National College of Ireland

Automated Cybersecurity Risk Assessment Tool for SMEs

MSc Research Project
Cybersecurity

Neha Swaminathan
Student ID: 23425741

School of Computing
National College of Ireland

Supervisor: Prof. Eric Gyamfi

National College of Ireland
Project Submission Sheet
School of Computing

Student Name:	Neha Swaminathan
Student ID:	23425741
Programme:	Cybersecurity
Year:	2025
Module:	MSc Research Project
Supervisor:	Prof. Eric Gyamfi
Submission Due Date:	11/12/2025
Project Title:	Automated Cybersecurity Risk Assessment Tool for SMEs
Word Count:	7047
Page Count:	29

I hereby certify that the information contained in this (my submission) is information pertaining to research I conducted for this project. All information other than my own contribution will be fully referenced and listed in the relevant bibliography section at the rear of the project.

ALL internet material must be referenced in the bibliography section. Students are required to use the Referencing Standard specified in the report template. To use other author's written or electronic work is illegal (plagiarism) and may result in disciplinary action.

Signature:	
Date:	10th December 2025

PLEASE READ THE FOLLOWING INSTRUCTIONS AND CHECKLIST:

Attach a completed copy of this sheet to each project (including multiple copies).	☐
Attach a Moodle submission receipt of the online project submission, to each project (including multiple copies).	☐
You must ensure that you retain a HARD COPY of the project, both for your own reference and in case a project is lost or mislaid. It is not sufficient to keep a copy on computer.	☐

Assignments that are submitted to the Programme Coordinator office must be placed into the assignment box located outside the office.

Office Use Only	
Signature:	
Date:	
Penalty Applied (if applicable):	

Automated Cybersecurity Risk Assessment Tool for SMEs

Neha Swaminathan
23425741

Abstract

Small and Medium Enterprises (SMEs) make up 99% of European businesses facing cybersecurity risks due to limited resources. 46% of data breaches target SMEs with phishing and ransomware attacks. Risk assessments can strengthen security posture of the company but can be challenging to implement due to complexity of global frameworks such as NIST CSF and ISO 27001 and manual errors. The proposed solution includes the development of an automated open-source risk assessment tool for SMEs with Python, HTML, CSS and MySQL. The tool consists of a 20-question qualitative questionnaire aligned by NIST, OWASP Top 10 and ENISA standards, automating a risk scoring methodology and generating a dynamic risk register with customised mitigation solutions and residual risk calculations. A dashboard is created with visualizations like heat maps and bar charts presenting key security metrics for easy decision-making. The tool was able to achieve 85% of threat coverage along with improvements highlighted in reducing the residual risk enhancing the security posture of the organization, supporting the usability and scalability of applications to SMEs. Limitations include the lack of quantitative or hybrid scoring models. Future work includes incorporation of AI in the tool for real-time monitoring and updated threat databases.
Keywords: Risk Assessment, Risk Register, SME Cybersecurity, Residual Risk, Mitigations, Visualizations, NIST

1 Introduction

1.1 Background

Small and Medium Enterprises (SMEs) are the backbone of today's economy globally and represent around 99% of organizations in Europe specifically employing over 88 million people and contributing to the economic growth (estimated at € 5.4 trillion in 2024). While being critical to businesses worldwide, SMEs are primary targets to cybersecurity threats due to increased vulnerabilities such as technical expertise, security personnel, financial and resource constraints (Katsinis et al.; 2024).
Cyber criminals target these companies for exploitation through gaps in implemented security measures compared to already secure and established systems. As per recent statistics analysing cyber incidents, 46% of data breaches impact small businesses with lesser than 1,000 employees. ENISA (European Union Agency for Cybersecurity) reported that over 90% of European SMEs confirmed that a cyber attack would severely impact their operations. These organizations rely on online services but may not have

strong defences in place against threats like malware and phishing thus leading to most likely face a cyber threat within a year of administration (Rahman et al.; 2024).

Risk Assessment is a systematic process of identifying, prioritising and evaluating risks from potential cyber threats and vulnerabilities in an organization's processes, networks, operations, assets and information systems. The likelihood of occurrence and the potential impact of risk on the business is evaluated determining mitigation solutions (to reduce the risks) through security protocols based on the severity level (Sánchez-García et al.; 2022). For SMEs, risk management is critical in understanding the company's security posture increasing cyber resilience and strategic decision-making while reducing the chances of facing operational disruption, data, financial and reputational loss. Existing cybersecurity frameworks like NIST CSF 2.0 (National Institute of Standards and Technology Cybersecurity Framework) and ISO 31000/27001 (International Standard of Information Security Management) provides extensive guidelines which are more suitable for larger organizations to implement with access to resources. NIST CSF highlights its 6 phases in the risk management process i.e., Govern, Identify, Protect, Detect, Respond and Recover to manage risks, perform active monitoring and prepare incident response plans leaving SMEs to prioritise tasks and use templates based on their business. These frameworks can be complex, expensive and time-consuming leaving SMEs to conduct manual risk assessments which are error prone. Automated GRC tools available in the market provide advanced features such as real-time threat detection, compliance checks with GDPR, NIS2, etc reducing manual efforts. In most cases, many conditions/clauses aren't applied for the risk management process due to limited departments and processes in place leading to inconsistencies in the risk findings El-Hajj and Mirza (2024).

My motivation for the project arises from the disadvantages faced by SMEs having minimal resources in conducting risk assessments and utilising available automated GRC tools. Challenges like scalability and limited threat coverage (focusing on vulnerabilities specific to SMEs) are addressed to make the proposed tool time and cost-effective, user-friendly and easy to understand.

1.2 Research Question (RQ)

Based on the identified gaps and limitations in existing risk management frameworks, the development of an automated risk assessment tool using Python, HTML, CSS and SQLite is explored. The following research question targets key gaps in threat coverage, automation, and scalability:

RQ: **How can a python-based automated cybersecurity risk assessment tool be implemented to integrate a risk register, custom mitigation strategies and a visualization dashboard while addressing gaps in threat coverage, automation and scalability in existing SME frameworks?**

- How can a questionnaire integrated in the risk assessment tool be developed in Python and HTML to identify weaknesses using SME-specific risks from NIST CSF, OWASP Top 10 and ENISA?
- How can qualitative risk-scoring be implemented in Python to calculate the likelihood, impact, severity level and residual risk?

- How can a risk register with custom mitigations be automated to reduce manual errors and improve risk tracking?
- How can a scalable and user-friendly dashboard be created to visualize the risk percentage and security posture for strategic decision-making?

1.3 Research Objectives (RO)

To answer the research question, the below objectives were identified:

- Development of an automated risk assessment tool incorporating a questionnaire with 20 questions for SMEs to identify vulnerabilities specific to the sector, taken from industry standards such as NIST CSF, OWASP Top 10 (Open Worldwide Application Security Project) and ENISA (European Union Agency for Cybersecurity) threat landscapes.
- Design a qualitative risk-scoring methodology to calculate the risk score based on the likelihood and impact by prioritising the risk category and gets the residual risk after mitigation.
- Automation of the risk register and customised mitigation strategies to reduce manual errors and support decision-making and convenient tracking of progress.
- Create a user-friendly and scalable dashboard to visualize the risk posture of the SME ensuring the threat database can be modified.

The tool will be evaluated based on the tool's effectiveness, usability and accuracy through simulated testing while being compared to the time taken to complete a manual risk assessment with the same process.

1.4 Limitations

Qualitative risk scoring can be limitation in the paper due to its subjective nature in the methodology implemented specifically for SMEs relying on the user's inputs. The results can vary when compared to quantitative methods and aren't suitable for larger organizations. The proposed framework also assumes basic digital access and knowledge among users with customisations needed for specific industries like healthcare and finance.

1.5 Summary of Remaining Sections

The report structure is listed below: Section 2 contains the Literature Review summarizing existing research on SME risk management and identifying gaps. Section 3 discusses the Research Methodology and section 4 details the Implementation presenting the proposed solution, tools/languages used and ethical considerations. Section 5 specifies the Design Specifications and section 6 contains the Evaluation covering the results, limitations and evaluation criteria. The paper is then followed by the Conclusion, Discussion and future research.

2 Literature Review

2.1 Challenges faced in SMEs

Small and medium enterprises (SMEs) face many security challenges due to limited resources, lack of technical expertise and increasing threat surfaces. Most companies are ignorant to recent attacks and their vulnerabilities, thus investing lesser into incident management. Ransomware and phishing attacks contribute to a significant number of breaches targeting SMEs, observed from evidence in risk assessments (Alahmari and Duncan; 2021). SMEs in the UK have limited cyber awareness, financial constraints and prioritise their newly administered business, thus investing less in implementing security measures (Rawindaran et al.; 2023). Due to all the listed limitations and the increasing rate of threats causing operational disruption, SMEs prefer utilising automated tools to reduce manual errors through self-assessments (Sánchez-García et al.; 2022). Even with policies in place, many organizations experience regulatory and cultural differences without automated evaluation tools. Saudi Arabia SMEs encountered similar issues as other SMEs i.e., limited employees and financial resources, lack of awareness in security processes when surveyed by non-governmental organizations (Hassan et al.; 2022).

SMEs in the Kumasi metropolis emphasize on risk identification through interviews and discussions, workshops, questionnaires and benchmarking with qualitative risk analysis being crucial (Arthur et al.; 2025). (El-Hajj and Mirza; 2024) utilise quantitative methodologies to analyse remediation from risk analysis responses. Limitations include locations having specific data. SMEs are vulnerable targets facing financial breachers of around 200,000 USD, severe operational disruptions and reputational damage. Common threats are categorized by priority but requires validation by quantitative tools as SMEs are unique with different methodologies and processes. These organizations need customised approaches based on their resources, awareness and competence (Shojaifar and Järvinen; 2021). Risk classification supports a diverse assessment with mitigations that can be customised. SMEs can experience difficulties in complying to regulatory standards like GDPR due to limited resources, thus resulting in the development of a user-friendly risk assessment tool for Irish SMEs (Curtin et al.; 2024).

