BTEC Level 3 IT

Unit 11 - Cybersecurity

Course Information

This is an exam unit.

There is no coursework.

The name of the unit is Unit 11 Cyber Security and Incident Management.

The exam is set for either December/January and May/June.

Unit 11 Course Information

- This unit is 120 guided learning hours.
- There are a total of five assessment outcome, I will go over these.
- The exam comes in two parts, Part A and Part B.
- Part A will be 5 hours.
- Part B will be 4 hours.

Specification Document

This document is to help you.

It is free.

I will provide a copy of it in the description.

It gives you all the information you will ever need for the exam.

Assessment Outcomes

- AO1 Demonstrate knowledge and understanding of technical language, security threats, system vulnerabilities and security protection methods, and implications resulting from successful threat.

- AO2 Apply knowledge and understanding of security threats, system vulnerabilities and security protection methods and implications in order to risk assess systems and select appropriate tools to secure them.

Assessment Outcomes

- AO3 Analyse forensic evidence data and information to identify security breaches and manage security incidents.
- AO4 Evaluate protection methods and security documentation to make reasoned judgements and draw conclusions about their efficacy.
- AO5 Be able to plan a secure computer network and manage security incidents with appropriate justification.

Unit Information

- This is a cumulative unit.
- That means you will need information you learnt from other units.
- This unit is a massive undertaking (it is a big unit).

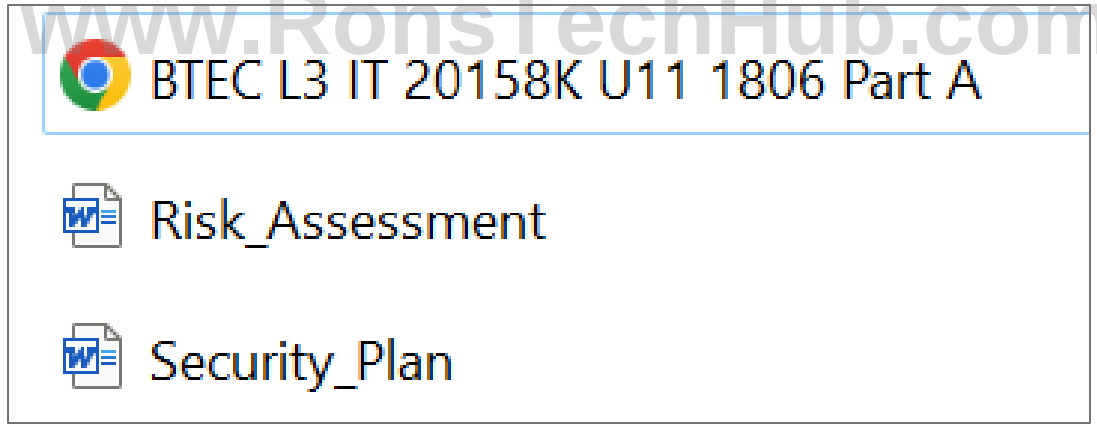
A Look Of The Exam

I want to jump straight in.

You will get the exam paper and some templates to fill in.

Part A Stuff You Get

- Here are the files/documents you get.



Part A Sections/Activities

Part A has a total of 3 activities.

The below was taken directly from the 2018 exam paper.

Activity 1: Risk Assessment.

Activity 2: Security Plan.

