# MENACE RECALL

A

Project Report

submitted in partial fulfilment of the

requirements for the award of the degree of

BACHELOR OF TECHNOLOGY

in

COMPUTER SCIENCE

Specialization in

Cyber Security & Forensics

By :

| Name | Roll No |
|---|---|
| Manik Garg | R134216076 |
| Kritika Sharma | R134216072 |
| Vikalp | R134216150 |

Under the guidance of

Dr. Susheela Dahiya
Assistant Professor (S.G.)
Department of Computer Application

Department of Systemics
School of Computer Science
UNIVERSITY OF PETROLEUM AND ENERGY STUDIES
Bidholi, Via Prem Nagar, Dehradun, Uttarakhand 2019-20

UPES

UNIVERSITY WITH A PURPOSE

# CANDIDATES DECLARATION

I/We hereby certify that the project work entitled Menace Recall in partial fulfilment of the requirements for the award of the Degree of Bachelor of Technology in Computer Science And Engineering with Specialization in Cyber Security & Forensics and submitted to the Department of Systemics at School of Computer Science, University of Petroleum And Energy Studies, Dehradun, is an authentic record of my/ our work carried out during a period from August, 2019 to November, 2019 under the supervision of Dr. Susheela Dahiya, Assistant Professor (S.G.), Department of Computer Application.

The matter presented in this project has not been submitted by us for the award of any other degree of this or any other University.

| | | |
|---|---|---|
| (Manik Garg) | (Kritika Sharma) | (Vikalp) |
| Roll No. R134216076 | Roll No. R134216072 | Roll No. R134216150 |

This is to certify that the above statement made by the candidate is correct to the best of my knowledge.

(Date: 25 November 2019)

(Dr. Susheela Dahiya)
Project Guide

Dr. Neelu Jyothi Ahuja

Head
Department of Systemics
School of Computer Science
University of Petroleum And Energy Studies
Dehradun - 248007 (Uttarakhand)

# ACKNOWLEDGEMENT

We wish to express our deep gratitude to our guide Dr. Susheela Dahiya, for all advice, encouragement and constant support she has given us throughout our project work. This work would not have been possible without her support and valuable suggestions.

We sincerely thank to our Head of the Department, Dr. Neelu Jyothi Ahuja, for her great support in doing our project Menace Recall at SoCS.

We are also grateful to Dr. Manish Prateek Professor and Director SoCS and Dr. Kamal Bansal Dean CoES, UPES for giving us the necessary facilities to carry out our project work successfully.

We would like to thank all our friends for their help and constructive criticism during our project work. Finally we have no words to express our sincere gratitude to our parents who have shown us this world and for every support they have given us.

| | | | |
|---|---|---|---|
| Name | Manik Garg | Kritika Sharma | Vikalp |
| Roll No. | R134216076 | R134216072 | R134216150 |

# 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. We will be using incremental process model to determine the life cycle of our project. Our project will consist of independent modules of each framework and one cumulative frontend system. We have chosen this model as it provides flexibility to us for adding further specification in form of independent modules. One more reason because of which we have chosen this model is that it will help us in getting at-least some workable modules before our next deadline.

**Keywords:** Security, Risk Assessment, CIA, Data, Risk, Threat, Vulnerability.

# TABLE OF CONTENTS

## Contents

# LIST OF TABLES

## List of Tables

# LIST OF FIGURES

## List of Figures

# 1 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.

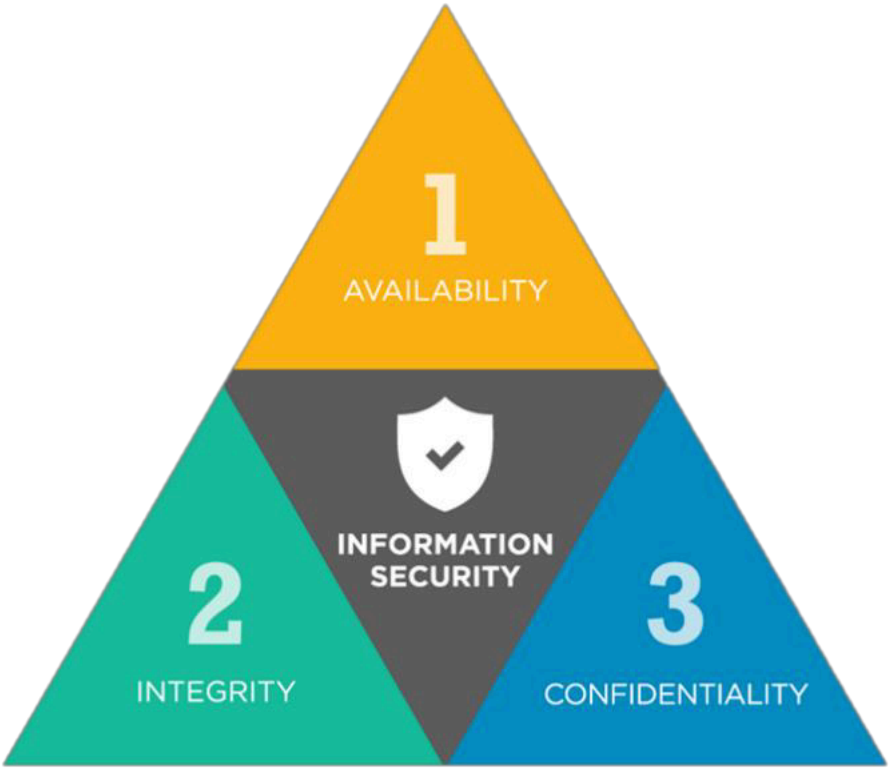


Figure 1: CIA Triad

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.

## 1.1 Risk Management

Risk management refers to the identification of vulnerabilities and threats associated with the information and thus deciding the countermeasures that can be applied to minimize the impacts of the risks associated with the information. Risk Management is a recurring process since the information and the environment is very dynamic and changes very rapidly, thus risk management is to be performed after a fixed interval or even after any significant change so that when the vulnerabilities or the threats associated with them changes, the risk will also change thus, the risk management strategy needs to be updated or completely changed.[4]

### 1.1.1 Factors of Risk:

a) Impact: This refers to the amount of damage that will be incurred if the risk materializes and the threat succeeds in exploiting the vulnerability.

b) Likelihood: This refers to the frequency of the occurring of that risk in a certain period of time.