This section highlights the criticality of evolving threats, rising cyber attacks and the difficulty faced by SMEs to stay updated due to their limitations, leading organizations to rely on manual processes with a slower recovery time.

2.2 Security Frameworks and Standards

NIST Cybersecurity Framework (CSF), ISO 27001, OWASP Top 10 and ENISA Threat Landscape are some of the critically used global standards for guidelines on SME risk management highlighting on information security management system processes (ISMS) and gaps like endpoint security. But these frameworks can be complex to implement for SMEs and are suitable for larger organizations (AL-Dosari and Fetais; 2023). While standards like NIST provide detailed step-by-step guidance for conducting risk assessments, it may not be practical in supporting gaps, testing out with resource and knowledge constraints (Alharbi et al.; 2021). The frameworks can focus on policy implementation without access to GRC applications. ISO 31000 contains details on SME risks simplifying the processes for different SME organizations (Pačaiová et al.; 2018). NIST and ENISA require SMEs to adapt to their methodology posing as a critical challenge among others. GRC frameworks like RUBiQ align with South African standards (King III) and SMEs by analysing

the difficulties faced in the processes, organization and technology (Abdullah; 2019).

2.3 Existing Risk Management Tools for SMEs

SMEs prefer using automated applications like the Cyber Resilience Self-Assessment Tool (CR-SAT) for self-evaluation of their risk management process which could validate and analyse the organization's cyber resilience. Cyber Resilience Operationalization Framework (CR-OF) proposed by (Carías et al.; 2020) which executes resilience regularly by assessing the risk and prioritising remediation. Tools can provide recommendations based on the questionnaires without dynamic scoring for a simple risk assessment. A threat-based approach can integrate real-time monitoring with updates made to the threat database, modified according to the SME prioritising risks. The shared cyber threat intelligence (CTI) can identify and process the risk data and provide recommendations based on the context. Customisation reduces bias and is convenient for SMEs to mitigate threats but increases the reliability on the logic (Van Haastrecht et al.; 2021). While threat incorporation may be a challenge to implement, (Shojaifar and Fricker; 2020) propose CYSEC which is also a self-assessment tool evaluated based on usability, regular user feedback and continuous improvement. This tool can improve the utilisation but doesn't contain automation of mitigation strategies. Risk assessments done manually can differ massively but may lack in threat coverage. An automated tool was created for Irish SMEs analysing existing GRC tools across countries to ensure the form to be user-friendly and inclusive of critical threats (Curtin et al.; 2024). A security risk metamodel proposed by (Ponsard; 2024) that checks secure DevOps, also maps threats based on testing available tools. (Benz and Chatterjee; 2020) proposed a cybersecurity evaluation tool (CET) that utilises a questionnaire based on a NIST survey for self-evaluation with recommendations supporting leadership without dynamic dashboards. A framework created by (El-Hajj and Mirza; 2024) categorizes threats by their criticality in their user-friendly tool for SMEs but requires quantitative validation taken from NIST CSF. (Rahman et al.; 2024) also develops a CET for a self-assessment but lacks in visualizations and customisations. (Sánchez-García et al.; 2022) highlights a limitation with existing tools prioritizing risks but unavailable to provide quantitative feedback for SMEs. This section presents the limitations identified from different proposed frameworks like scalability across organizations, limited threat coverage and lack of real-time monitoring. These applications support decision-making of SMEs depending on the organizations to complete the self-assessments.

2.4 Risk Scoring, Register and Mitigation Strategies

Risk prioritisation was implemented using analytic hierarchy process (AHP) to calculate the score based on the defined criteria and a qualitative comparison analysis to reduce partiality (Igor; 2023). The risk is categorized into hierarchical levels depending on the criticality and complexity. The risk mitigation framework discussed by (Turgay et al.; 2023) covers a detailed step-by-step guide on the different mitigation strategies like accept, avoid, mitigate/terminate and transfer. Remediation solutions are critical to be updated regularly along with threat databases to protect SMEs against evolving cyber attacks. (Rahman et al.; 2024) also discusses the 4 mitigation strategies with progress tracked in the risk register. Risk management frameworks for SMEs researched by (AL-Dosari and Fetais; 2023) contain risk assessments being regularly conducted with mitigation treat-

ment processes. Progress is tracked as part of the risk register like maintaining logs of assets, process and personnel changes, threats and vulnerabilities. Risk management is supported by global guidelines like ISO 27005 which can be complex to implement for SMEs, while NIST covers details on specific phases like risk identification, assessment, response and monitoring. A hybrid approach was implemented by (Sánchez-García et al.; 2022) for SMEs combining NIST and Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE) frameworks for a simple execution with an efficient scoring system and regular logging. IT GRC-based framework developed by (Yu et al.; 2013) integrates aspects for governance policies and strategies, risk management and CSA for compliance against threats like insider attacks. This approach covers critical aspects in risk management but can contain limited information on upcoming threats.

2.5 Visualization and Dashboards

(Rahman et al.; 2024) discusses the importance of dashboards for analysing trends and providing visualizations to present the severity of risks to support SME decision-making. GRC tools like RUBiQ contain visualization aligned with King III standard by analysing the challenges faced in the organization and processes. The tool is evaluated based on the context within the country as part of the governance solution (Abdullah; 2019). The Dynamic Adaptive Symbol System (DASS) improves cyber awareness with visualizations based on the severity of the threat from the risk assessment. The dashboard developed in python has an interactive interface instead of static values for threat detection and filters (Macrino et al.; 2025). A dashboard implemented by NLP processes tweets from X, formerly known as Twitter real-time to classify incidents and visualize the results further. The tweets are categorized between high/normal/no risk and is visualized in the form of bar charts for the number of cyber attacks and data tables for details on tweets. The dashboard was developed in Tableau with geographical visualizations, header panels and filters for the location and attack (Lughbi et al.; 2024). BubbleNet is a dashboard created by (McKenna et al.; 2016) used to identify and summarise security patterns to visualize threats for easy decision-making. With a similar interactive design, the dashboard is used to detect patterns and provides generic feedback rather than a detailed risk assessment. Visualization methods for cyber-physical security review include threat monitoring and risk analysis in the dashboards (Cobilean et al.; 2023). The dashboard contains an interactive heat map and vulnerability trend matrix highlighting the criticality of scalable visualizations in cybersecurity. (Sánchez-García et al.; 2022) analyses the benefits of heat maps in an interactive dashboard that enhances threat monitoring.

2.6 Literature Review Summary

Table 2.6 displays the summary of research done across various sections supporting the proposed methodology and implementation.

Author	**Proposed Solution**	**Limitations**	**Published Date**	**Gaps identified and addressed in research**

(El-Hajj and Mirza; 2024)	Developed a risk assessment framework for SMEs with a user-friendly tool. Common threats are categorised by criticality with NIST and ISO guidelines for the tool.	Requirement of quantitative validation as the tool uses a qualitative analysis.	02/10/2024	Tested with less number of scenarios with a specific industry or region. Critical threats addressed in the tool leaves out other risks that SMEs may face, automated threat detection and updates.
(Sánchez-García et al.; 2022)	Performed a mapping review of 35 risk assessment tools and created a hybrid risk model with the validated variables. Security metrics were identified with each tool being analysed.	Existing tools utilise a qualitative subjective scoring system and adhere to global standards like ISO and NIST preferrable to larger organizations.	28/12/2022	Critical calculations like risk register and residual risks are not implemented with risk scoring done minimally. The proposed model combines both qualitative and quantitative methods but can be complex for SMEs without automations.
(Rahman et al.; 2024)	Developed a detailed risk assessment tool (AssessITS) combining frameworks like NIST, COBIT and ISO 31000. The framework contains procedures, defined evaluation metrics to assign risk values accurately.	Metrics are defined and static causing the tool to be difficult in updating evolving threats and global standards being integrated with a clear context.	02/10/2024	Conditions are static during development without room to modify data. Quantifying risks may be challenging for some categories as cases can be subjective and vary with context.

(Curtin et al.; 2024)	Developed a user-friendly risk assessment tool for Irish SMEs based on analysing GRC tools used world-wide and SME feedback. The tool aligns with global standards like GDPR and uses minimal technical jargons for easy understanding.	Limited to a particular location reduces the scalability and accessibility of the tool. Customised remediations aren't explored in the tool.	28/08/2024	Some threats and regulations outside of Europe aren't addressed in the tool emphasizing on use of automation, accessibility to any global SME and threat coverage.
(Benz and Chatterjee; 2020)	Developed a Cybersecurity Evaluation Tool (CET) as a self-risk assessment based on NIST framework with 35 questions. The tool covers all 5 NIST categories and generates maturity scores with recommendations.	The tool is a static questionnaire for a one-time purpose without interactive dashboards or monitoring.	04/05/2020	Risk register tracking, visualizations and real-time monitoring aren't integrated in the tool presenting the assessment without regular updates made to the threat database.
(Lughbi et al.; 2024)	Developed a dashboard to identify, classify and visualize real-time tweets on cyber attacks. The NLP machine learning algorithm categorizes the tweet and displays the data in maps and charts.	The tool takes the dataset from social media with a higher chance in bias reducing threat coverage.	28/02/2024	The tool doesn't include assessment checks on the processes and systems in SMEs like incident response and backups, while relying on only the defined dataset.