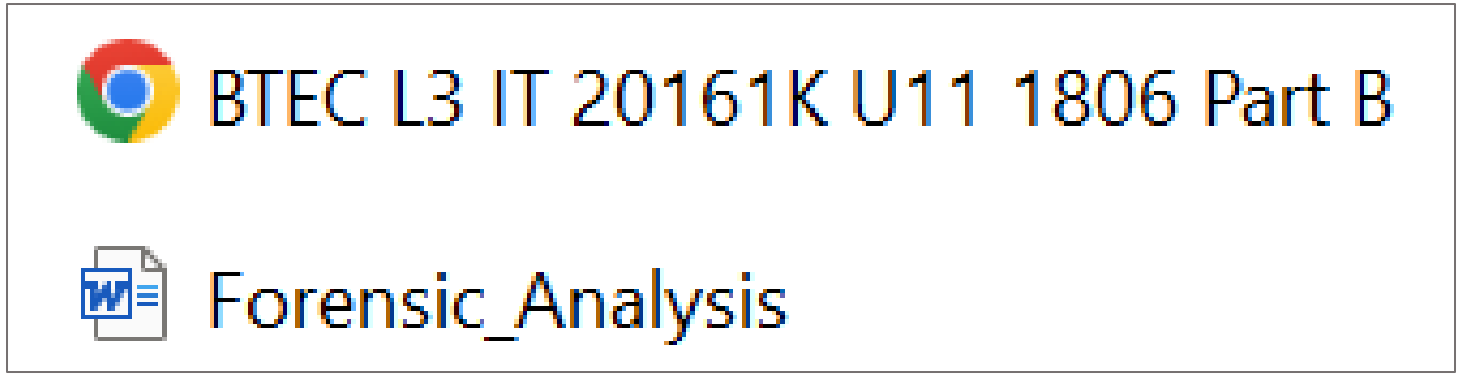
Activity 3: Management Report.

Exam Part A

- You get Activity 1: Risk Assessment.
- You get Activity 2: Security Plan.
- You do not get Activity 3: Management Report.

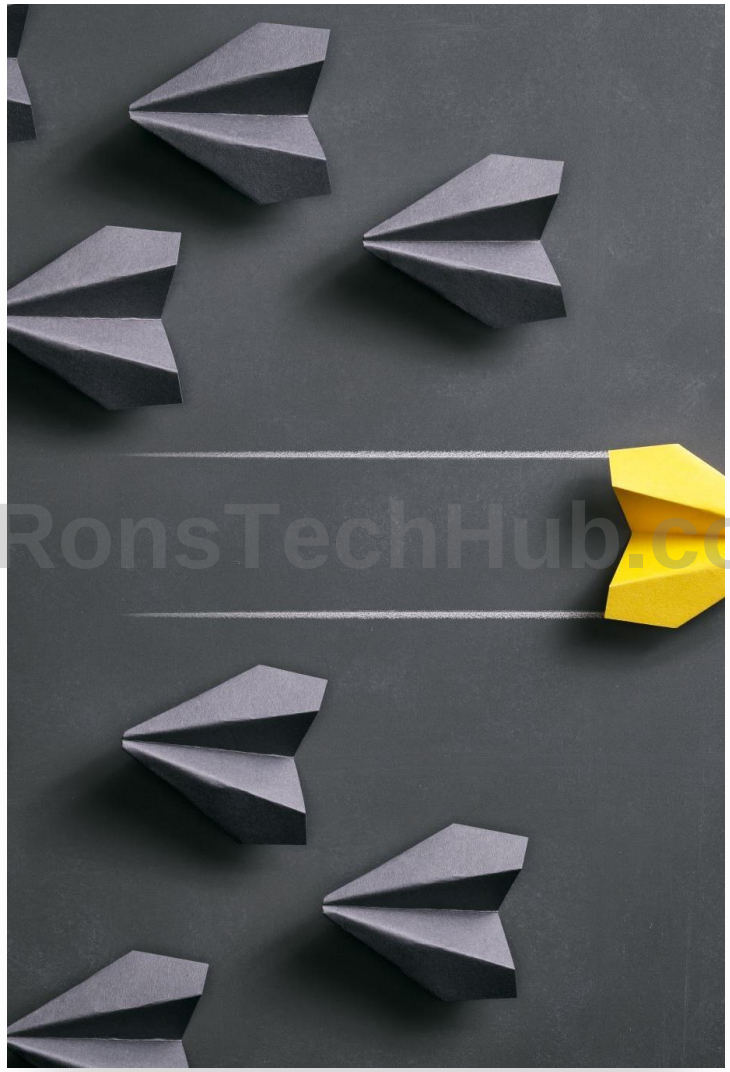
Part B Stuff You Get

- Here are the files/documents you get.