### 1.1.2 Phases of Risk Management Process:

There are 5 key steps in the complete risk management process.[4]

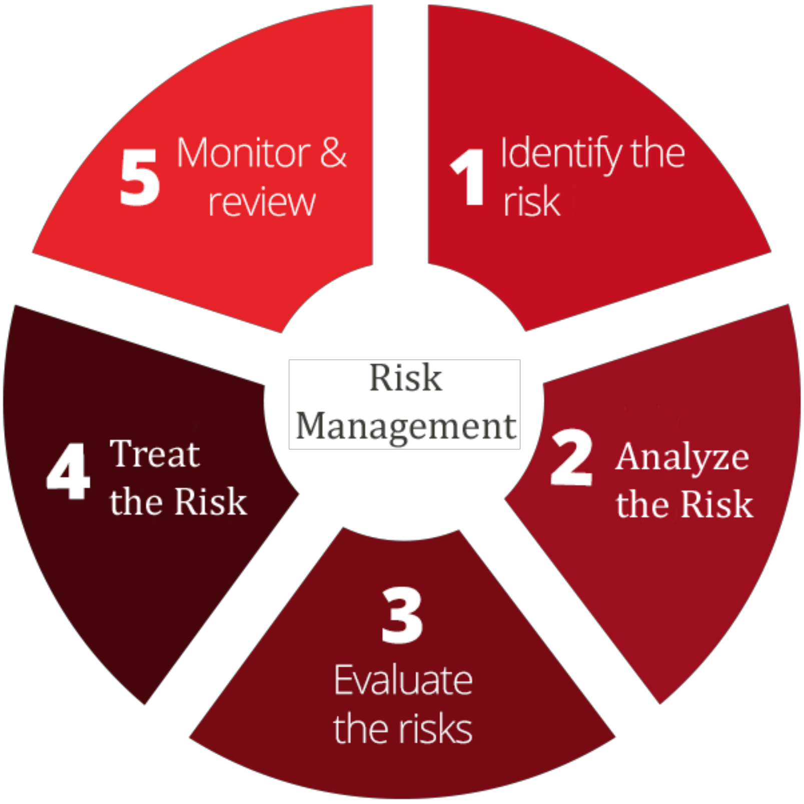


Figure 2: Risk Management

a) Risk Identification: In this phase the risks associated the organization are identified and listed in form of a risk register containing the vulnerability, threat, risk, risk rating, etc. This phase involves some basic processes such as asset identification, asset classification, threat identification, etc.

b) Risk Analysis: In this phase the likelihood and the impact of the risks are determined and added to the risk register. Also, the nature of the risk and its consequence on the business is calculated.

c) Risk Evaluation: In this phase the likelihood and impact are combined to assign a risk ranking. This ranking helps in risk prioritization and deciding what action to perform upon a risk.

d) Risk Treatment: In this phase the controls are deployed based upon the risk treatment option selected. The risks are treated according to their rankings set in the previous phase.

e) Review & Monitor: During this phase we monitor and track the risks from the risk register. Since, risks are likely to reoccur thus they should be monitored regularly.[5]

### 1.1.3 Risk Treatment Methods:

There are 4 ways of treating a risk: -

a) Risk Avoidance: This refers to using an alternate way to avoid that risk or dropping the whole process altogether which is linked to that risk. This methodology is used when you have secondary processes or approaches.

b) Risk Acceptance: This methodology is used where the cost of implementing a control to treat a risk is more than the actual cost incurred if the risk materializes. We basically accept the risk and no action is performed for that risk.

c) Risk Mitigation: This is actually where we deploy controls to treat the risk or reduce its impact to the best possible level. e.g. IDS, IPS, Firewall, etc.

d) Risk Transfer: In this methodology the impact of the risk is transferred to someone else remove the loss from the parent organization. e.g. insurance, outsourcing, etc.

**Note that in case of Risk Mitigation it is not possible to reduce the impact of risk completely. Thus, there is always some amount of risk left that has to further treated in form of avoidance, acceptance or transfer. This small amount of risk that is left is known as Residual Risk.[4]

### 1.1.4 Types of controls:

There are three basic types of controls deployed for risk management:

a) Preventive Controls: This type of controls are placed to prevent errors from occurring in the very first place. These controls are implemented beforehand as part of the risk management process. E.g. Backing up of data.

b) Detective Controls: These controls are deployed to find errors after they have occurred. They are used for checking policy efficiency and protecting assets. E.g. Review processes.

c) Corrective Controls: These are the controls that correct the errors detected by the detective controls. E.g. Reporting an issue.[4]

# 2 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 CIA triad.

[3] ISO 19011 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] ISO 27005 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] ISO 31010 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.

# 3 Problem Statement

Create a tool for risk assessment along with the functionality to use various models from the quantitative risk assessment category. Also, provide a functionality to calculate the average risk value from these models using root mean square method.

# 4 Objective

To create tool using different technologies for cumulative risk assessment: -

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

# 5 Design 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 analysing 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 analysed 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.

*This will mark the end of requirement verification

Detailed Design: - Here we will work on Level 1 DFD to show sub modules and implementable functions. We will also worke on developing the 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: -