Table 2: Summary of reviewed risk management tools and frameworks

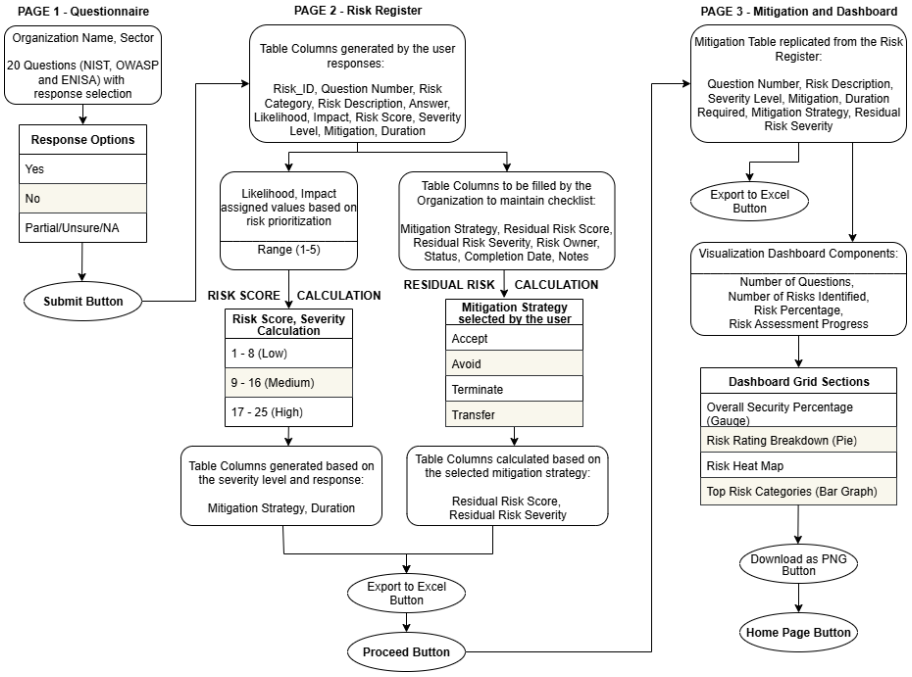

Figure 1: Flowchart of the Proposed Methodology

2.7 Gaps in Current Literature

Existing frameworks supported by global guidelines like NIST CSF, ISO 27005 and ENISA are complex for SMEs to implement with most research covering a theoretical analysis rather than developing user-friendly tools that can be used to track the progress with a detailed risk assessment and register. Automated tools for SMEs don't have automation integrated for real-time monitoring due to limited resources. Many papers discussed in the literature review present a qualitative risk analysis and default risk identification mechanisms, thus leading to approach a new methodology consisting of dynamic risk scoring and hybrid models suited for SMEs. Tools like CR-SAT and CYSEC have a similar risk assessment process designed for specific sectors and locations. While the tools may be user-friendly, some of the limitations include scalability, threat coverage, easy tracking with customised remediation and visualizations. These gaps justify the research question utilising python and HTML to develop an automated risk assessment tool and address these limitations to further enhance SME risk management effectively.

3 Methodology

3.1 Flowchart Diagram

Diagram 1 showcases the process layout and key components of the risk assessment tool's interface, starting from the home page with the questionnaire leading to the automated risk register with mitigation strategies and lastly, displaying calculated residual risks and a visualization dashboard. This flowchart presents an optimised workflow for SMEs to assess, mitigate and monitor their identified risks efficiently.

3.2 Proposed Methodology

3.2.1 Frameworks and Design Specifications

The research done for the risk assessment tool development includes a structured approach taken focused on qualitative priority-weighted risk assessments for SMEs. The comprehensive literature review supported the analysis of critical risks being identified that are faced by SMEs regularly. The review was also focused on exploring security and operational vulnerabilities/weaknesses from frameworks such as NIST CSF 2.0, ENISA and OWASP Top 10 addressing financial, operational and compliance risks. Below are the risk categories refined from the frameworks contributing towards 80-90% of SME cyber incidents:

- **NIST CSF:** Few of the critical risks include ransomware, denial of service (DoS) and injection (SQLi) attacks, phishing and business email imposters. Ransomware attacks cause severe business losses due to operational disruption and malware infections spread through malicious code exploits unpatched systems. Phishing and business email imposters trick employees into revealing credentials or accessing malicious attachments, emphasizing on the implementation of secure wireless networks, remote access, website and network security (NIST; 2025).

- **ENISA:** Some of the risks prioritised in Europe for SMEs include protection against ransomware, malware and social engineering attacks. Malware attacks exploit the limited endpoint security protocols while social engineering like phishing attacks utilise the weaknesses of employees with less awareness training to gain unauthorized access. Threats related to data security and availability (DoS attacks for user interfacing applications) are critical as SMEs are primarily targeted in data breaches for handling sensitive information without extensive measures in place (ENISA; 2025).

- **OWASP Top 10:** Some web-application based risks include security misconfigurations, outdated software components (unpatched systems), SQL injection (exploitation of user input fields), authentication failures (weak passwords or lack of multi-factor authentication) and improper access control (role-based permissions) targeting online services. Secure development of applications with regular monitoring and vulnerability scans also ensures active incident management (OWASP; 2025).

3.2.2 Risk Register and Scoring

The 4 fundamental pillars to maintain a strong security posture are: implementing strong passwords, deploying anti-virus/malware software, ensuring regular automatic updates and performing backups.
Researching all the listed sources supported narrowing down **20 key risk categories** and 5 sections *(Information Security Management System, Data Encryption and Backup, Employee Awareness from Phishing, Network Security and Vulnerability Scanning, Protection against Ransomware and DoS Attacks)* for the questionnaire. The questions were designed with **3 response** options - Yes (low exposure), No (high exposure) and Partial/Unsure/Not Applicable (medium or uncertain exposure) enabling a qualitative self-assessment based on the user input without requiring quantitative data (Figures 5, 6).

The responses are saved with the company details and are mapped to an **automated risk register** calculating the risk score based on the likelihood of occurrence and impact of the risk (both parameters are on a scale from 1-5) (El-Hajj and Mirza; 2024).

- **Likelihood of Occurrence**: This parameter measures how probable the risk is based on the response.
  1: Rare - Almost never occurs as a basic security setup can prevent risks.
  2: Unlikely - Can happen occasionally and is rare with basic scans.
  3: Occasional - Could occur under specific conditions specifically if risks are overlooked.
  4: Moderate - Happens frequently without attention paid to remediate the risk.
  5: Constant - Occurs very often and is a recurring risk impacting operations.

- **Impact of Risk**: This parameter measures the damage/disruption caused by the risk if the event occurs.
  1: Insignificant - Minimal impact like a short downtime that can be mitigated immediately without cost involved.
  2: Minor - Small effect of the risk is noticed but is easy to recover from with low cost and a small pause in the business.
  3: Moderate - Significant disruption caused that may take time and resources to recover.
  4: Major - Severe damage caused facing financial, data loss or reputational damage.
  5: Severe - Critical risk resulting in a cyber attack disrupting operations significantly. (Sánchez-García et al.; 2022)

- Formula used for calculation:
  Risk Score = Likelihood of Occurrence × Impact of Risk

Priority-weighted qualitative scoring assigns different weightage values to the likelihood and impact prioritizing risks while calculating the risk score (Figure 7). This approach is designed to be focused on the business impact emphasizing on categorizing threats with limited available resources. Each question is assigned a priority depending on the impact of the business and the user's response (Yes/No/Partial/Unsure) controls the likelihood score. While the results may vary based on subjective conditions, the risk management process is simplified and structured for SMEs enabling strategic decision making and risk remediation. The **risk score** lies within the range of 1-25 and decides the severity level of the risk (Low/Medium/High) i.e., score of 1-8 is a low risk, 9-16 is a medium risk and 17-25 is a high risk (India; 2023).

3.2.3 Risk Mitigation and Residual Risks

A **mitigation solution** is displayed with an estimated duration for completion based on the user response. Common mitigation strategies were researched ensuring that the SMEs could resolve the risk within their limitations and resources. The mitigations were framed to be easy in understanding with clear steps to achieve and less technical jargons. For example, responses such as 'Yes' and 'Not Applicable' may have a low risk but mitigations emphasize on security maintenance like conducting regular audit reviews. The estimated duration includes an average time required to complete the activity based on the risk level. While this duration serves as a reference to users, the organization can have their own timelines listed for tracking (Figure 12).

The risk register contains a few columns after the above discussed sections for the organization to maintain their progress for tracking such as the Mitigation Strategy, Risk Owner, Status and Completion Date which can be inputted in the text form or dropdown. The **residual risk** is calculated based on one of the 4 selected mitigation strategies (Figure 8).

- **Accept:** The risk is accepted without implementing any additional controls which is convenient for low risk threats as mitigation costs can outweigh other benefits. The residual risk retains the original risk score without any changes, recommending SMEs to monitor and review the risk regularly.

- **Avoid:** The risk is eliminated completely by avoiding exposure of the risk like discontinuing a vulnerable process, setting the likelihood of the risk to 0. Removing the threat altogether changes the residual risk to 0, making it suitable to implement for high severity risks. SMEs prioritize their business to avoid larger threats to impact them further avoiding costs and damage.

- **Terminate/Mitigate:** The risk is reduced by mitigating the threat like patching systems or training employees. The impact of the risk reduces by 2 levels through terminating a vulnerability or implementing a security control. It is recommended for medium risk threats as average costs and resources are utilised to mitigate a major risk.

- **Transfer:** The risk is transferred to a third-party organization through insurance, contracts, etc reducing the impact by 3 levels. SMEs with resource constraints and limited knowledge can outsource risk management and remediation support shifting the responsibility externally (Rahman et al.; 2024).