Part B
Sections/Activities

- Part B has a total of 2 activities.
- The below was taken directly from the 2018 exam paper.
- Activity 4: Incident Analysis.
- Activity 5: Security Report.



Exam Part B

You only get the Forensic Analysis.

A Big Unit

- There is a lot to learn.
- I will not have the time to go over all the content you have to learn.
- Please, please, please have a look at the specification.
- *Show example: Internal and External Threats.*
- *Show example: Delivery Guide*

Specification and Delivery Guide

The specification give you all the information you will need for the entire unit.

The delivery guide gives us teachers an example as to how we can teach the unit.

I think students should have access to both these documents once they are explained.

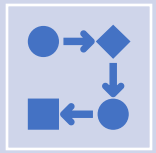
Files I Am Adding

- Specification
- Delivery Guide
- 2018 Paper – Part A
- 2018 Paper – Part B
- 2018 Examiners Report

Please Have A Look At The Documents

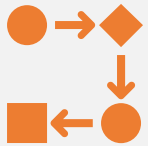
Please ask your teacher to share these files with you.

Please ask for them to explain how to use them.



Please have a look through them.

What I Will Show



I will show how to do each activity.

I will use examples from previous exams or exemplars.

I will try to always explain the **what** and **why**.

Words and Terms To Know

- There are a lot of words and terms you need to know.
- Please keep a word document of all the important words which pop up.
- Be able to define/explain each one.

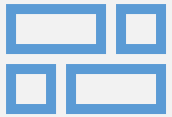
Read It All and Pay Attention

- Please read the ENTIRE paper.
- Might seem obvious, but please, do not overlook anything.
- For example, the **Instruction To Learners** section tells you the names your files needs to be submitted as.

Top Tip

- Spend the bulk of your time focusing on CYBER threats or the potential of such.
- Things like fires and floods are threats.
- Highlighting these is **NOT** wrong, however, getting too detailed is a waste of time.

Templates



Show the Templates given for:

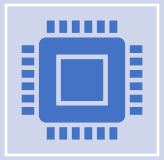
Part A.

Part B.

Activity 1 – Risk Assessment

- A risk assessment is the process of identifying what hazards currently exist or may appear in the workplace.
- That was a definition copied from Google.
- Google Search: Define Risk Assessment.

From An Examiner's Report



This activity requires learners to assess the cyber security implications of the scenario and produce a risk assessment.

A risk assessment template is provided, together with a simple matrix for determining risk severity.