1. Create a module for main menu interface along with the listing of different models.

2. Create independent modules for calculation of risk rating based on the frameworks upon the collection matrices.

3. Create a module for comparative study and mean risk rating.

4. Club the Modules using Bottom Up approach.

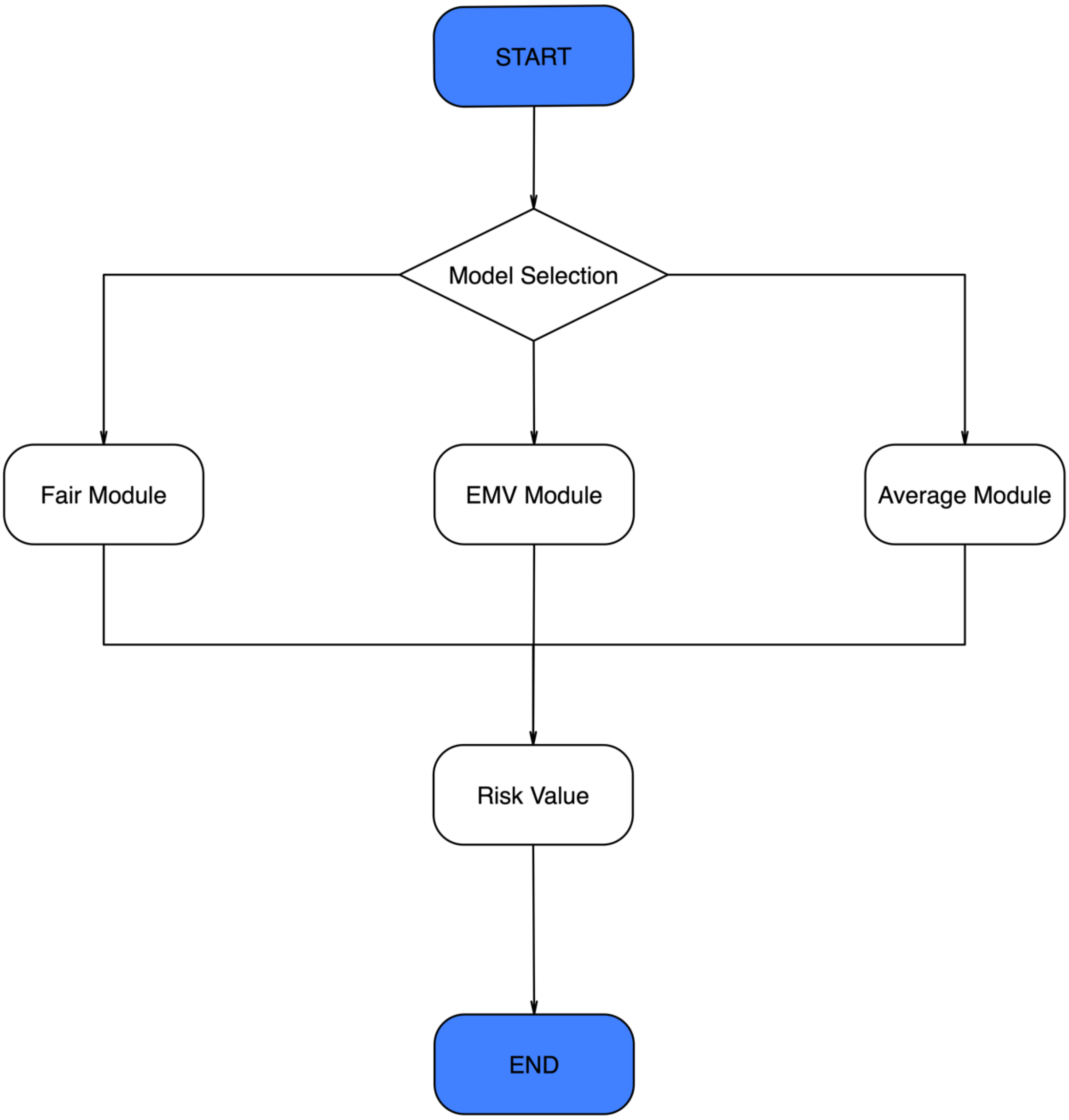


Figure 3: Flow Chart

The below shown is the use case diagram for the tool showing the 4 modules and the only actor using the tool: -

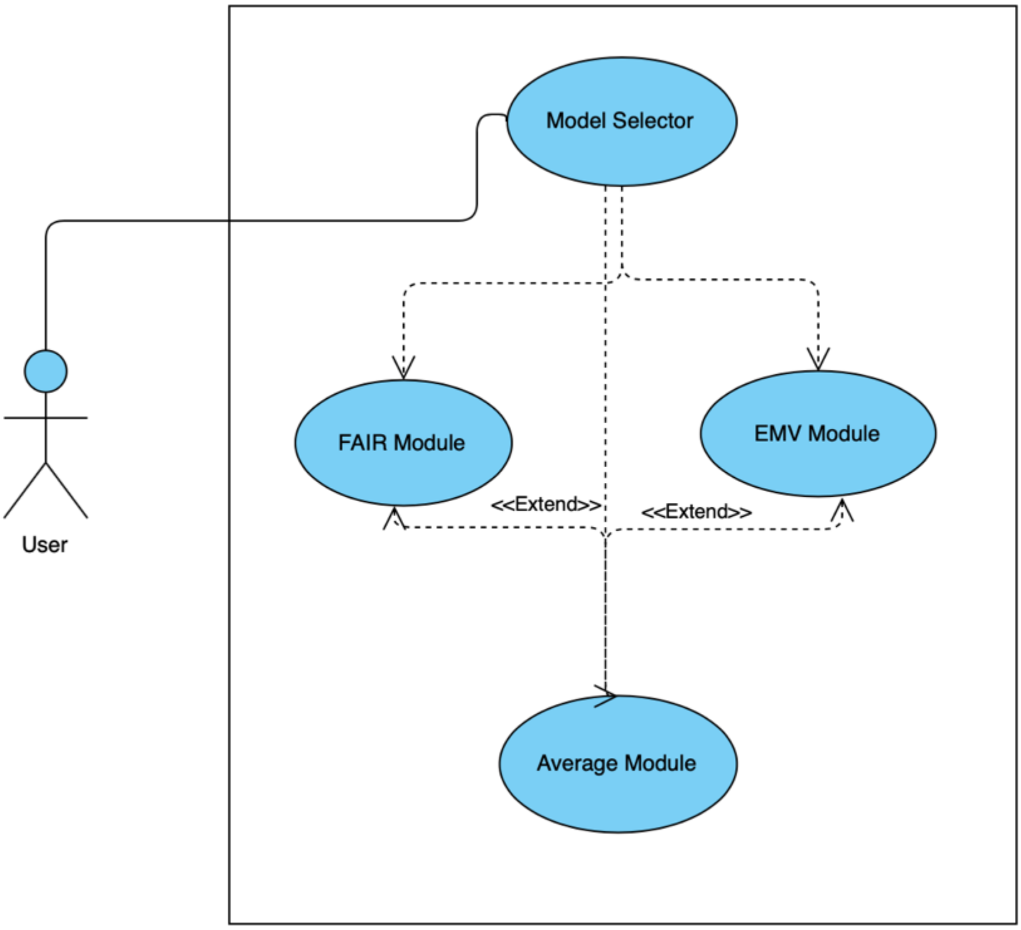


Figure 4: Use Case Diagram

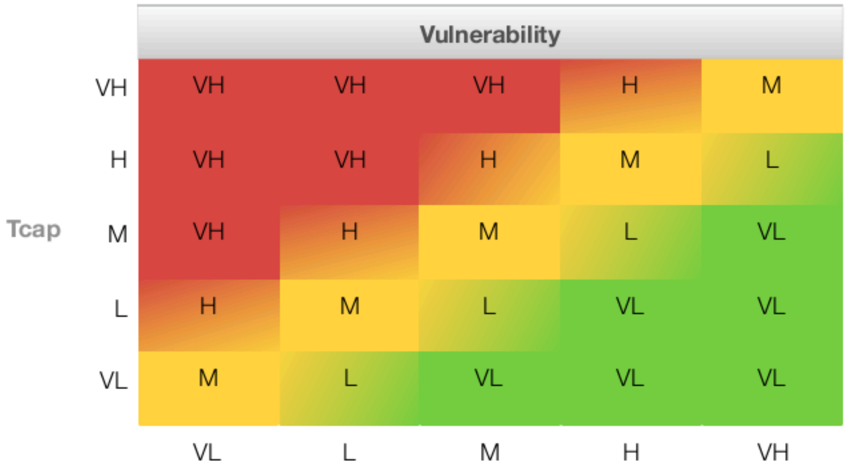
# 6 Implementation

The FAIR and EMV models are given as option on the main interface. Once the user selects the model a new window based upon the parameters of the model is opened.

In case of FAIR model the inputs that are passed serve as matrix values to derive further ratings and finally the risk factor is provided to the user based on the hardcoded matrix values.