- Formula used for calculation after applying the chosen remediation treatment:
  Residual Risk = Residual Likelihood × Residual Impact
  Accept: Residual Risk Score = Likelihood × Impact
  Avoid: Residual Risk Score = 0 × Impact = 0
  Terminate: Residual Risk Score = Likelihood × max (1, Impact - 2)
  Transfer: Residual Risk Score = Likelihood × max (1, Impact - 3)

The selected mitigation strategy is updated in the SQLite database dynamically using conditional statements in python and the residual risk score, residual severity level are calculated based on the formula listed above once the submit button is clicked (Figure 21). The **residual risk score** follows the same criteria as the risk score (range of 1-25) with the severity level as Low/Medium/High i.e., score of 1-8 is a low risk, 9-16 is a medium risk and 17-25 is a high risk (Sánchez-García et al.; 2022).

The tool consists of an '*Export to Excel*' button below the table which captures the risk register and mitigation table along with the filled in information by the user to track progress and maintain the spreadsheet for closing out action items (Figures 9, 10, 13). The '*Download Image*' button exports the dashboard with all visualization charts as a PNG image (Figure 15).

3.2.4 Visualization Dashboards

The user-friendly **visualization dashboard** supports SMEs in making efficient informed decisions with optimised and precise summaries on their identified risks and security posture. The summary of the risk assessment states clear, understandable definitions for SMEs and highlights the overall severity with the risk and security percentage with the top risk categories displayed containing the highest risk score (Figure 11). Key metrics presented in visualization charts help users identify critical vulnerabilities and prioritize remediation based on risks without technical expertise (Figure 14). It contains 4 visualizations highlighting some critical metrics in the header such as the total number of questions, number of identified risks (calculated from the responses), risk percentage (average percentage calculated based on the risk weightage) and the risk assessment progress (El-Hajj and Mirza; 2024).

- **Overall Security Percentage:** A gauge chart displaying the security posture of the company as a percentage, calculated by the formula (100 - risk percentage). 0-40% is considered low security percentage, 41-70% is considered medium security percentage and 70-100% is considered high security percentage with a low risk.
- **Risk Rating Breakdown:** A pie chart categorized by the severity level - Low, Medium and High based on the risk score of each question, highlighting critical risks for prioritizing remediation.
- **Risk Heat Map:** A matrix plotted with the labels - likelihood (Constant to Rare) vs impact (Insignificant to Severe) colour coded as green, yellow and red. The risk score is displayed in the particular blocks with the matrix range of 5x5 based on the risk categories.
- **Top Risk Categories:** A bar chart showcasing the score of each top risk category (Asset Management, Policy and Compliance, Data and Access Security, Infrastructure and Network Security, Threat Detection and Prevention, Incident Response and Recovery) assists SMEs in understanding sector-specific risks. Responses such as 'No' adds 1 to the value and 'Unsure/Partial' adds 0.5 to the score ranking the category with most risks (Sierra; 2025).

4 Implementation

The final output includes the web application with 3 pages – questionnaire form for self-assessment, automated risk register generated from the responses with risk and residual score calculations and mitigation tracking with visualization dashboards. The tool also contains export options to download the image and excel sheet, making it suitable and user-friendly for SMEs.

- An automated risk register table is generated based on the responses (Yes, No, Unsure/Partial/Not Applicable) of 20 questions in a checklist-like format for progress monitoring.
- The risk score (range of 1-25) is calculated with the likelihood and impact through priority-weighted scoring. Severity levels are defined on the risk criticality with custom mitigation solutions and estimated duration.

- The residual risks (range of 1-25) are calculated with the likelihood and impact after treatment based on the selected mitigation strategy (Accept, Avoid, Terminate and Transfer).
- The dashboard displays 4 visualizations based on the presented data – critical security metrics, risk heat map, gauge chart for overall security percentage, pie chart for the severity breakdown and bar chart for the top risk categories.

4.1 Materials and Equipment Used

Global framework standards and templates such as NIST's CSF 2.0 small business quick-start guide, ENISA's SME cybersecurity toolkit, CISA's cyber essential starters kit and OWASP's risk rating methodology provided a baseline in creating the questionnaire and the risk scoring methodology (Rahman et al.; 2024; El-Hajj and Mirza; 2024). Standard laptops were used with access to online resources and tools, ensuring downloadable exports for Microsoft Excel and PNG images were successful. No additional equipment is required for the project as the goal is to create a low-cost convenient tool accessible for SMEs with minimal digital requirements.

4.2 Tools and Languages Used

HTML5 and CSS3 were used to create the user interface with JavaScript embedded for the logic customisation and integration of the library packages. Python 3.12.7 was utilised for backend processing like risk and residual score calculations and automated entries, updates made to the database (Figure 16). SQLite 3.13.1 was used for data storage with 5 tables (Figures 17, 18, 19, 20, 21) created to maintain the question descriptions, responses, risk register entries, mitigation solutions and mapping of the responses with the risk and residual score (El-Hajj and Mirza; 2024). Kleopatra GPG 3.3.0 was utilised to encrypt the database file for additional security. Open-source libraries through CDN like Chart.js was used for heat maps and bar charts while html2canvas was used to export the dashboard to a PNG image and SheetJS was used to create downloadable excel files for the risk register and mitigation tables (Rahman et al.; 2024).

4.3 Data Storage

Sensitive organizational data wasn't stored in the SQLite database except the SME name and sector to reduce data exposure. Input fields in the risk register (eg: risk owner and notes) were intentionally excluded from the database ensuring a secure risk assessment process and transparent tracking for the user with minimal data required from the company. While the data isn't encrypted or masked in storage, the database file is encrypted at rest with a specific user permissions (Role-based access) using Kleopatra, an open-source GPG-based encryption tool. This cryptographic tool manages encryption keys and provides password protection, making it suitable for tools handling non-critical data (OpenPGP; 2025). With better resources in the future to enhance the proposed tool, secure SQL database applications like SQLCipher can be utilised which integrates data encryption in storage.

5 Evaluation

The below evaluation metrics were considered based on risk assessments:

- **Identification of Key Risk Indicators (KRIs)** – Key risk categories are measured on relevance to SMEs and threat coverage. A benchmark is set to cover at least 80% of critical risks that are faced by SMEs in the risk assessment (Rahman et al.; 2024).
- **Risk Score Metrics** – Dependent on the likelihood and impact value for the calculation *(Risk Score = Likelihood × Impact)*, accuracy and precision are measured for classifying values to risks based on the severity between the range of 1-5. The risk score can fall within the range of 1-25 presenting a low/medium/high severity.
- **Mitigation Effectiveness** – Security protocols must be utilised in the implementation of mitigations while being efficient for SMEs ensuring partial/complete closure of the risk. The percentage decrease of the risk is evaluated before and after remediation, irrespective of the risk treatment (El-Hajj and Mirza; 2024).
- **Residual Risk Metrics** – Residual risk is calculated and compared with the original risk score with the chosen risk response to identify the remaining exposure. The metric measures the effectiveness of the risk after mitigation(AL-Dosari and Fetais; 2023).
- **Visualization Metrics** – Usability of the dashboard is evaluated based on the practical and efficient use of charts for SMEs with accuracy, level of understanding and completeness being some of the critical evaluation metrics.

5.1 Discussion

The automated risk assessment tool designed for SMEs was able to achieve the objective of the research question. The tool was developed to be user-friendly and accessible with a qualitative scoring system covering critical risk categories and providing automated mitigations and visualizations. Threat coverage includes over 85% of the critical risks covered based on global guidelines and ENISA benchmarks with a significant reduce in the residual risk after mitigation treatment. The below test cases provide the variation in results depicting all the 5 visualization charts for responses that have an overall low, medium and high security posture. Each case will be discussed on the individual security metrics and the insights taken from the dashboard.

5.2 Test Case 1

Figure 2 simulates a regular SME that has achieved an average security posture with cybersecurity protocols in place. The security metrics showcase 7 identified risks out of 20 questions with 35% of risk percentage. The gauge chart displays the overall security percentage as 65%, a medium-level criticality with top risk categories to be prioritised as Vendor Management, Ransomware Incidents, Data Backup and Recovery. The pie chart breaks down the severity rating of the risk assessment as 60% low (green), 25% medium (yellow) and 15% high (red). The heatmap differentiates the severity of each risk category based on the likelihood and impact with 12 questions having low risk, 5 questions having

a medium risk and 3 questions having a critically high risk. The bar chart ranks the top risk categories as threat detection and prevention as the highest, followed by policy and compliance, incident response and recovery. This test case has a balanced security percentage with improvements required to reduce the identified risks.

Figure 2: Test Case 1 - Medium level Severity

5.3 Test Case 2

Figure 3 simulates an organization that has achieved a high security posture with 3 identified risks out of 20 questions and 15% of risk percentage. The gauge chart displays the overall security percentage as 85%, a low-level criticality with the top risk categories that are to be addressed as Endpoint and Network Security, DoS Incidents, Detection and Monitoring. The pie chart breaks down the severity rating as 80% low (green) and 20% medium (yellow). The heatmap displays the risk severity based on the likelihood and impact with no questions achieving a higher risk and 4 questions having a medium risk. The bar chart ranks the top risk category as infrastructure and network security. This test case has a good security percentage acting as a benchmark for SMEs with minor risks that can enhance the security percentage to 100%.