Activity

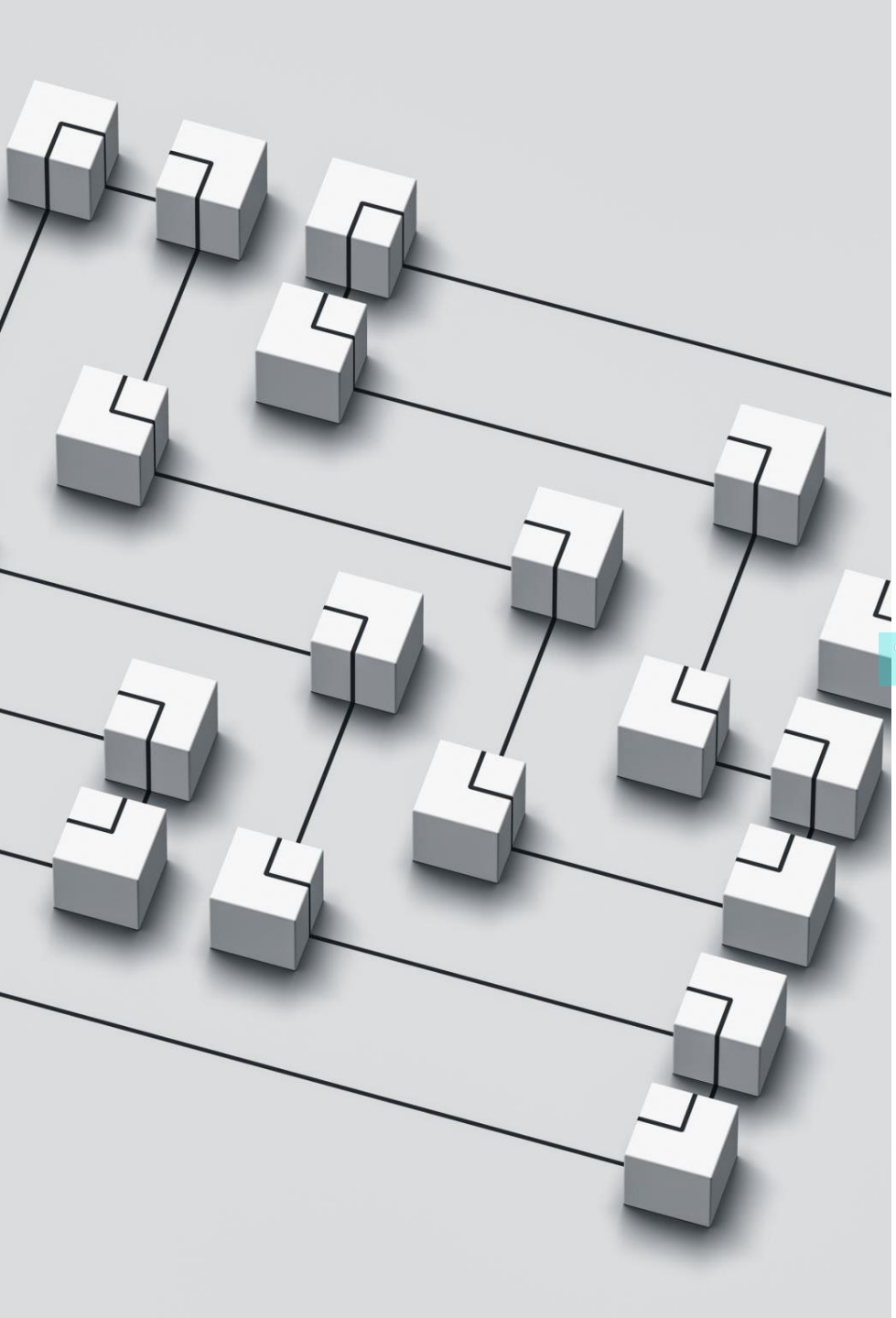
What To Do?

You will get a scenario on the exam paper.

You will need to read and make some notes from the scenario.

There will be weaknesses.

Some will be obvious, others not so much.



The Scenario

- The scenario will have all the information you need.
- The scenario will have information of the company.
- The hardware and software the company uses.
- A plan of the building.
- A network diagram and how the network and its devices are arranged.

Activity 1 – What To Do?

- You will need to find these weaknesses.
- I suggest making a list of all the things you find.
- Make this list exhaustive at fist (make a big list).
- Then trim the list down if you need to.

Risk Severity Matrix

- For every threat/weakness that you have found, you do one of these.

Risk severity matrix

Probability of threat occurring	Very likely	Medium	High	Extreme
	Likely	Low	Medium	High
	Unlikely	Low	Low	Medium
		Minor	Moderate	Major
	Size of the loss			

Risk Severity Matrix

- There are two things we need to do using the matrix.
- The probability.

- Potential Size of Loss.
- How severe the threat is (implications if it happens).

Activity 1 – Things You Need To Do

1) List of all the threats.

2) Do the below for each threat:
   1)Threat Probability, liklihood of it happenning.
   2)Possible threat Impact, how miuch damage could it cause.

Risk Severity Matrix Example

- THREAT: No encryption on the admin server.
- Image this is my threat.
- Let's give this worst-case scenario, A popular secondary school.
- I need to use the risk severity matrix to work out **the probability** and the **possible size of the loss.**

Probability Of Threat Occuring

- THREAT: No encryption on the admin server.

- Probability: Very Likely (an educated guess based on scenario).

Risk severity matrix

Probability of threat occurring	Very likely	Medium	High	Extreme
	Likely	Low	Medium	High
	Unlikely	Low	Low	Medium
		Minor	Moderate	Major
	Size of the loss			

Size Of The Loss

- THREAT: No encryption on the admin server.
- I would say major.

