MAJOR PROJECT - I

A Project Report

On

MENACE RECALL

Submitted By –

Manik Garg(R134216076)

Vikalp(R134216150)

Kritika Sharma(R134216072)

Under the guidance of

Dr. Susheela Dahiya

Abstract

The idea is to create a tool for risk assessment. The tool will give an option to select a framework from a list of options and use that particular framework for calculating risk rating. The analysis will be done on the given data and will result in a comparative study of the risk from different frameworks. We will also combine the qualities of each framework to derive an efficient calculation of the risk assessment.

Introduction

Security is one of the most important aspect in current world scenario. Data being the most important and private part of our lives, needs to be protected and for that purpose we need to implement various security controls at all places which are involved in any sort of data related operations. Security controls refer to the mechanisms used to restrict the access to the data or assets so as to maintain confidentiality, integrity and availability thus maintaining the CIA Triad.

Information security risks can be defined as consequence of uncertainty on information security Objectives. A control is a measure implemented to prevent from or to reduce the impact of security risks. A control can decrease the risk by reducing the possibility of an event, the impact or both. Information security risk management is very important for business, government, and also for individuals in order to protect their information. To manage the risks, organizations need to assess the security risks to their valuable assets and plan for mitigating control actions to address these risks

Information security Risk Assessment represents a process to ensure that the appropriate security measures are identified and applied to meet the management's expectations for a secure and trusted computing environment. Careful selection of Risk Assessment methods can help organizations to identify, manage, and evaluate the risks to their assets.

Problem Statement

We need to create a cumulative tool that uses various risk assessment models and perform a comparative study based on their outcomes.

Literature Review

[1] ISO/IEC 27001 specifies a management system that is intended to bring information security under management control and gives specific requirements. Organizations that meet the requirements may be certified by an accredited certification body following successful completion of an audit.

[2] ISO/IEC 27002 provides best practice recommendations on information security controls for use by those responsible for initiating, implementing or maintaining information security management systems (ISMS). Information security is defined within the standard in the context of the C-I-A triad.

[3] The standard offers four resources to organizations to "save time, effort and money": A clear explanation of the principles of management systems auditing, guidance on the management of audit programs, guidance on the conduct of internal or external audits and advice on the competence and evaluation of auditors.

[4] The purpose of ISO 31000:2018 is to provide principles and generic guidelines on risk management. ISO 31000 seeks to provide a universally recognized paradigm for practitioners and companies employing risk management processes to replace the myriad of existing standards, methodologies and paradigms that differed between industries, subject matters and regions.

[5] ISO 22301:2012 is a management system standard that specifies requirements to plan, establish, implement, operate, monitor, review, maintain and continually improve a documented management system to protect against, reduce the likelihood of occurrence, prepare for, respond to, and recover from disruptive incidents when they arise. It is intended to be applicable to all organizations or parts thereof, regardless of type, size and nature of the organization.

[6] The standard provides guidelines for information security risk management and supports the general concepts specified in ISO/IEC 27001 and is designed to assist the satisfactory implementation of information security based on a risk management approach.

[7] This standard provides guidance on the selection and application of techniques for assessing risk in a wide range of situations. The techniques are used to assist in making decisions where there is uncertainty, to provide information about particular risks and as part of a process for managing risk. The document provides summaries of a range of techniques, with references to other documents where the techniques are described in more detail.

[8] ISO 27017 standard provides guidance on the information security aspects of cloud computing, recommending and assisting with the implementation of cloud-specific information security controls supplementing the guidance in ISO/IEC 27002 and other ISO27k standards.

Objectives

To create tool using different technologies for cumulative risk assessment –

- Modules for different frameworks
- Risk calculation derivation
- Comparative study

Risk Assessment models

Risk Assessment is the process of identifying the potential threats that can negatively harm an organization to disrupt its business functioning.

It is performed to determine the procedures, controls, and measures to reduce the impact of the risk associated with the organization.

For performing the quantitative analysis of risk, we will use following models –

- FAIR model
- EMV model

Fair model

Factor analysis of Information Risk

A framework for understanding, analysing, and measuring information risk.

FAIR provides a reasoned and logical framework for answering these questions:

- A taxonomy of the factors that make up information risk. This taxonomy provides a foundational understanding of information risk, without which we couldn't reasonably do the rest. It also provides a set of standard definitions for our terms.
- A method for measuring the factors that drive information risk, including threat event frequency, vulnerability, and loss.
- A computational engine that derives risk by mathematically simulating the relationships between the measured factors.
- A simulation model that allows us to apply the taxonomy, measurement method, and computational engine to build and analyze risk scenarios of virtually any size or complexity.

EMV model

Expected monetary value

Expected monetary value (EMV) is a statistical technique in risk management that is used to quantify the risks, which in turn, assists the project manager to calculate the contingency reserve.

Expected monetary value analysis is a statistical concept that calculates the average outcomes when the future includes the scenarios that may or may not happen.”

Therefore, you can say:

- It helps in calculating the amount required to manage all identified risks.
- It helps in selecting the choice which involves less money to manage the risks.

You must have the probability, and the impact should it occur to calculate the expected monetary value of an event.

Once you calculate this data, you will multiply the probability by the impact, and the result will be the expected monetary value.

Expected Monetary Value (EMV) = Probability * Impact

Methodology

Since, we are using the Incremental SDLC Model thus our methodology will be including all the phases of that model.

- System Feasibility: We will be analyzing the feasibility of our product that whether it will be implementable or not. This phase has already been completed during the title analysis.
- Software Plans & Requirements: During this phase we analyzed all the requirements and planned the development cycle.
- Product Design: We will be developing zero Level DFD in this phase to know what modules are needed for this product.
- Detailed Design: Here we will work on Level 1 DFD to show sub modules and implementable functions. We will be also working on developing the required Use Case diagram.