5.4 Test Case 3

Figure 4 simulates a SME in danger that has achieved a low security posture with few cybersecurity protocols in place. The security metrics showcase 13 identified risks out of

Figure 3: Test Case 2 - Low level Severity

20 questions with 65% of risk percentage. The gauge chart displays the overall security percentage as 35%, a high-level criticality with top risk categories to be prioritised as Vendor Management, Ransomware Incidents and Phishing Incidents. The pie chart breaks down the severity rating as 35% low (green), 45% medium (yellow) and 20% high (red). The heatmap displays the risk severity based on the likelihood and impact with 7 questions having low risk, 9 questions having a medium risk and 4 questions having a critically high risk. The top risk categories are present in almost every section but threat detection and prevention, infrastructure and network security gained a high score of 3 in the bar graph. It is then followed by policy and compliance, data and access security, incident response and recovery. This test case showcases a worst-case scenario for SMEs with a low security percentage prioritising immediate remediation of critical risks to prevent potential incidents.

Figure 4: Test Case 3 - High level Severity

5.5 Scope and Generalizability

The scope of the project is developing an open-source tool for self-risk assessments in cybersecurity through a questionnaire across 5 sections with scoring, mitigations and a dashboard. Generalizability is medium for SMEs with a basic IT setup. The framework follows a global standard that can also specify US and European laws, thus can face regional concerns.

5.6 Strengths and Limitations

Benefits of the implementation include a simple, scalable and usable methodology applied to develop the tool covering critical risks in a questionnaire convenient for SMEs, providing an efficient solution compared to other complex frameworks. The tool is cost-effective and supports progress tracking and visualization dashboards that can be exported to excel and image files without the requirement of other paid applications. It is also developed dynamically to include additional risk categories with evolving threats and modifications regularly made to the mitigation solutions. Implications include the lack of emerging threats or specific areas like AI-based attacks, IoT vulnerabilities being addressed in the risk assessment for real-time monitoring and detection, justifying the remaining 10% of the risk categories not being added in the risk assessment. Qualitative scoring can introduce bias (approximately 20-30%) due to its subjective nature. The tool has a limited scope in security targeting all SMEs instead of selective sectors.

5.7 Further Work and Improvements

Based on the limitations discussed, integrating AI for real-time monitoring and automated threat updates could significantly enhance the tool. Addressing risk categories which aren't covered that target SMEs can be a critical improvement in the assessment for threat exposure. A hybrid model could be implemented for a better result combining qualitative and quantitative methods in the risk scoring. Kleopatra was utilised to encrypt the database file, but with future advancements in the framework, all sensitive data must be securely stored and encrypted at rest and in transit. Lastly, publishing the application on a public platform for SMEs globally to have access to risk assessments can help identify and improve their security posture.

6 Conclusion and Future Work

The research question for this project (*How can a python-based automated cybersecurity risk assessment tool be implemented to integrate a risk register, custom mitigation strategies and a visualization dashboard while addressing gaps in threat coverage, automation and scalability in existing SME frameworks?*) was addressed by developing a questionnaire using Python and HTML to identify critical risks targeted by SMEs based on NIST CSF, OWASP Top 10 and ENISA frameworks. The tool uses a qualitative risk scoring model to calculate the likelihood of occurrence, impact, risk score and the severity level. A risk register is generated from the responses of the assessment with customised mitigations and residual risk, followed by a dashboard containing visualizations presenting critical security metrics like risk percentage. Python was utilised for the backend development with libraries (Chart.js, html2canvas, SheetJS) for export and chart formations with HTML, CSS and JavaScript serving the frontend connecting to the data stored in SQLite. The tool was validated through multiple test cases comparing responses yielding a balanced, high-risk and low-risk profile.

This project was successful in answering the research question and achieving all 4 research objectives as the tool was able to identify critical gaps from a questionnaire of 20 risk categories with 85% of threat coverage. Reducing manual errors, this risk assessment tool is designed to be scalable and user-friendly while supporting SMEs in their decision-making process and understanding their security posture with a medium to track their

progress.

Key findings: Implementation of the SME risk assessment framework could simplify complex guidelines like NIST CSF to manage risks and be accessible. Qualitative scoring supports risk prioritization for SMEs which is also analysed through the risk rating pie chart breakdown, heat maps and top risk categories in bar charts.
Implications: The tool is efficient, user-friendly and improves cyber resilience in the SME by having a strong risk management process in place, reducing incidents by 40-50% based on global benchmarks like ENISA.
Limitations: Qualitative models can lead to bias due to its subjectivity impacting the scores. The lack of quantitative measures can reduce the precision in high-risk cases. The tool didn't address the remaining 10% of risks which aren't included in the risk assessment with categories like IoT and AI security. These limitations would be executed as part of future work.
Future Work: Integration of AI in the framework can support real-time monitoring and regular updates made to threat databases with evolving risks. Implementation of a hybrid model can improve the risk scoring system to take context and numbers into consideration increasing the accuracy.
Commercialization: The tool can be published online on GitHub as an open-source application for SMEs globally. Based on feedback from organizations, the tool can be enhanced and be a SaaS available for self-risk assessments.

References

Abdullah, H. (2019). Analyzing the technological challenges of governance, risk and compliance (grc), *2019 4th International Conference on Electrical, Electronics, Communication, Computer Technologies and Optimization Techniques (ICEECCOT)*, IEEE, pp. 274–282.

AL-Dosari, K. and Fetais, N. (2023). Risk-management framework and information-security systems for small and medium enterprises (smes): A meta-analysis approach, *Electronics* **12**(17): 3629.

Alahmari, A. A. and Duncan, R. A. (2021). Towards cybersecurity risk management investment: A proposed encouragement factors framework for smes, *2021 IEEE International Conference on Computing (ICOCO)*, IEEE, pp. 115–121.

Alharbi, F., Alsulami, M., Al-Solami, A., Al-Otaibi, Y., Al-Osimi, M., Al-Qanor, F. and Al-Otaibi, K. (2021). The impact of cybersecurity practices on cyberattack damage: The perspective of small enterprises in saudi arabia, *Sensors* **21**(20): 6901.

Arthur, J. L., Amofah, K., Arthur, S. D., Boateng, R. and Oppong, D. (2025). Small and medium enterprise approach to risk management in the kumasi metropolis, *Journal of Innovation and Entrepreneurship* **14**(1): 1–22.

Benz, M. and Chatterjee, D. (2020). Calculated risk? a cybersecurity evaluation tool for smes, *Business horizons* **63**(4): 531–540.

Carías, J. F., Borges, M. R., Labaka, L., Arrizabalaga, S. and Hernantes, J. (2020). Systematic approach to cyber resilience operationalization in smes, *IEEE access* **8**: 174200–174221.

Cobilean, V., Mavikumbure, H. S., Mcbride, B. J., Vaagensmith, B., Singh, V. K., Li, R., Rieger, C. and Manic, M. (2023). A review of visualization methods for cyber-physical security: Smart grid case study, *IEEE Access* **11**: 59788–59803.

Curtin, M., Sheehan, B., Gruben, M., Kozma, N., O'Carroll, G. and Murray, H. (2024). Development of a cyber risk assessment tool for irish small business owners, *arXiv preprint arXiv:2408.16124* .

El-Hajj, M. and Mirza, Z. A. (2024). Protectingsmall and medium enterprises: A specialized cybersecurity risk assessment framework and tool, *Electronics (Switzerland)* **13**(19): 3910.

ENISA (2025). Enisa threat landscape 2025 — enisa.
URL: *https://www.enisa.europa.eu/publications/enisa-threat-landscape-2025*

Hassan, M., Saeedi, K., Almagwashi, H. and Alarifi, S. (2022). Information security risk awareness survey of non-governmental organization in saudi arabia, *The International Research & Innovation Forum*, Springer, pp. 39–71.

Igor, N. (2023). Risk prioritizing method at the stage of qualitative risk analysis in the process of project implementation, *International Journal of Accounting, Finance and Risk Management* **8**(2): 43–48.

India, I. (2023). Assigning scores to qualitative risks - irm india affiliate.
URL: *https://www.theirmindia.org/blog/assigning-scores-to-qualitative-risks/*

Katsinis, A., Lagüera-González, J., Di Bella, L., Odenthal, L., Hell, M. and Lozar, B. (2024). *Annual Report on European SMEs 2023/2024: SME Performance Review 2023/2024*, Publications Office of the European Union.

Lughbi, H., Mars, M. and Almotairi, K. (2024). A novel nlp-driven dashboard for interactive cyberattacks tweet classification and visualization, *Information* **15**(3): 137.

Macrino, N., Pallas Enguita, S. and Chen, C.-H. (2025). Enhancing cyber situational awareness through dynamic adaptive symbology: The dass framework, *Sensors* **25**(20): 6300.

McKenna, S., Staheli, D., Fulcher, C. and Meyer, M. (2016). Bubblenet: A cyber security dashboard for visualizing patterns, *Computer Graphics Forum*, Vol. 35, Wiley Online Library, pp. 281–290.

NIST (2025). Nist csf.
URL: *https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf*

OpenPGP (2025). Kleopatra - openpgp.
URL: *https://www.openpgp.org/software/kleopatra/*

OWASP (2025). Owasp top 10:2025 rc1.
URL: *https://owasp.org/Top10/*

Pačaiová, H., Markulik, Š., Turisová, R. and Nagyová, A. (2018). How to build risk-based thinking methodology based on process approach., *Acta Mechanica Slovaca* **22**(1).

Ponsard, C. (2024). Building a cybersecurity risk metamodel for improved method and tool integration, *arXiv preprint arXiv:2409.07906* .

Rahman, M. M., Kshetri, N., Sayeed, S. A. and Rana, M. M. (2024). Assessits: Integrating procedural guidelines and practical evaluation metrics for organizational it and cybersecurity risk assessment, *arXiv preprint arXiv:2410.01750* .