Risk severity matrix

Probability of threat occurring	Very likely	Medium	High	Extreme
	Likely	Low	Medium	High
	Unlikely	Low	Low	Medium
		Minor	Moderate	Major
	Size of the loss			

Risk Severity

- THREAT: No encryption on the admin server.

- I would say extreme.

Risk severity matrix

Probability of threat occurring	Very likely	Medium	High	Extreme
	Likely	Low	Medium	High
	Unlikely	Low	Low	Medium
		Minor	Moderate	Major
	Size of the loss			

Risk Severity Matrix

- Copy and paste that table as many times as you need it.
- Do the same for the assessment itself (the next section).
- OR.
- Create a shortened version of what the table shows.

Risk Severity Matrix

THREAT: No encryption on the admin server.

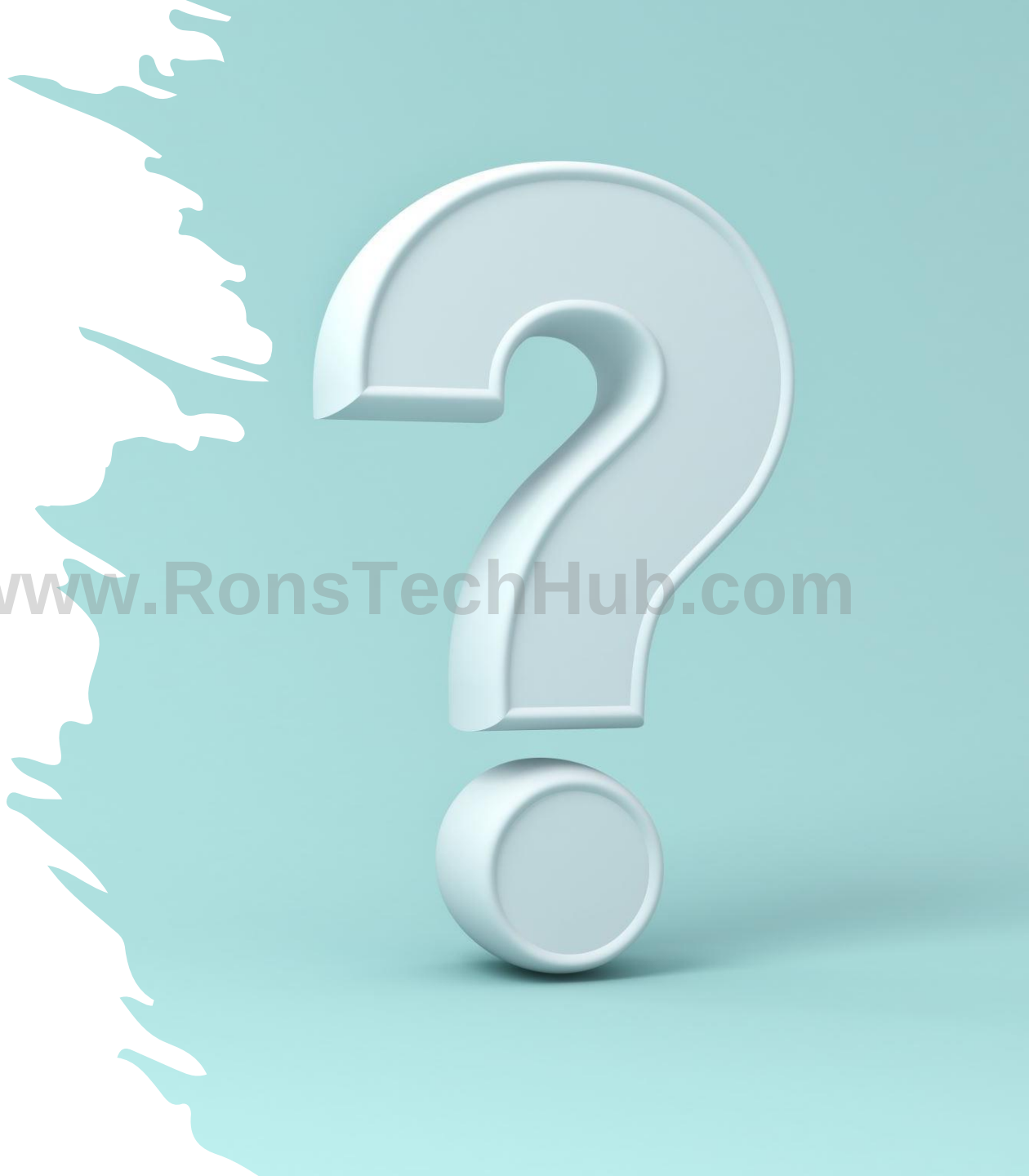
Probability: Very Likely.

