**ASSIGNMENT 2 FRONT SHEET**

|  |  |  |  |
| --- | --- | --- | --- |
| **Qualification** | **BTEC Level 5 HND Diploma in Computing** | | |
| **Unit number and title** | Unit 5: Security | | |
| **Submission date** | 22nd June, 2023 | **Date Received 1st submission** |  |
| **Re-submission Date** |  | **Date Received 2nd submission** |  |
| **Student Name** |  | **Student ID** |  |
| **Class** |  | **Assessor name** | Michael Omar |
| **Student declaration**  I certify that the assignment submission is entirely my own work and I fully understand the consequences of plagiarism. I understand that making a false declaration is a form of malpractice. | | | |
|  |  | **Student’s signature** |  |

**Grading grid**

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| P5 | P6 | P7 | P8 | M3 | M4 | M5 | D2 | D3 |
|  |  |  |  |  |  |  |  |  |

|  |  |  |
| --- | --- | --- |
| **❒ Summative Feedback: ❒ Resubmission Feedback:** | | |
| **Grade:** | **Assessor Signature:** | **Date:** |
| **Lecturer Signature:** | | |

# Table of contents

[Table of contents 2](#_Toc137539882)

[List of figures 3](#_Toc137539883)

[List of tables 3](#_Toc137539884)

[Introduction: 3](#_Toc137539885)

[P5 Discuss risk assessment procedures. 4](#_Toc137539886)

[Definition of a security risk: 4](#_Toc137539887)

[How to conduct risk assessment: 4](#_Toc137539888)

[Definition of assets: 5](#_Toc137539889)

[Definition of threats: 5](#_Toc137539890)

[Discussion on Threat identification procedures with examples: 5](#_Toc137539891)

[Explanation for the risk assessment and procedure: 5](#_Toc137539892)

[List of risk identification and steps: 5](#_Toc137539893)

[P6 Explain data protection processes and regulations as applicable to an organization. 5](#_Toc137539894)

[Data protection definition: 6](#_Toc137539895)

[Explanation for data protection process in an organization: 6](#_Toc137539896)

[The importance of data protection and security regulation. 6](#_Toc137539897)

[P7 Design and implement a security policy for an organization. 6](#_Toc137539898)

[Definition of a security policy and discussion. 6](#_Toc137539899)

[Definition of security policy: 6](#_Toc137539900)

[Discussion on policies: 6](#_Toc137539901)

[The example for each of the policies: 7](#_Toc137539902)

[The most and should that must exist while creating a policy. 8](#_Toc137539903)

[The three most common elements : 8](#_Toc137539904)

[Give the steps to design a policy 8](#_Toc137539905)

[P8 The main components of an organizational disaster recovery plan, justifying the reasons for inclusion. 9](#_Toc137539906)

[Discussion and explanation about business continuity 9](#_Toc137539907)

[The components of recovery plan 9](#_Toc137539908)

[All the steps required in disaster recovery process: 9](#_Toc137539909)

[The policies and procedures that are required for business continuity: 9](#_Toc137539910)

[Conclusion 9](#_Toc137539911)

[References 9](#_Toc137539912)

# List of figures

[Figure 1 Risk Assessment procedure 4](#_Toc137539913)

# List of tables

[Table 1 Policy Must and should 8](#_Toc137539914)

# Introduction:

AS an IT consultant specialist, working for a security consultant.

A manufacturing company “Wheelie good” in Ho Chi Min City making bicycle parts for export has called for the consultation and expertised of my company to propose a Security Policy for their organization, after reading stories in the media related to security breaches, etc. in organizations and their ramifications.

As part of mt tasks

In preparation for this presentation, I will prepare a report considering:

* The security risks faced by the company.
* How data protection regulations and ISO risk management standards apply to IT security.
* The potential impact that an IT security audit might have on the security of the organization.
* The responsibilities of employees and stakeholders in relation to security.

**Task 2**

Following your report:

* You will now design and implement a security policy
* While considering the components to be included in disaster recovery plan for Wheelie good, justify why you have included these components in your plan.

**Task 3**

In addition to your security policy, you will evaluate the proposed tools used within the policy and how they align with IT security. You will include sections on how to administer and implement these policies.