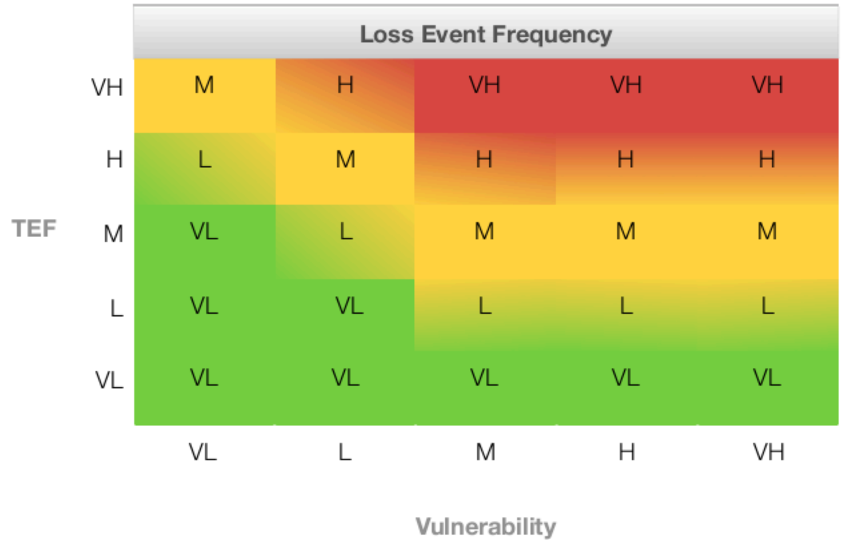
## 6.1 Pseudocode

The model calculator is programmed by hardcoding the derivation matrices in form of index values where 0 represents Very low, 1 represents Low and so on. Initially 4 inputs are taken in the FAIR model calculator and these 4 inputs use the hardcoded matrices to derive the remaining 3 values.



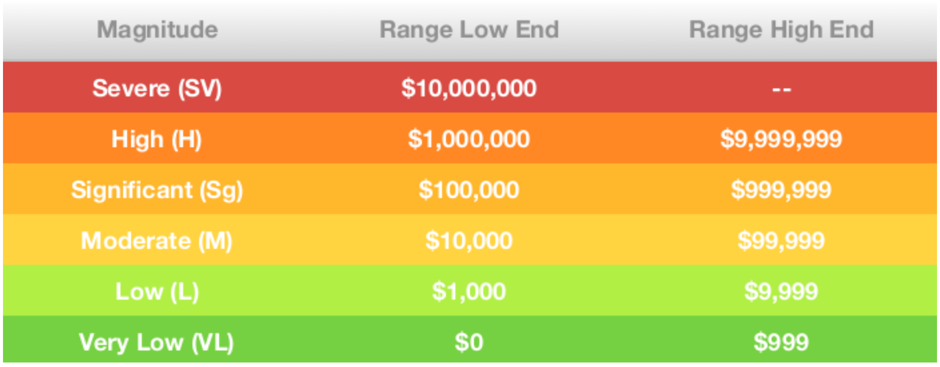
| | | Vulnerability | | | | |
|---|---|---|---|---|---|---|
| | VH | VH | VH | VH | H | M |
| | H | VH | VH | H | M | L |
| Tcap | M | VH | H | M | L | VL |
| | L | H | M | L | VL | VL |
| | VL | M | L | VL | VL | VL |
| | | VL | L | M | H | VH |

Table 1: Threat Capability vs Control Strength



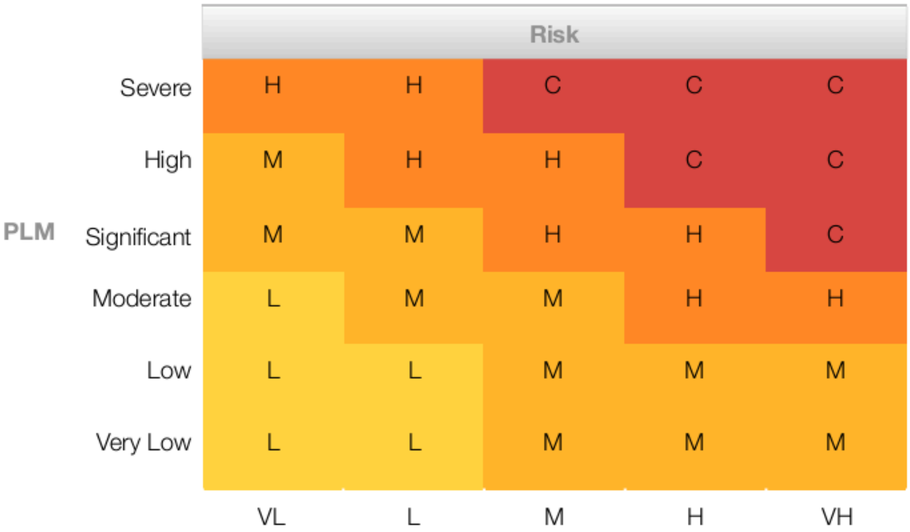
| | | Loss Event Frequency | | | | |
|---|---|---|---|---|---|---|
| | VH | M | H | VH | VH | VH |
| | H | L | M | H | H | H |
| TEF | M | VL | L | M | M | M |
| | L | VL | VL | L | L | L |
| | VL | VL | VL | VL | VL | VL |
| | | VL | L | M | H | VH |
| | | | | Vulnerability | | |

Table 2: Threat Event Frequency vs Vulnerability



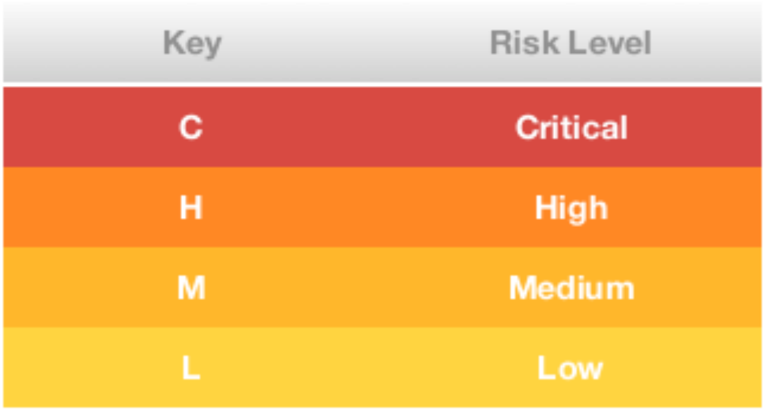
| Magnitude | Range Low End | Range High End |
|---|---|---|
| Severe (SV) | $10,000,000 | -- |
| High (H) | $1,000,000 | $9,999,999 |
| Significant (Sg) | $100,000 | $999,999 |
| Moderate (M) | $10,000 | $99,999 |
| Low (L) | $1,000 | $9,999 |
| Very Low (VL) | $0 | $999 |

Table 3: Probable Loss Magnitude



| | | Risk | | | | |
|---|---|---|---|---|---|---|
| | Severe | H | H | C | C | C |
| | High | M | H | H | C | C |
| PLM | Significant | M | M | H | H | C |
| | Moderate | L | M | M | H | H |
| | Low | L | L | M | M | M |
| | Very Low | L | L | M | M | M |
| | | VL | L | M | H | VH |