- Code: This will be our main phase which will be our implementation phase where we will code all the modules. Here we will also do the unit testing.
- Integration: This phase will aim at making the product out of the modules i.e. we will be merging the modules.
- Implementation: This will be our system testing phase. We will test all the merged modules. This will act as level one testing for our product.
- Operations & Maintenance: This is our last phase where will work towards achieving feedback and further improvements will be done accordingly.

Steps

- Create a module for main menu interface along with the listing of different models.
- Create independent modules for calculation of risk rating based on the frameworks upon the collection matrices.
- Create a module for comparative study and mean risk rating.
- Club the Modules using Bottom Up approach.

System Requirements

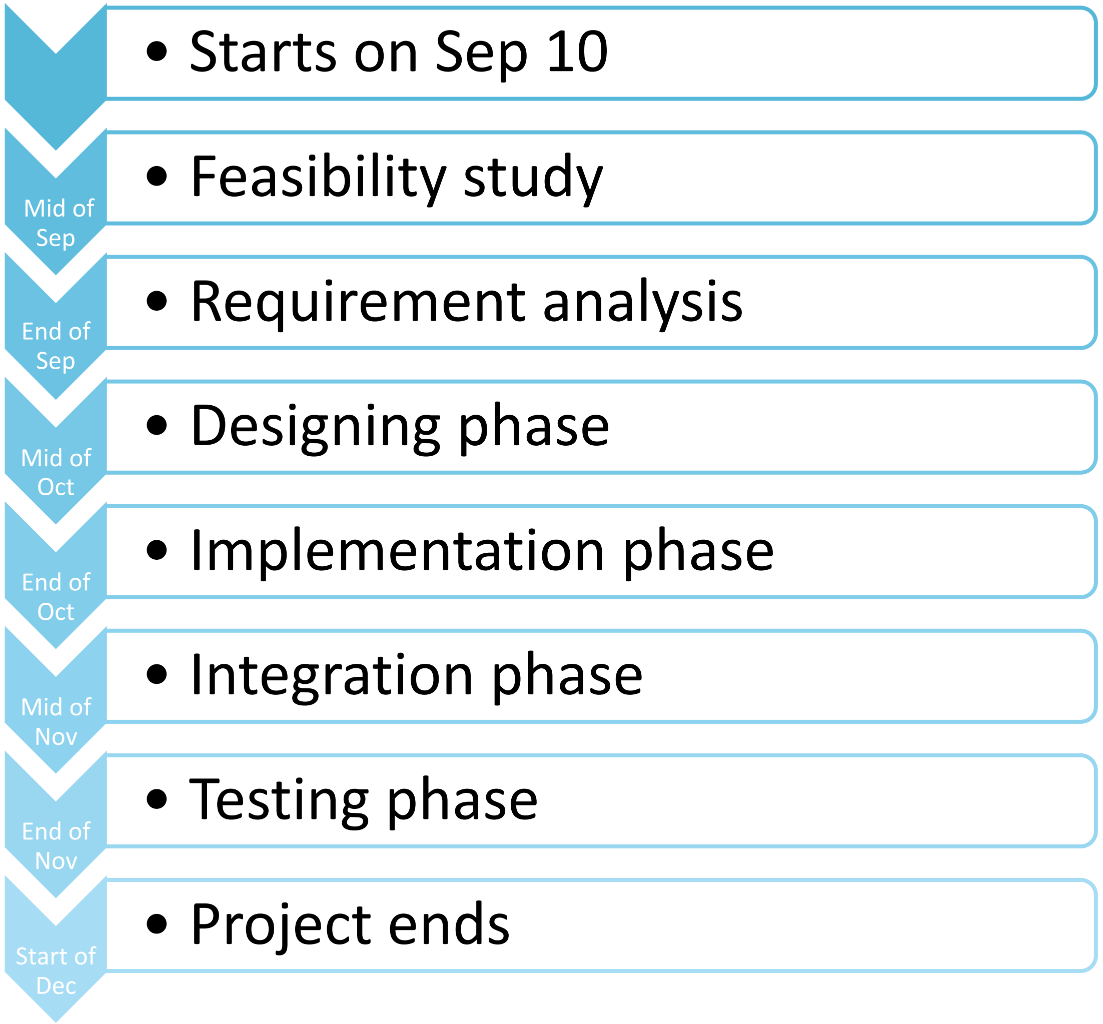
Hardware

- 8 GB Ram
- Intel Core i5 64 bit Processor
- Keyboard
- Mouse
- Printer

Software

- Windows 10 1807 64 bit
- Visual Studio Code
- Microsoft Visio
- Microsoft Office Suite
- Gcc Compiler

Schedule



	• Starts on Sep 10
Mid of Sep	• Feasibility study
End of Sep	• Requirement analysis
Mid of Oct	• Designing phase
End of Oct	• Implementation phase
Mid of Nov	• Integration phase
End of Nov	• Testing phase
Start of Dec	• Project ends

References

[1] ISO/IEC 27001:2013(E) Information technology – Security techniques – Information security management systems – Requirements.

[2] ISO/IEC 27002:2013 Information technology – Security techniques – Code of practice for information security controls.

[3] ISO 19011:2018 Guidelines for auditing management systems.

[4] ISO 31000:2018 Risk management – Guidelines.

[5] ISO 22301:2012 Societal security -- Business continuity management systems – Requirements

[6] ISO 27005:2018 Information technology -- Security techniques -- Information security risk management.

[7] IEC 31010:2019 Risk management -- Risk assessment techniques

[8] ISO/IEC 27017:2015 Information technology - Security techniques -- Code of practice for information security controls based on ISO/IEC 27002 for cloud services

THANK YOU ☺