Rawindaran, N., Jayal, A., Prakash, E. and Hewage, C. (2023). Perspective of small and medium enterprise (sme's) and their relationship with government in overcoming cybersecurity challenges and barriers in wales, *International Journal of Information Management Data Insights* **3**(2): 100191.

Sánchez-García, I. D., Mejía, J. and San Feliu Gilabert, T. (2022). Cybersecurity risk assessment: a systematic mapping review, proposal, and validation, *Applied Sciences* **13**(1): 395.

Shojaifar, A. and Fricker, S. A. (2020). Smes' confidentiality concerns for security information sharing, *International Symposium on Human Aspects of Information Security and Assurance*, Springer, pp. 289–299.

Shojaifar, A. and Järvinen, H. (2021). Classifying smes for approaching cybersecurity competence and awareness, *Proceedings of the 16th International Conference on Availability, Reliability and Security*, pp. 1–7.

Sierra, C. (2025). 5 cybersecurity dashboards your board will actually understand. **URL:** *https://cybersierra.co/blog/cybersecurity-dashboard-examples/*

Turgay, S., Aydin, A. et al. (2023). Risk mitigation for smes: A step-by-step guide to implementing an effective framework, *Financial Engineering and Risk Management* **6**(8): 71–80.

Van Haastrecht, M., Sarhan, I., Shojaifar, A., Baumgartner, L., Mallouli, W. and Spruit, M. (2021). A threat-based cybersecurity risk assessment approach addressing sme needs, *Proceedings of the 16th International Conference on Availability, Reliability and Security*, pp. 1–12.

Yu, Y. R., Seo, S. C. and Kim, B. K. (2013). It grc-based it internal control framework, *2013 15th International Conference on Advanced Communications Technology (ICACT)*, IEEE, pp. 382–385.

7 Appendix

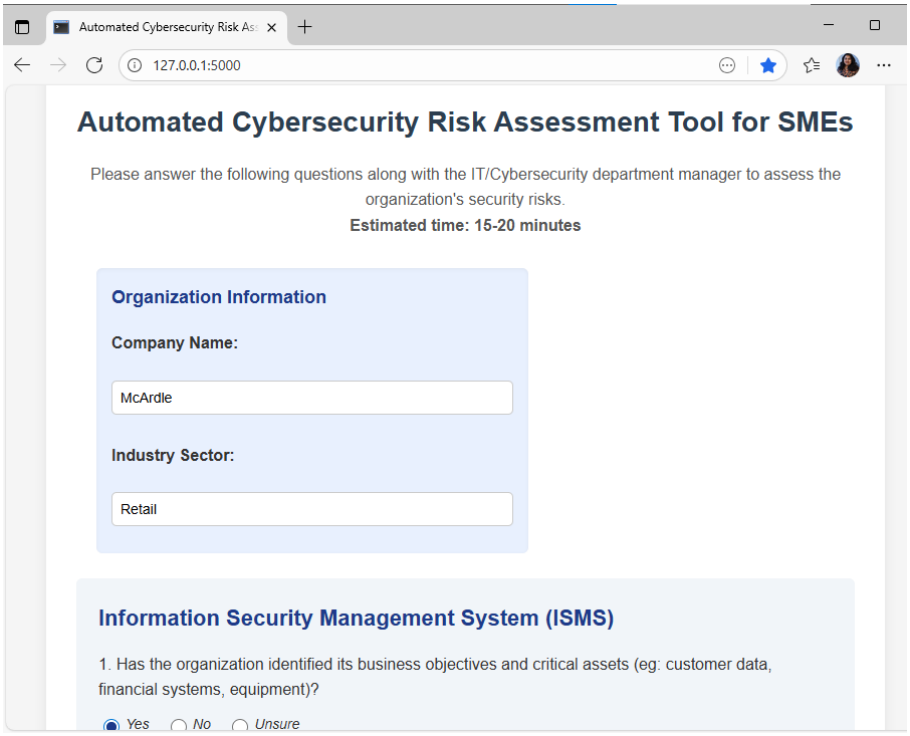

Figure 5: Home page - Company Name and Sector to be filled

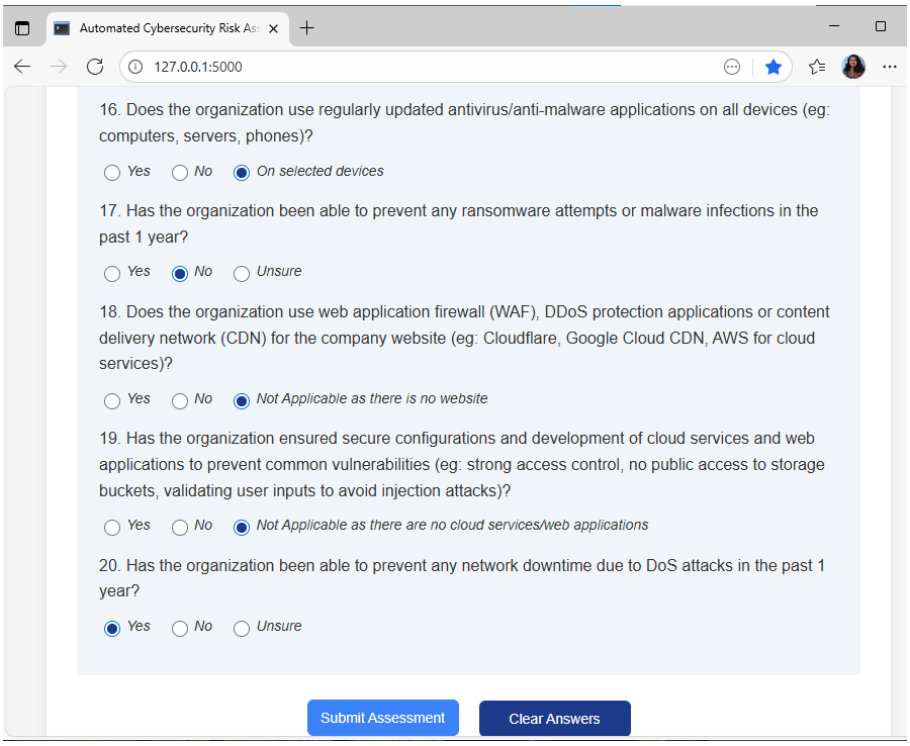

Figure 6: Questionnaire of the tool with Clear and Submit buttons

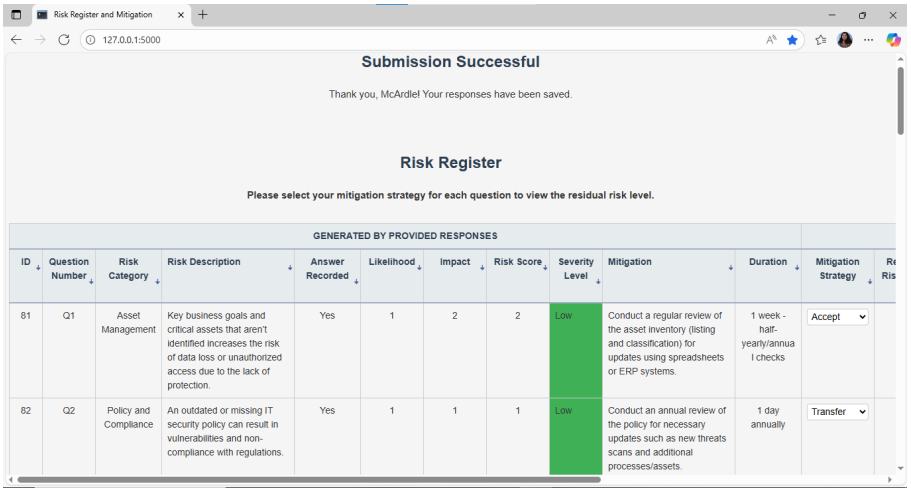

Figure 7: Risk Register generated from the Page 1 responses - contains Risk Category and Description, Response, Likelihood, Impact, Risk Score and Severity, Recommended Mitigation and Duration

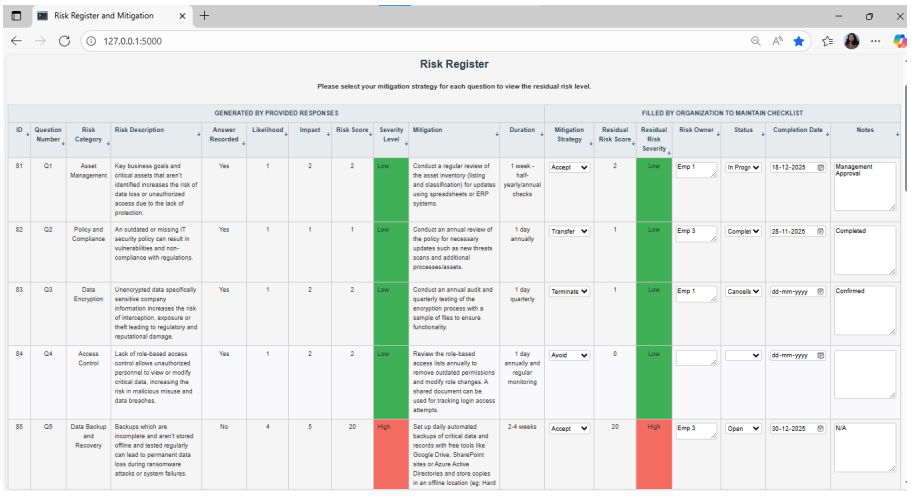

Figure 8: Mitigation Strategy selected to view the Residual Risk Score and Severity with other details filled as part of the checklist