Table 4: Probable Loss Magnitude vs Loss Event Frequency



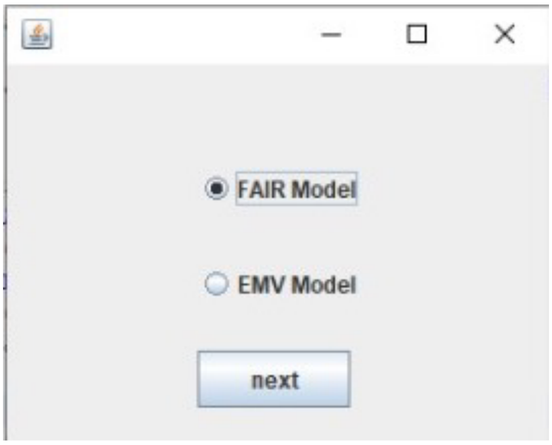
| Key | Risk Level |
|---|---|
| C | Critical |
| H | High |
| M | Medium |
| L | Low |

Table 5: Risk

The above shown matrices are used to derive and calculate the values.

## 6.2 Output Screen

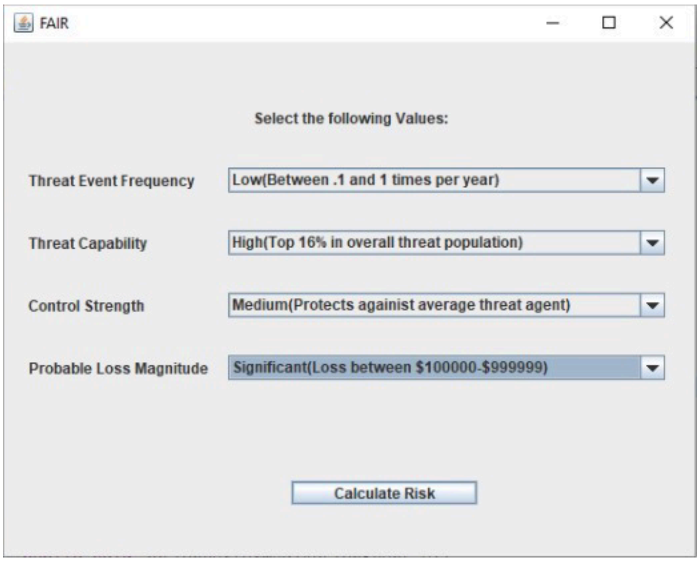
The program is made in such a way that post inputs it calculates the risk basis on the equations laid by the model using the java backend function..



● FAIR Model

○ EMV Model

Figure 3: Screen 1



Select the following Values:

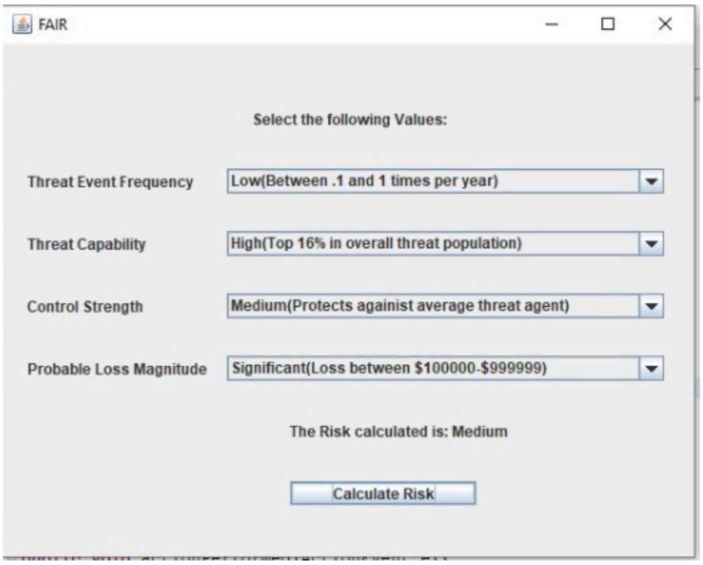
Threat Event Frequency: Low(Between .1 and 1 times per year)

Threat Capability: High(Top 16% in overall threat population)

Control Strength: Medium(Protects agaiinst average threat agent)

Probable Loss Magnitude: Significant(Loss between $100000-$999999)

Figure 4: Screen 2



Select the following Values:

Threat Event Frequency: Low(Between .1 and 1 times per year)

Threat Capability: High(Top 16% in overall threat population)

Control Strength: Medium(Protects agaiinst average threat agent)

Probable Loss Magnitude: Significant(Loss between $100000-$999999)

The Risk calculated is: Medium

Figure 5: Screen 3

## 6.3 Result Analysis

The results show that the FAIR model is a great model to derive the risk rating for any organization for any scenario . Quantitative risk assessment models are a better way to obtain statistical facts about a risk program and thus take implement better strategies to deal with the risks.

EMV model however works for a single asset and cannot provide organization based risk rating. Also, it depends on very less factors as compared to FAIR thus, is less accurate is used for top level analysis of risk related to a certain department.

# 7 Conclusion and Future Scope

The project is a great tool for auditors and implementors who aim at implementing ISO 27001 in an organization. This tool automates the manual risk calculation process and is easy to use. Also, risk assessment tools need to have more and more models in it and this tools satisfies this need. The main audience that will be benefited by this tool is students who are in the learning stage. They can use this tools to implement their theoretical knowledge practically.

The future scope of this project is to add more models from the quantitative risk assessment category in this project. Also, to automate the comparative study module. A new functionality can be added to keep check on the previous risk assessments done . The GUI can be improved to an extreme level and features like graph creation can be added.

Furthermore, this tool can also club qualitative risk assessment models and be compatible with their input and output requirements . Thus, can become a full stack risk assessment software for enterprise level usage.

