are more flexible for capturing data. Often used in machine learning to predict the value of target variables by learning simple decision rules inferred from historical data. These trees are prone to overfitting, larger trees output worse sample predictions.

## 8. Programming Languages

The various aspects of this project influence the choice of programming languages available to work with. For instance, when developing a machine learning program, it is commonplace to develop it in Python. Similarly, Python is used in general development of various tools and websites with it being a versatile programming language, though it is often paired with other languages to achieve its goals such as java.

### 8.1 Python–

This language is a general-purpose option, meaning it can be used to create almost any type of computer program. Its powerful enough for some of the most advanced applications out there, the most important to note is the aforementioned machine learning. Python makes use of frameworks, which can help provide structure to any program or website you are developing.

### 8.2 Visual Basic–

This language is used in Excel to develop the proof of concept for the project idea. It's a relatively easy to learn language that is not used very often outside of office applications. This language is still versatile despite this and allows considerable modification to the otherwise straightforward Microsoft Office Applications.