# P5 Discuss risk assessment procedures.

## Definition of a security risk:

## How to conduct risk assessment:

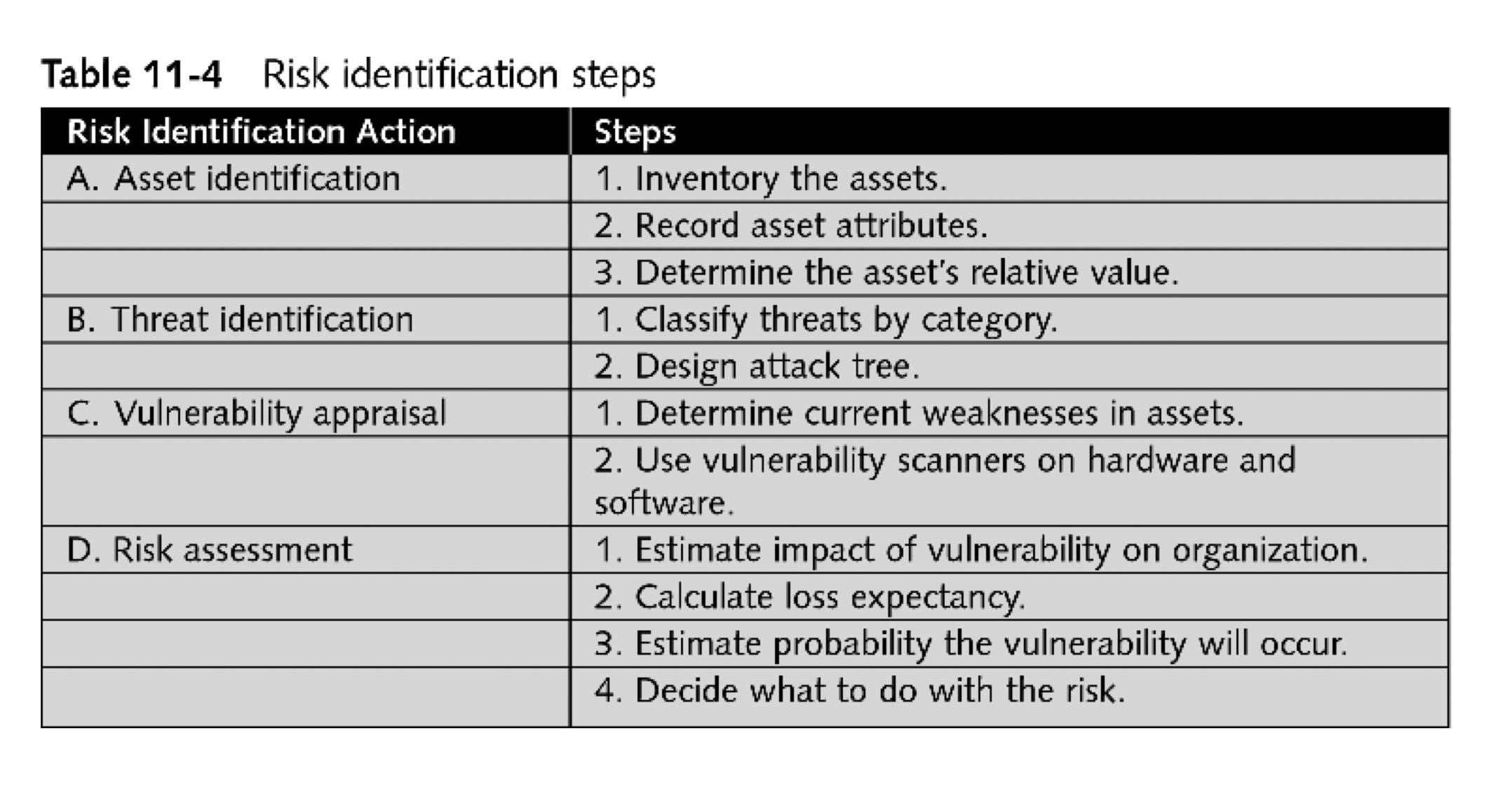


Figure 1 Risk Assessment procedure

## Definition of assets:

## Definition of threats:

## Discussion on Threat identification procedures with examples:

## Explanation for the risk assessment and procedure:

## List of risk identification and steps:

# P6 Explain data protection processes and regulations as applicable to an organization.

## Data protection definition:

## Explanation for data protection process in an organization:

## The importance of data protection and security regulation.

# P7 Design and implement a security policy for an organization.

## Definition of a security policy and discussion.

### Definition of security policy:

### Discussion on policies:

#### Human resource policy (HR):

Human resource

#### Due care policy(DC):

#### Incidence response policy (IR):

#### Disaster recovery policy (DR):

#### Business continuity policy (BC):

#### Security policy (SP):

#### Acceptable use policy (AUP)

#### Disposal policy (DP)

#### Privacy policy (PP)

#### 10) Password management policy (PMP)

## The example for each of the policies:

#### Human resource policy (HR):

Human resource

#### Due care policy(DC):

#### Security policy (SP):

#### Disposal policy (DP)

#### 10) Password management policy (PMP)

## The most and should that must exist while creating a policy.

For example, a **security policy**

|  |  |  |
| --- | --- | --- |
| S/N | **Security policy must** | **Security policy should** |
| 1 | Be able to implement and enforce it | States reasons why the policy is necessary |
| 2 | Be concise and easy to understand | Describe what is covered by the policy |
| 3 | Balance protection with productivity | Outline how violations will be handled |

Table 1 Policy Must and should

**The elements of a security policy**

Security policies are formal documents that outlines acceptable and unacceptable employee behaviors, legal element is often included in these documents.

### The three most common elements :

#### Due care

#### Separation of duty

#### Need to Know.

To verify the element of the security, the management conducts the first step as Risk analysis, – deployed the second step as Security policy and end the process with compliance monitoring and evaluation.

For example, Password management policy (PMP)

|  |  |  |
| --- | --- | --- |
| S/N | **Password management policy must** | **Password management policy should** |
| 1 | Be able to implement and enforce it | States reasons why the policy is necessary |
| 2 | Be concise and easy to understand | Describe what is covered by the policy |
| 3 | Balance protection with productivity | Outline how violations will be handled |

**The elements of a password security policy**

Security policies are formal documents that outlines acceptable and unacceptable employee behaviors, legal element is often included in these documents.

### The three most common elements :

#### Due care

#### Separation of duty

#### Need to Know.

To verify the element of the security, the management conducts the first step as Risk analysis, – deployed the second step as Security policy and end the process with compliance monitoring and evaluation.

## Give the steps to design a policy

# P8 The main components of an organizational disaster recovery plan, justifying the reasons for inclusion.

## Discussion and explanation about business continuity

## The components of recovery plan

## All the steps required in disaster recovery process:

## 

## The policies and procedures that are required for business continuity:

# Conclusion

# References