# 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.

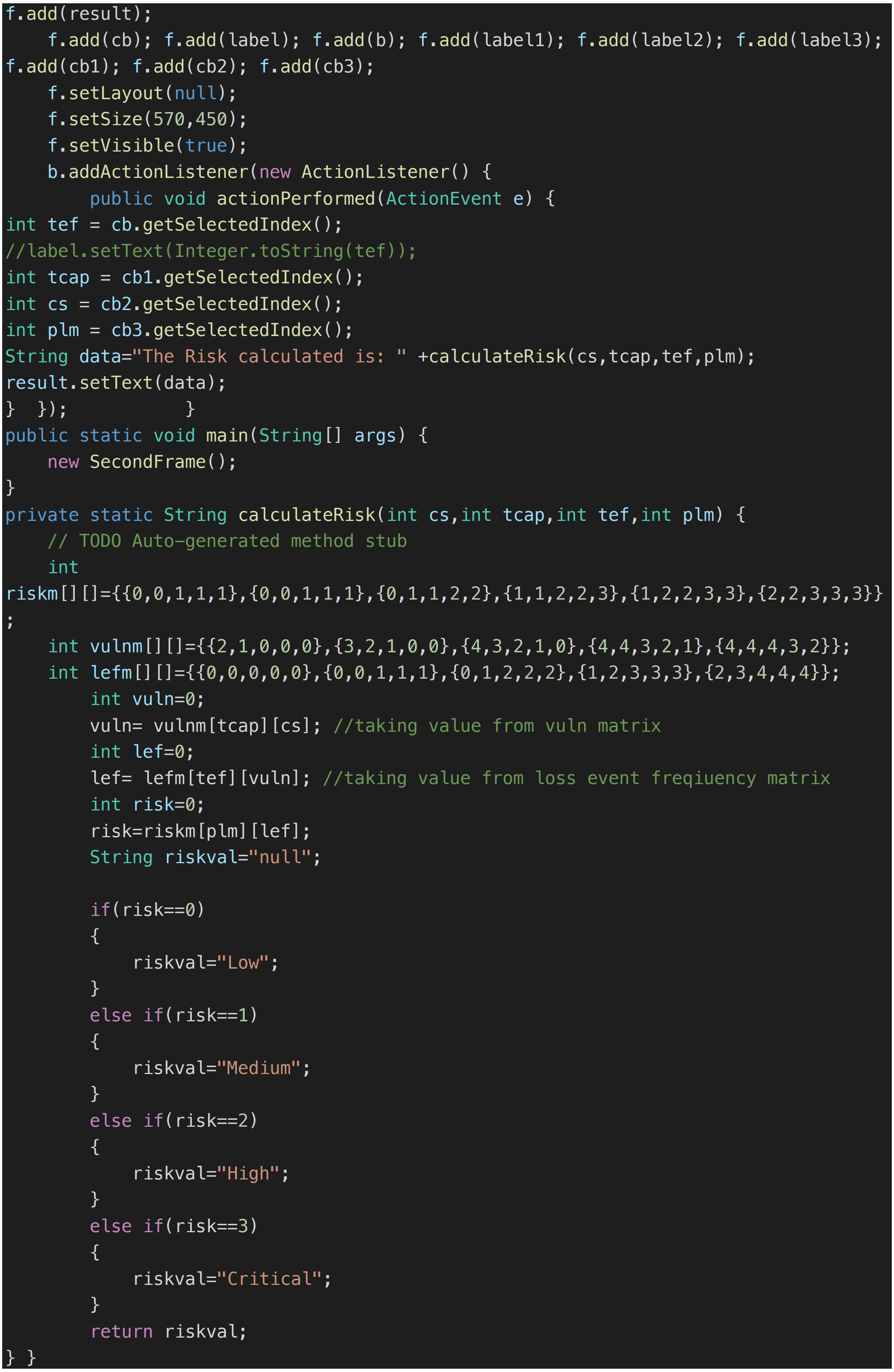
# A APPENDIX I PROJECT CODE

**GUI.java**

```java
import javax.swing.*;
import java.awt.event.*;
class first extends JFrame implements ActionListener{
JRadioButton rb1,rb2,rb3;
private JFrame f = new JFrame("Select the Risk Assessment Model");
JButton b;
first(){
f.setDefaultCloseOperation(JFrame.HIDE_ON_CLOSE);
rb1=new JRadioButton("FAIR Model");
rb1.setBounds(100,50,100,30);
rb2=new JRadioButton("EMV Model");
rb2.setBounds(100,100,100,30);
rb3=new JRadioButton("Hybrid");
rb3.setBounds(100,150,100,30);
ButtonGroup bg=new ButtonGroup();
bg.add(rb1);bg.add(rb2);bg.add(rb3);
b=new JButton("next");
b.setBounds(100,180,80,30);
b.addActionListener(this);
add(rb1);add(rb2);add(rb3);add(b);
setSize(300,300);
setLayout(null);
setVisible(true);
}
public void actionPerformed(ActionEvent e){
if(rb1.isSelected()){
f.dispose();
new SecondFrame();
}
if(rb2.isSelected()){
f.dispose();
new ThirdFrame();
}
if(rb3.isSelected()){
f.dispose();
new HybridFrame();
}
}
public static void main(String args[]){
new first();
}}
```

