National College of Ireland

Configuration Manual

MSc Research Project
Cybersecurity

Amandeep Singh
Student ID: X20185294

School of Computing
National College of Ireland

Supervisor: Mark Monaghan

National College of Ireland

MSc Project Submission Sheet

School of Computing

Student Name: ……. ……Amandeep Singh……

Student ID: ……X20185294……..……

Programme: ……MSc in Cybersecurity …… **Year:** ……2021……..

Module: …… Research Project/Internship ……..……

Lecturer: …… Mark Monaghan ……..……

Submission Due Date: ……12th August 2024……..……

Project Title: Evaluating the Effectiveness of Cybersecurity Measures: A Quantitative Analysis of Threat Types and Implementation of NIST and ISO 27001 Framework

Word Count: ……676…… **Page Count:** ……3……..……..……

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: ……Amandeep Singh……

Date: ……11/08/2024……

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):	

Configuration Manual

Amandeep Singh
Student ID: x20185294

1 Introduction

1.1 Purpose

This manual provides step-by-step instructions for setting up, conducting, and analysing a study to evaluate the effectiveness of cybersecurity measures. The focus is on assessing the threat types and implementation of NIST and ISO 27001 frameworks.
This configuration manual provides detailed instructions for setting up the software, tools, and environments used in the research project.

1.2 Scope

This configuration manual is intended for researchers and cybersecurity professionals who aim to quantitatively analyse cybersecurity threats and the effectiveness of mitigation measures. It covers data collection methods, analysis techniques, and interpretation of results.

1.3 Prerequisites

- Basic understanding of cybersecurity frameworks (NIST, ISO 27001).
- Familiarity with statistical analysis tools and methods.
- Access to secondary data sources on cybersecurity threats and frameworks

2 Research Setup

2.1 System Requirements

Hardware

- Processor: Intel Core i5 or equivalent
- RAM: 8 GB minimum (16 GB recommended)
- Storage: 100 GB of free space

Software

- Operating System: Windows 10 / macOS 10.15 / Ubuntu 20.04
- Python: Version 3.8 or later
- R: Version 4.0 or later
- RStudio: Version 1.3 or later
- Jupyter Notebook: Latest version
- Anaconda: Latest distribution

2.2 Research Objectives

- Analyze various cybersecurity threats, including malware and APTs.
- Evaluate the effectiveness of the NIST and ISO 27001 frameworks in mitigating these threats.
- Understand the role of human factors in cybersecurity.

2.3 Defining Research Questions

- How do different cybersecurity threats impact stakeholders in the digital age?
- To what extent do NIST and ISO 27001 mitigate identified threats?
- How do human factors influence cybersecurity vulnerabilities?

2.4 Scope and Limitations

- Scope- Quantitative analysis using secondary data sources.
- Limitations- Dependence on the quality and availability of secondary data, which may not fully capture the dynamic nature of real-world cybersecurity scenarios.

3 Methodology

3.1 Research Design

The study employs a quantitative research design, focusing on secondary data analysis to assess cybersecurity threats and the effectiveness of security measures.

3.2 Data Collection Techniques

- Secondary Data Sources: Gather data from reputable sources such as cybersecurity reports, incident databases, and previous research studies.
- Sample Selection: Select data that is representative of various sectors and time periods to ensure a comprehensive analysis.

3.3 Variables and Measurement Instruments

- Variables: Types of cybersecurity threats, frequency of incidents, implementation levels of NIST and ISO 27001 frameworks, and human error factors.
- Measurement Tools: Utilize statistical software (e.g., SPSS, R) to analyze the collected data.

3.4 Data Analysis Techniques

- Descriptive Analysis Summarize the data to understand the distribution and basic characteristics.
- Correlation Analysis: Determine the relationship between different variables (e.g., implementation of frameworks and reduction in incidents).
- Regression Analysis: Assess the impact of various factors on the effectiveness of cybersecurity measures.

3.5 Validity and Reliability

- Ensure the validity of the data by cross-referencing multiple sources.
- Maintain reliability by using consistent data collection and analysis procedures.

3.6 Ethical Considerations

- Ensure data privacy and confidentiality when handling sensitive information.
- Obtain necessary permissions for using secondary data sources.

4. Data Collection and Analysis

4.1 Data Collection Process

- Step 1: Identify and access relevant secondary data sources.
- Step 2: Extract data related to cybersecurity threats and the implementation of NIST and ISO 27001 frameworks.
- Step 3: Organize the data in a structured format for analysis.

4.2 Data Analysis Procedure

- Descriptive Analysis: Conduct an initial analysis to describe the data and identify patterns.
- Statistical Analysis: Use correlation and regression techniques to examine the relationships between variables.

4.3 Interpretation of Results

- Summary of Findings: Present the key outcomes of the analysis, highlighting significant trends and correlations.
- Discussion Compare the findings with previous research and discuss their implications for cybersecurity strategies.

5. Conclusion and Recommendations

5.1 Summary of Study

Recap the research objectives, methodology, and key findings.

5.2 Recommendations

- For Organizations: Implement a dual approach by integrating both NIST and ISO 27001 frameworks.
- For Policymakers: Develop policies that enhance cybersecurity awareness and training programs.
- For Researchers: Explore new avenues of research, particularly focusing on emerging threats and innovative cybersecurity frameworks.

5.3 Future Research Directions

Suggest areas where further empirical research is needed to address gaps identified during the study.