Size Of Loss: Major.

Risk Severity: Extreme

Show Example Word Document

- I will be using the 2018 past paper.
- This was the only one of the website not locked.
- You should also have access to the this one if you Google.
- Google Search: BTEC level 3 IT



Activity 1- Risk Assessment

- This carries on from the previous section.
- You still need all those risks and the severities.
- Fill the table in for EVERY threat you have identified.
- Copy and paste this for as many threats/weaknesses you have found.

Assessment

Threat number.	
Threat title.	
Probability.	
Potential size of loss / impact level.	
Risk severity.	
Explanation of the threat in context.	

Activity 2

Security Plan

- You need to use the template **Security_Plan.rtf** produce a cyber security plan for the computer network using the results of the risk assessment.
- You should use the template provided to you.
- There are several things you must consider.
- You **MUST** use the same threats you found in Activity 1.

Activity 2

Headings To Use

- 1) Threat(s) addressed by the protection measure.
- 2) Details of action(s) to be taken.
- 3) Reasons for the actions.
- 4) Overview of constraints – technical and financial.
- 5) Overview of legal responsibilities.
- 6) Overview of usability of the system.
- 7) Outline cost-benefit.
- 8) Test plan.

Activity 2 Overview

- You are advised to spend 2 hours and 30 minutes on this activity.
- Produce a cyber security plan for the computer network using the results of the risk assessment.
- Come up with a plan to help solve the potential problems you found in Activity 1.

How To Do Activity 2

- There are more obvious threats that can be grouped, I did not do all the threats.
- The main router is broadcasting its WiFi signal, it **can be** attacked.
- Staff and Visitor WiFi can be attacked.
- These can be grouped. This was an over simplified example.
- Threats can be grouped if they have similar solutions. The above: Wifi being attacked.

Threat/s and Protection Measure

- For every threat you have you will need a protection measure.
- A protection measure is essentially a way to fix the potential issue you have found.
- Having multiple fixes is recommended as you will need this for Activity 3.
- Having two or three per threat is good, you can have more.

Details of action(s) to be taken

- We simply give ways in which we can fix te potential problem.
- Turn off the router's WiFi and staff WiFi, make them not discoverable(searchable), have only the visitor WiFi discoverable.
- Have WiFi access to staff and Router limited to MAC Addresses (physical address, not changeable).

Reasons for the actions

- Give details on why this action is necessary.
- Why turn off the WiFi on the main router?
- Why only make the visitor WiFi discoverable?
- Why only allow connection via mac addresses?

Overview of constraints – technical and financial

A constraint is simply the limitations or restrictions we must work with.

Google Search: Define Constraint.

Speak on the technical constraints.

Then speak on the financial constraints.

Overview of constraints – technical and financial

- Technical: The thing you want to do, is it technically possible with current technology?
- Technical: The thing you want to do, if it is technically possible, are there people in or outside of the company that can be hired to do it?
- Financial: How much **money** and time will it take to get this done?

Overview Of Legal Responsibilities

Think about all the acts.

Copyright Design and Patents Act.

Data Protection Act.

Health and Safety Act.

Computer Misuse act.