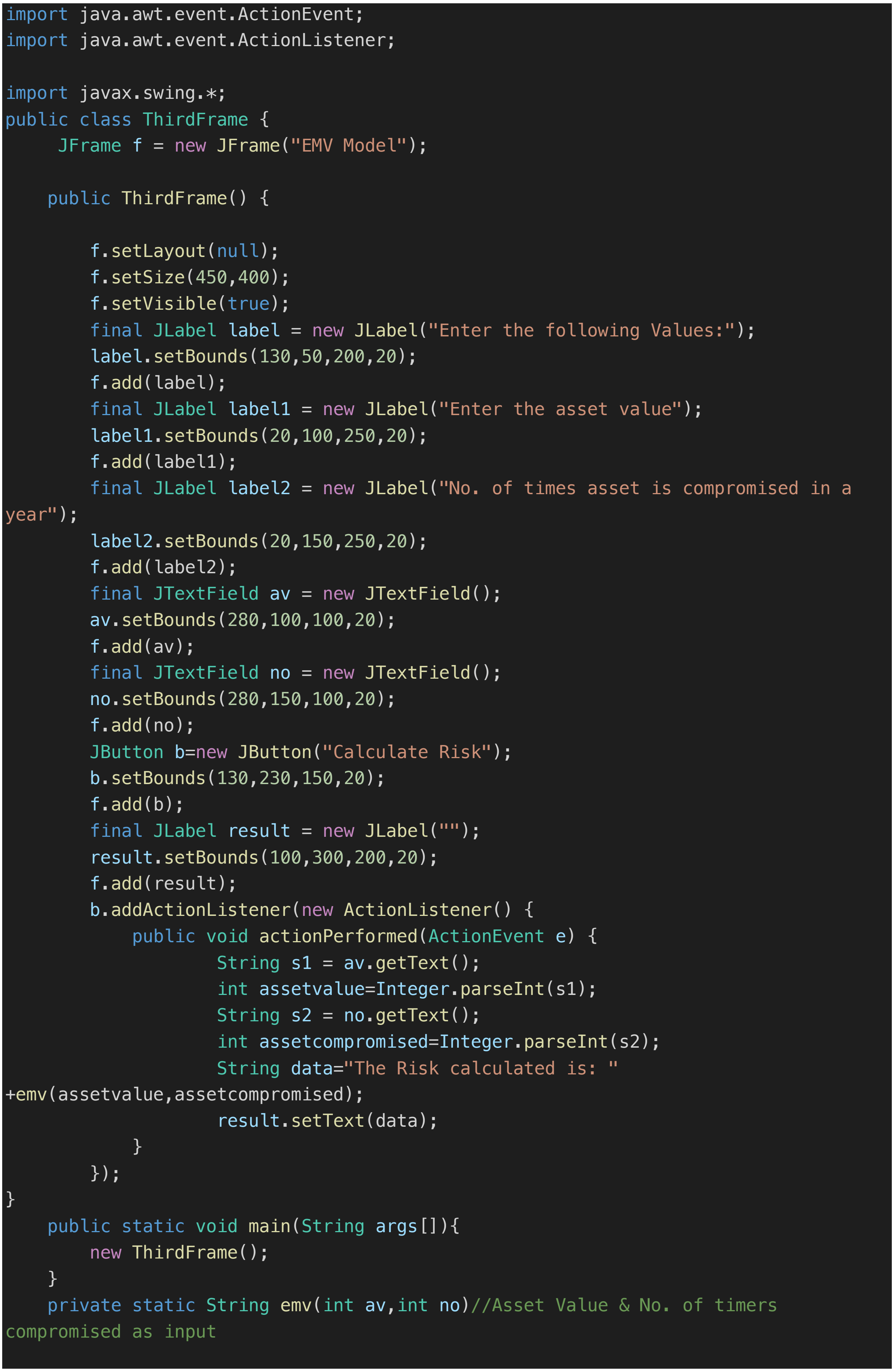
## Second Frame.java

```
import javax.print.DocFlavor.STRING;
import javax.swing.*;
import java.awt.event.*;
public class SecondFrame {
JFrame f;
SecondFrame(){
    f=new JFrame("FAIR");
    final JLabel labell = new JLabel("Select the following Values:");
    labell.setBounds(200,50,200,20);
    f.add(labell);
    final JLabel label = new JLabel("Threat Event Frequency");
    label.setBounds(20,100,200,20);
    JLabel label1 = new JLabel("Threat Capability");
    label1.setBounds(20,150,200,20);
    JLabel label2 = new JLabel("Control Strength");
    label2.setBounds(20,200,200,20);
    JLabel label3 = new JLabel("Probable Loss Magnitude");
    label3.setBounds(20,250,200,20);


    String TEF[]={"Very Low(less than .1 times per year)","Low(Between .1 and 1
times per year)",
            "Medium(Between 1 and 10 times per year)","High(Between 10 and 100
times per year)",
            "Very High(more than 100 times per year)"};
    final JComboBox cb=new JComboBox(TEF);
    cb.setBounds(180,100,350,20);
    String TCap[]={"Very Low(Bottom 2% in overall threat population)"
            ,"Low(Bottom 16% in overall threat population)",
            "Medium(Between bottom 16% and top 16% in overall threat population)",
            "High(Top 16% in overall threat population)",
            "Very High(Top 2% in overall threat population)"};
    final JComboBox cb1=new JComboBox(TCap);
    cb1.setBounds(180, 150,350,20);
    String CS[]={"Very Low(Only protects againist bottom 2% of overall threat)"
            ,"Low(Only protects againist bottom 16% of overall threat)",
            "Medium(Protects againist average threat agent)",
            "High(Protects againist all but top 16% of overall threat)",
            "Very High(Protects againist all but top 2% of overall threat)"};
    final JComboBox cb2=new JComboBox(CS);
    cb2.setBounds(180, 200,350,20);
    String PLM[]={"Very Low(Loss between $0-$999)",
            "Low(Loss between $1000-$9999)",
            "Moderate(Loss between $10000-$99999)",
            "Significant(Loss between $100000-$999999)",
            "High(Loss between $1000000-$9999999)","Severe(Loss more than or equal
to 10000000"};
    final JComboBox cb3=new JComboBox(PLM);
    cb3.setBounds(180, 250,350,20);
    JButton b=new JButton("Calculate Risk");
    b.setBounds(230,350,150,20);
    final JLabel result = new JLabel("");
    result.setBounds(230,300,200,20);
```



```
f.add(result);
    f.add(cb); f.add(label); f.add(b); f.add(label1); f.add(label2); f.add(label3);
f.add(cb1); f.add(cb2); f.add(cb3);
    f.setLayout(null);
    f.setSize(570,450);
    f.setVisible(true);
    b.addActionListener(new ActionListener() {
        public void actionPerformed(ActionEvent e) {
int tef = cb.getSelectedIndex();
//label.setText(Integer.toString(tef));
int tcap = cb1.getSelectedIndex();
int cs = cb2.getSelectedIndex();
int plm = cb3.getSelectedIndex();
String data="The Risk calculated is: " +calculateRisk(cs,tcap,tef,plm);
result.setText(data);
}  });           }
public static void main(String[] args) {
    new SecondFrame();
}
private static String calculateRisk(int cs,int tcap,int tef,int plm) {
    // TODO Auto-generated method stub
    int
riskm[][]={{0,0,1,1,1},{0,0,1,1,1},{0,1,1,2,2},{1,1,2,2,3},{1,2,2,3,3},{2,2,3,3,3}}
;
    int vulnm[][]={{2,1,0,0,0},{3,2,1,0,0},{4,3,2,1,0},{4,4,3,2,1},{4,4,4,3,2}};
    int lefm[][]={{0,0,0,0,0},{0,0,1,1,1},{0,1,2,2,2},{1,2,3,3,3},{2,3,4,4,4}};
        int vuln=0;
        vuln= vulnm[tcap][cs]; //taking value from vuln matrix
        int lef=0;
        lef= lefm[tef][vuln]; //taking value from loss event freqiuency matrix
        int risk=0;
        risk=riskm[plm][lef];
        String riskval="null";

        if(risk==0)
        {
            riskval="Low";
        }
        else if(risk==1)
        {
            riskval="Medium";
        }
        else if(risk==2)
        {
            riskval="High";
        }
        else if(risk==3)
        {
            riskval="Critical";
        }
        return riskval;
} }
```