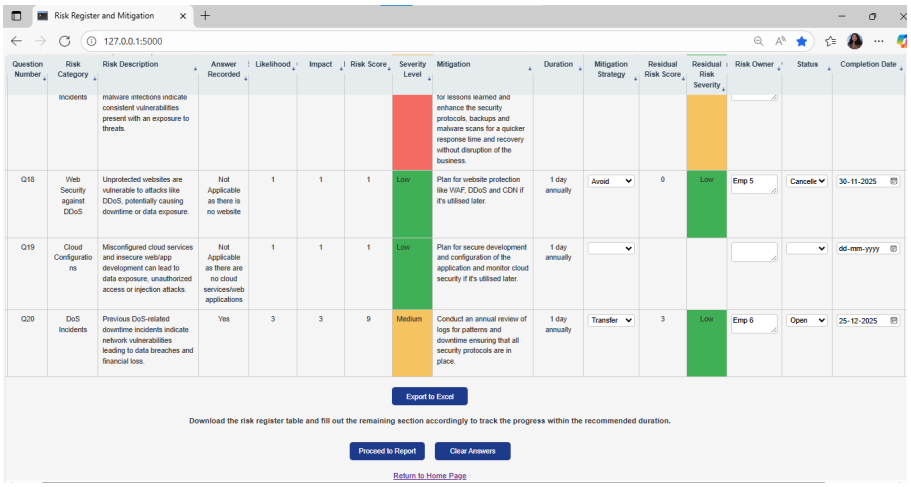

Figure 9: Table can be exported to an excel or the user can select the Submit or Clear buttons

Fields that are optional to be filled by the user - Mitigation Strategy, Risk Owner, Status, Completion Date, Notes

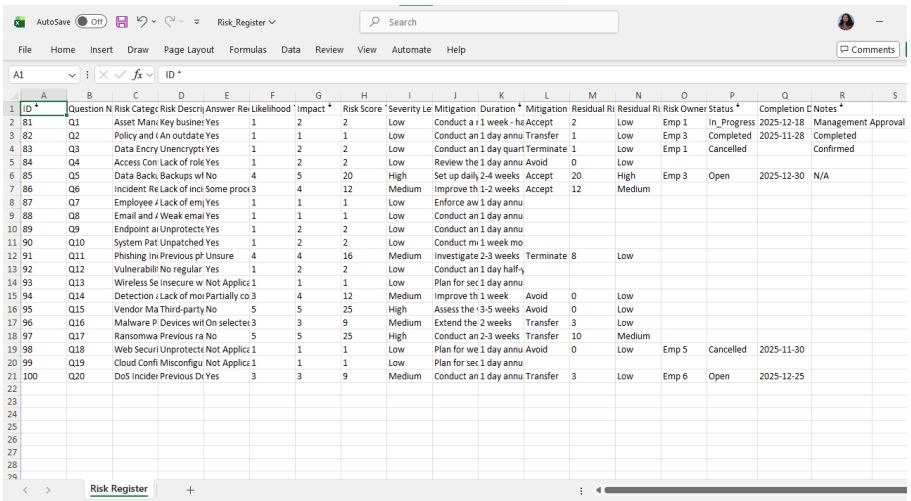

Figure 10: Risk Register Table exported to an excel with all fields

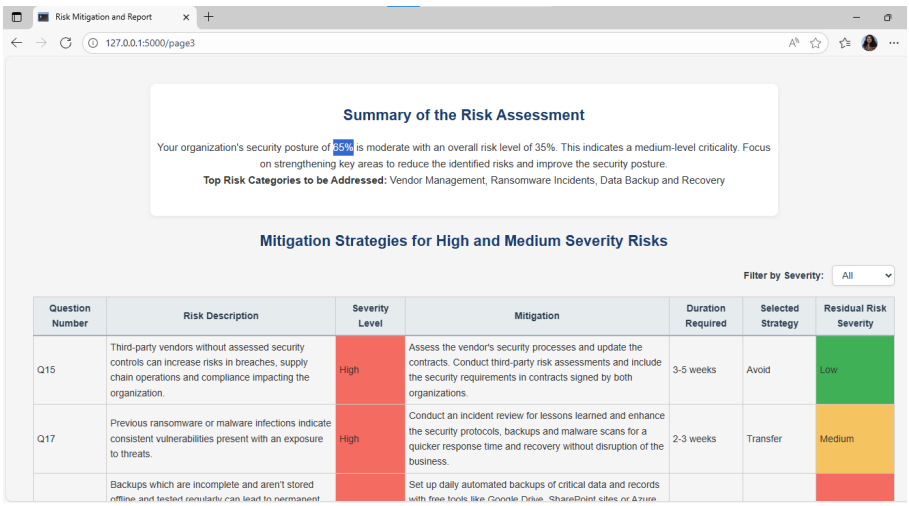

Figure 11: Summary Report generated from the responses and risk register from Page 2 presenting the Security and Risk Posture of the organization with Top Risk Categories

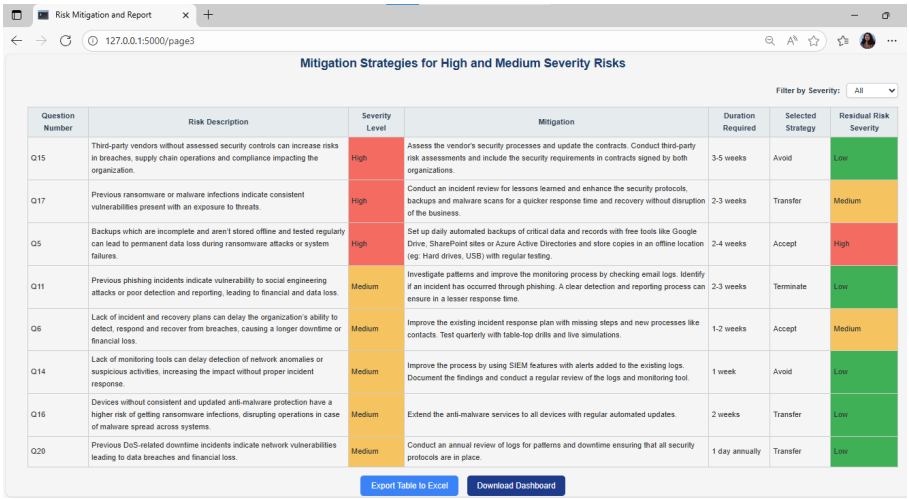

Figure 12: Risk Mitigation table displaying the Mitigation solution, Duration, Selected Mitigation Strategy and Residual Risk for the identified medium and high severity risks

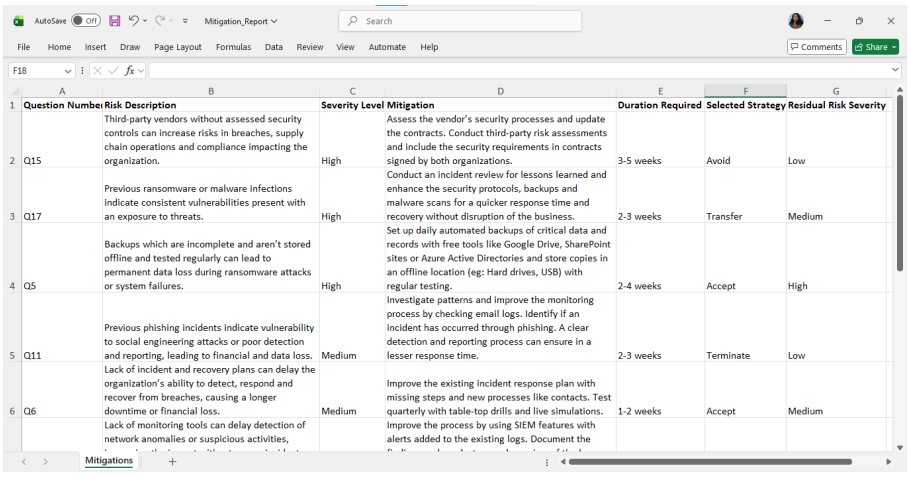

Figure 13: Mitigation table exported to an excel with the displayed columns

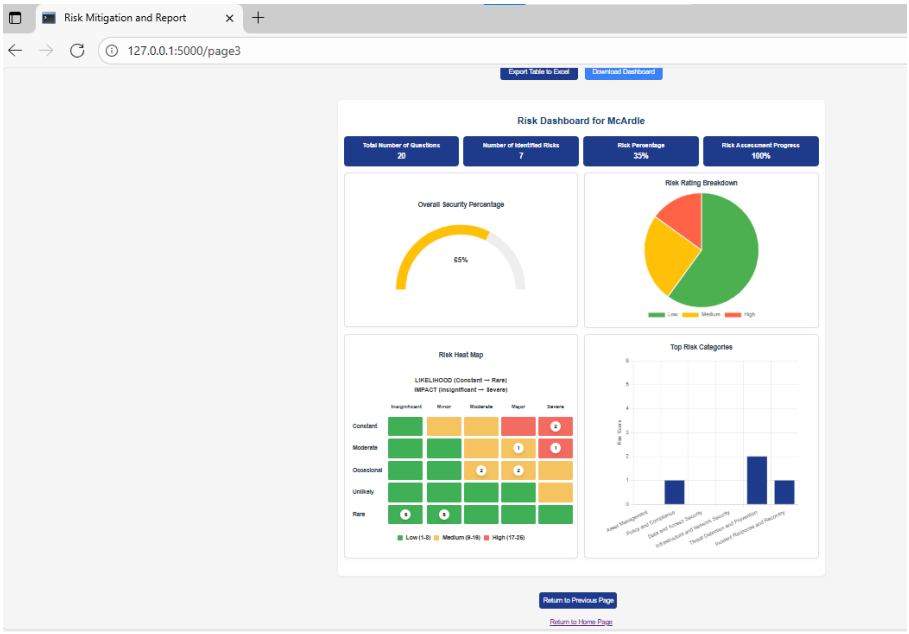

Figure 14: Dashboard generated on the calculated scores with risk metrics for efficient visualization, followed by the Return to Homepage button