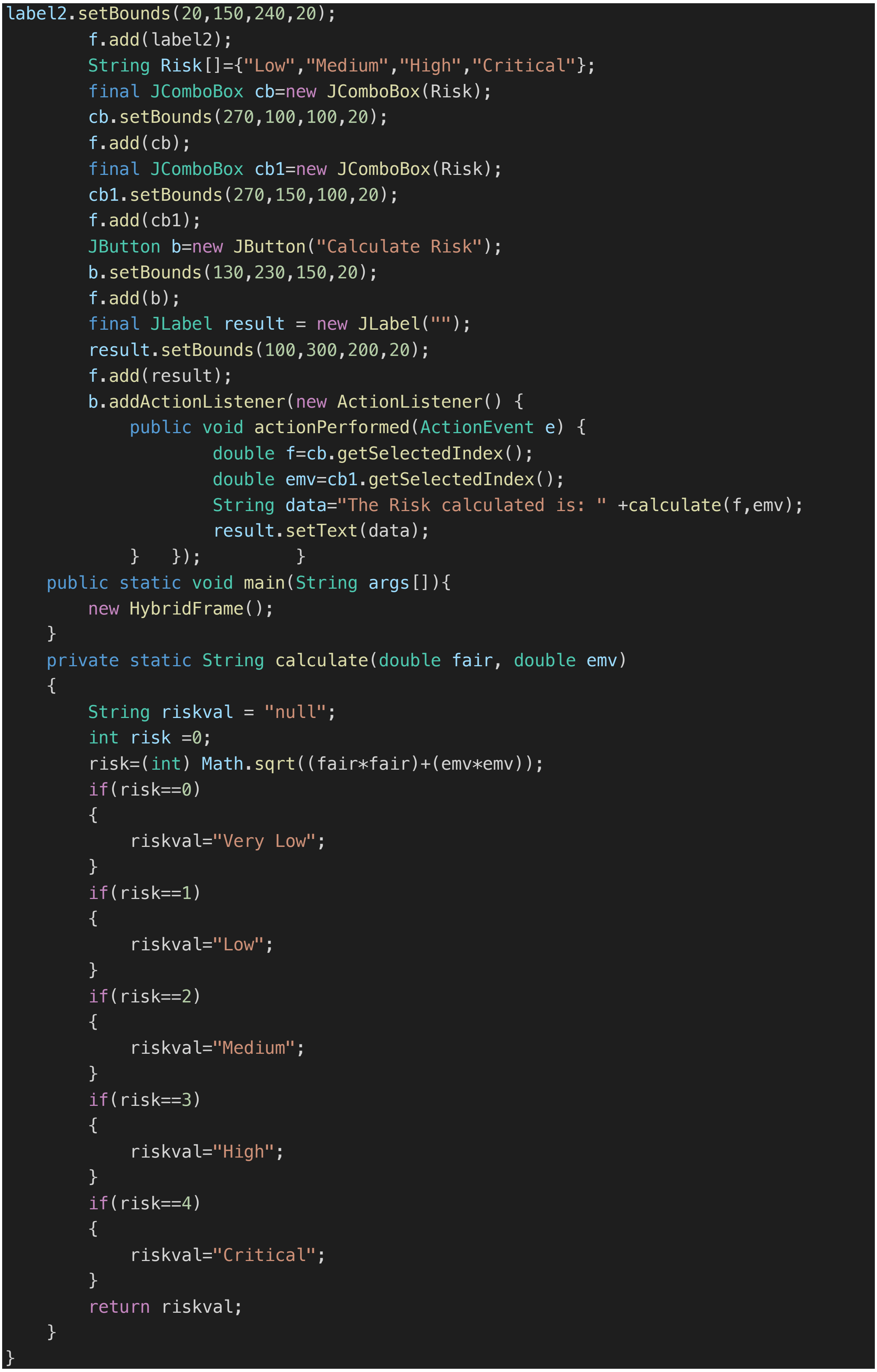
**Third Frame.java**



```java
import java.awt.event.ActionEvent;
import java.awt.event.ActionListener;

import javax.swing.*;
public class ThirdFrame {
     JFrame f = new JFrame("EMV Model");

    public ThirdFrame() {

        f.setLayout(null);
        f.setSize(450,400);
        f.setVisible(true);
        final JLabel label = new JLabel("Enter the following Values:");
        label.setBounds(130,50,200,20);
        f.add(label);
        final JLabel label1 = new JLabel("Enter the asset value");
        label1.setBounds(20,100,250,20);
        f.add(label1);
        final JLabel label2 = new JLabel("No. of times asset is compromised in a 
year");
        label2.setBounds(20,150,250,20);
        f.add(label2);
        final JTextField av = new JTextField();
        av.setBounds(280,100,100,20);
        f.add(av);
        final JTextField no = new JTextField();
        no.setBounds(280,150,100,20);
        f.add(no);
        JButton b=new JButton("Calculate Risk");
        b.setBounds(130,230,150,20);
        f.add(b);
        final JLabel result = new JLabel("");
        result.setBounds(100,300,200,20);
        f.add(result);
        b.addActionListener(new ActionListener() {
            public void actionPerformed(ActionEvent e) {
                    String s1 = av.getText();
                    int assetvalue=Integer.parseInt(s1);
                    String s2 = no.getText();
                    int assetcompromised=Integer.parseInt(s2);
                    String data="The Risk calculated is: " 
+emv(assetvalue,assetcompromised);
                    result.setText(data);
            }
        });
}
    public static void main(String args[]){
        new ThirdFrame();
    }
    private static String emv(int av,int no)//Asset Value & No. of timers 
compromised as input
{
        int emv=0;
        emv= av*no;

        int risk=0;
        String riskval="null";
        if(emv>=0&&emv<=999)
        {
            risk=0;
            riskval="Low";
        }
        else if(emv>999&&emv<=9999)
        {
            risk=1;
            riskval="Medium";
        }
        else if(emv>9999&&emv<=99999)
        {
            risk=2;
            riskval="High";
        }
        else if(emv>99999)
        {
            risk=3;
            riskval="Critical";
        }

        return riskval;
    }
}
```

**Hybrid.java**

```
import java.awt.event.ActionEvent;
import java.awt.event.ActionListener;

import javax.swing.*;
public class HybridFrame {
    JFrame f = new JFrame("Hybrid Model");
    public HybridFrame()
    {
        f.setLayout(null);
        f.setSize(400,400);
        f.setVisible(true);
        final JLabel label = new JLabel("Enter the following values:");
        label.setBounds(100,50,200,20);
        f.add(label);
        final JLabel label1 = new JLabel("Enter risk rating obtained from Fair
model");
        label1.setBounds(20,100,240,20);
        f.add(label1);
        final JLabel label2 = new JLabel("Enter risk rating obtained from EMV
model");
```



```
label2.setBounds(20,150,240,20);
        f.add(label2);
        String Risk[]={"Low","Medium","High","Critical"};
        final JComboBox cb=new JComboBox(Risk);
        cb.setBounds(270,100,100,20);
        f.add(cb);
        final JComboBox cb1=new JComboBox(Risk);
        cb1.setBounds(270,150,100,20);
        f.add(cb1);
        JButton b=new JButton("Calculate Risk");
        b.setBounds(130,230,150,20);
        f.add(b);
        final JLabel result = new JLabel("");
        result.setBounds(100,300,200,20);
        f.add(result);
        b.addActionListener(new ActionListener() {
            public void actionPerformed(ActionEvent e) {
                    double f=cb.getSelectedIndex();
                    double emv=cb1.getSelectedIndex();
                    String data="The Risk calculated is: " +calculate(f,emv);
                    result.setText(data);
            }   });         }
    public static void main(String args[]){
        new HybridFrame();
    }
    private static String calculate(double fair, double emv)
    {
        String riskval = "null";
        int risk =0;
        risk=(int) Math.sqrt((fair*fair)+(emv*emv));
        if(risk==0)
        {
            riskval="Very Low";
        }
        if(risk==1)
        {
            riskval="Low";
        }
        if(risk==2)
        {
            riskval="Medium";
        }
        if(risk==3)
        {
            riskval="High";
        }
        if(risk==4)
        {
            riskval="Critical";
        }
        return riskval;
    }
}
```