Figure 15: Dashboard downloaded as a PNG image with 5 visualizations - Risk metrics header, Overall Security Percentage, Risk Rating Breakdown, Risk Heat Map and Top Risk Categories

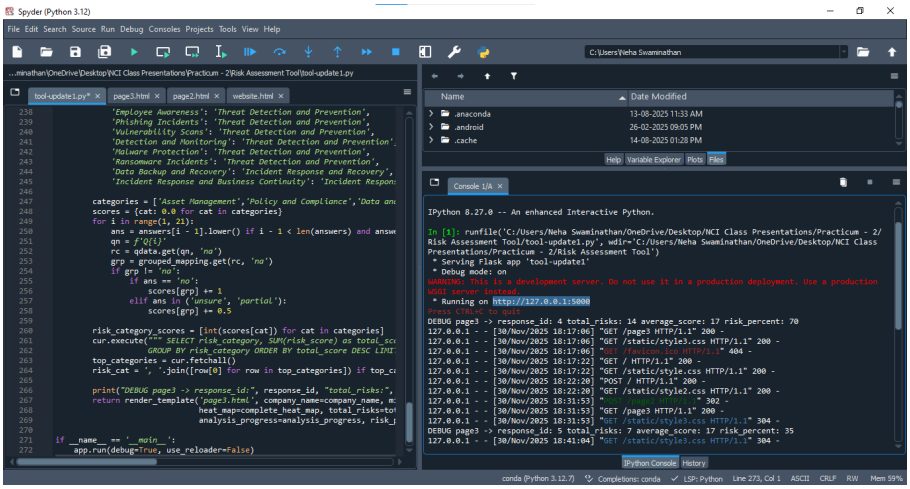

Figure 16: Python file configured on Spyder to run the HTML application

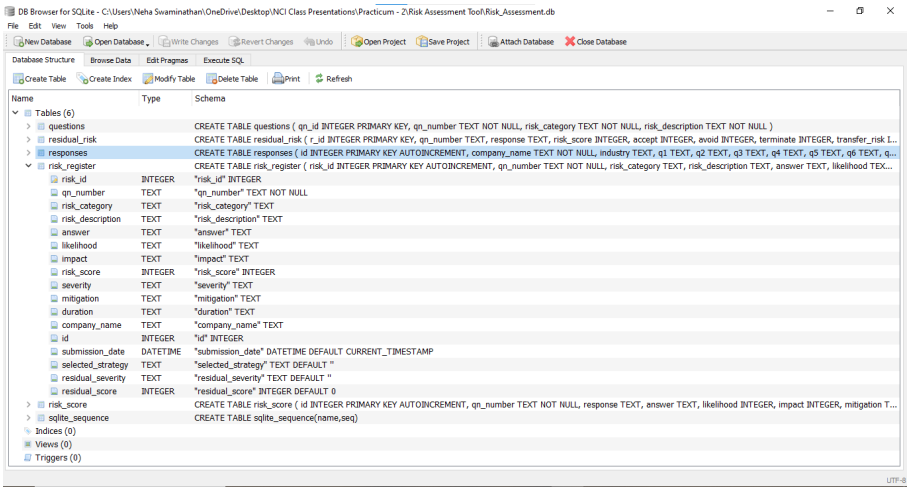

Figure 17: Risk assessment SQL database and 4 tables connected to the application back-end in SQLite

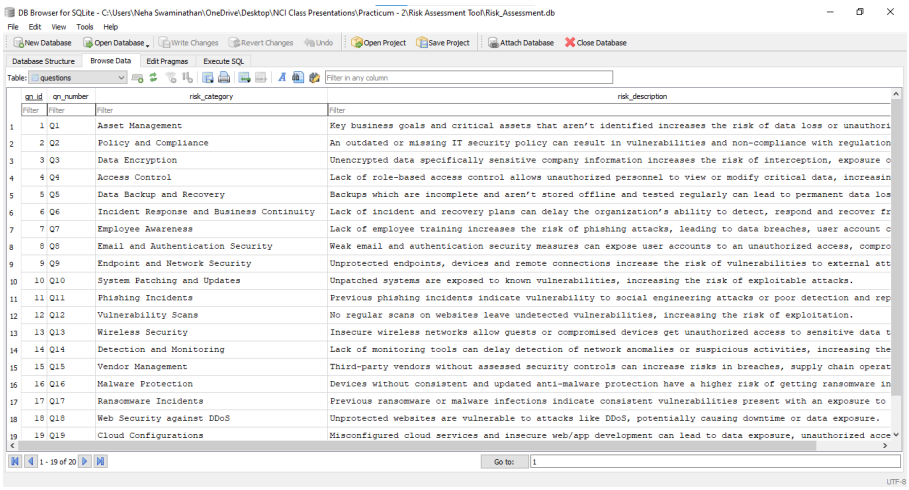

Figure 18: Table 1: Questions - Stores all the questions with the Risk Category and Description

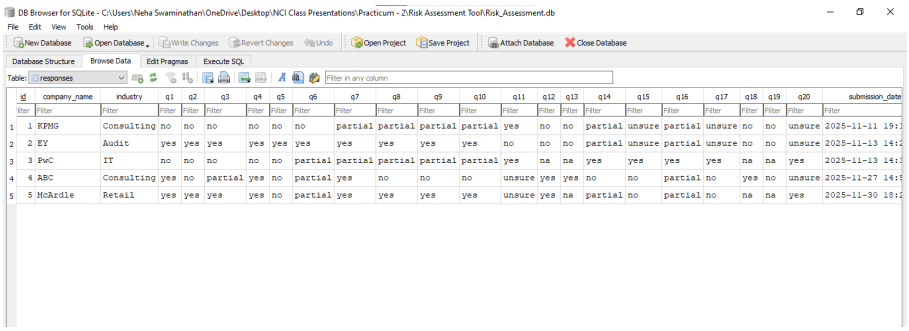

Figure 19: Table 2: Responses - Stores all the response entries with the Company Name, Industry, Answers Recorded and Submission Date

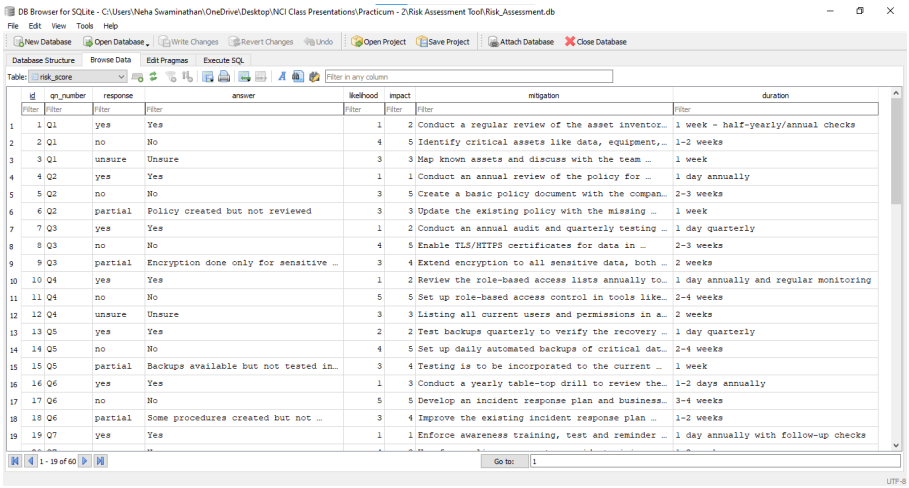

Figure 20: Table 3: Risk Score - Stores the Likelihood and Impact values, Mitigation solution and Duration for all options of responses (Yes/No/Unsure/Partial/NA) for each question

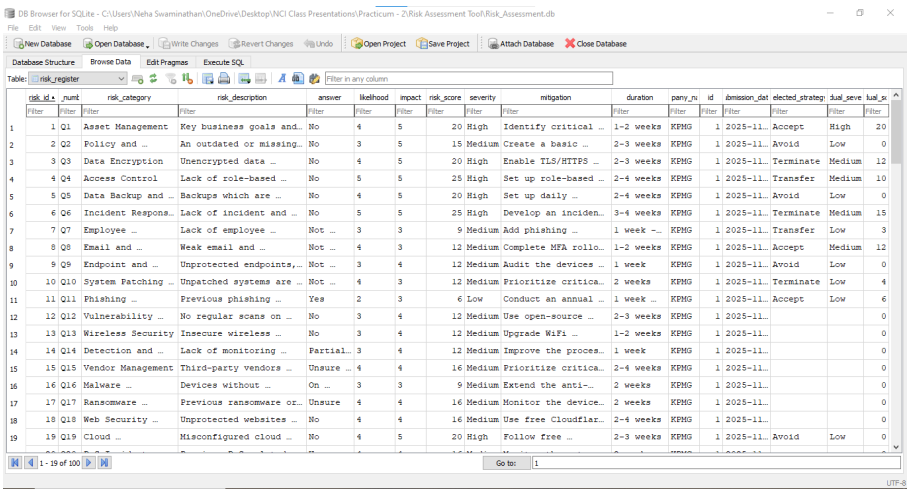

Figure 21: Table 4: Risk Register - Stores all the entries for the Page 2 Risk Register table with the fields connected from previously displayed tables, Risk Score and Severity which are calculated based on the Likelihood and Impact

Mitigation Strategy chosen by the user automatically generates the Residual Risk Score and Severity and is updated in the Risk Register table once the Proceed button is clicked supporting the Page 3 tables and visualizations