Overview Of Legal Responsibilities

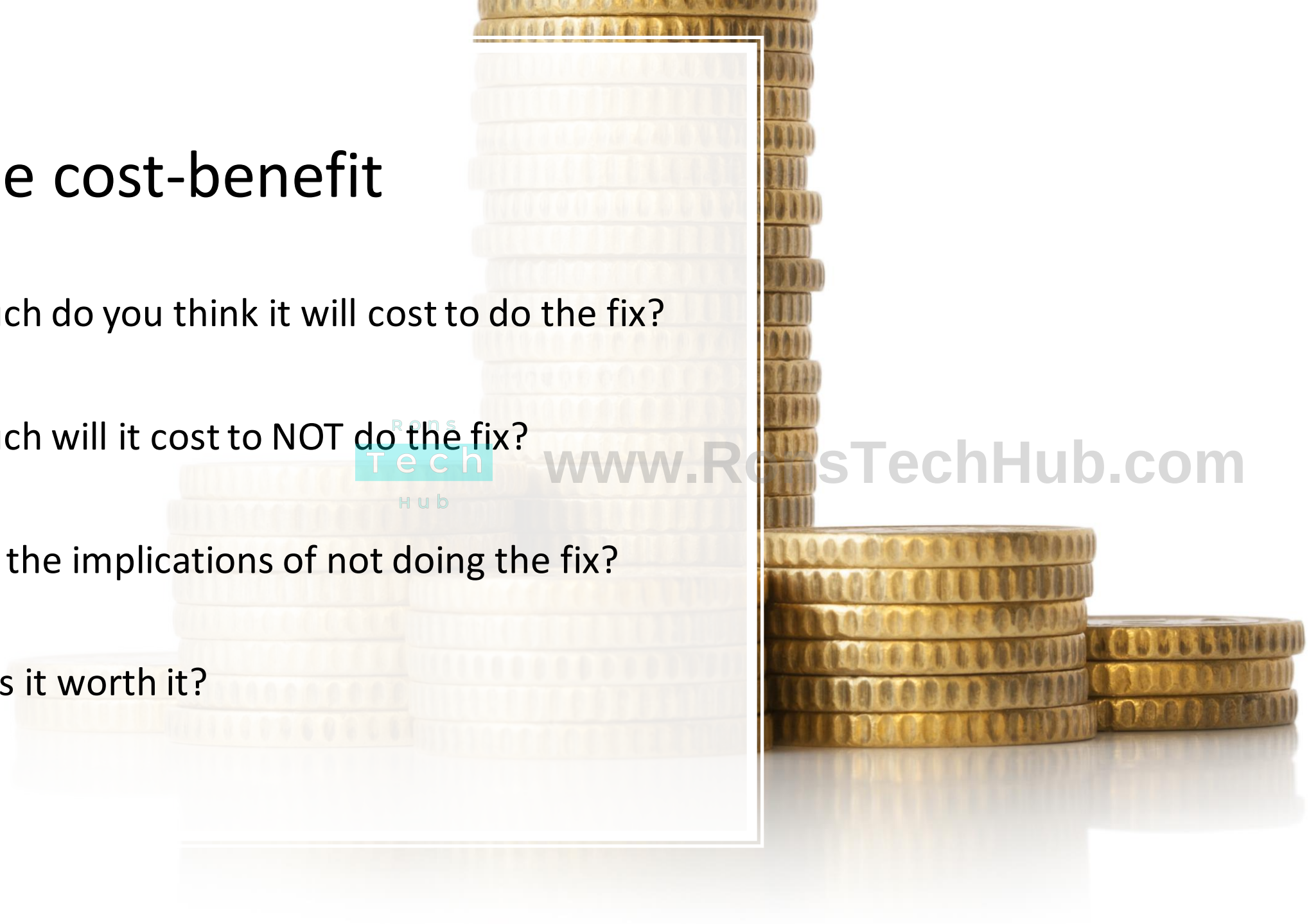
- Will the fix you want to implement/do have any of the acts to consider?
- If so, which of the acts?
- Explain why?

Overview of usability of the system

- Will the fix you want to implement/do make the system better to use or worse to use in general?
- If it is going to be better explain how it is going to make it better.
- If it is going to be worse explain how it is going to make it worse.
- If worse, give a brief explanation why this choice was still worth it.

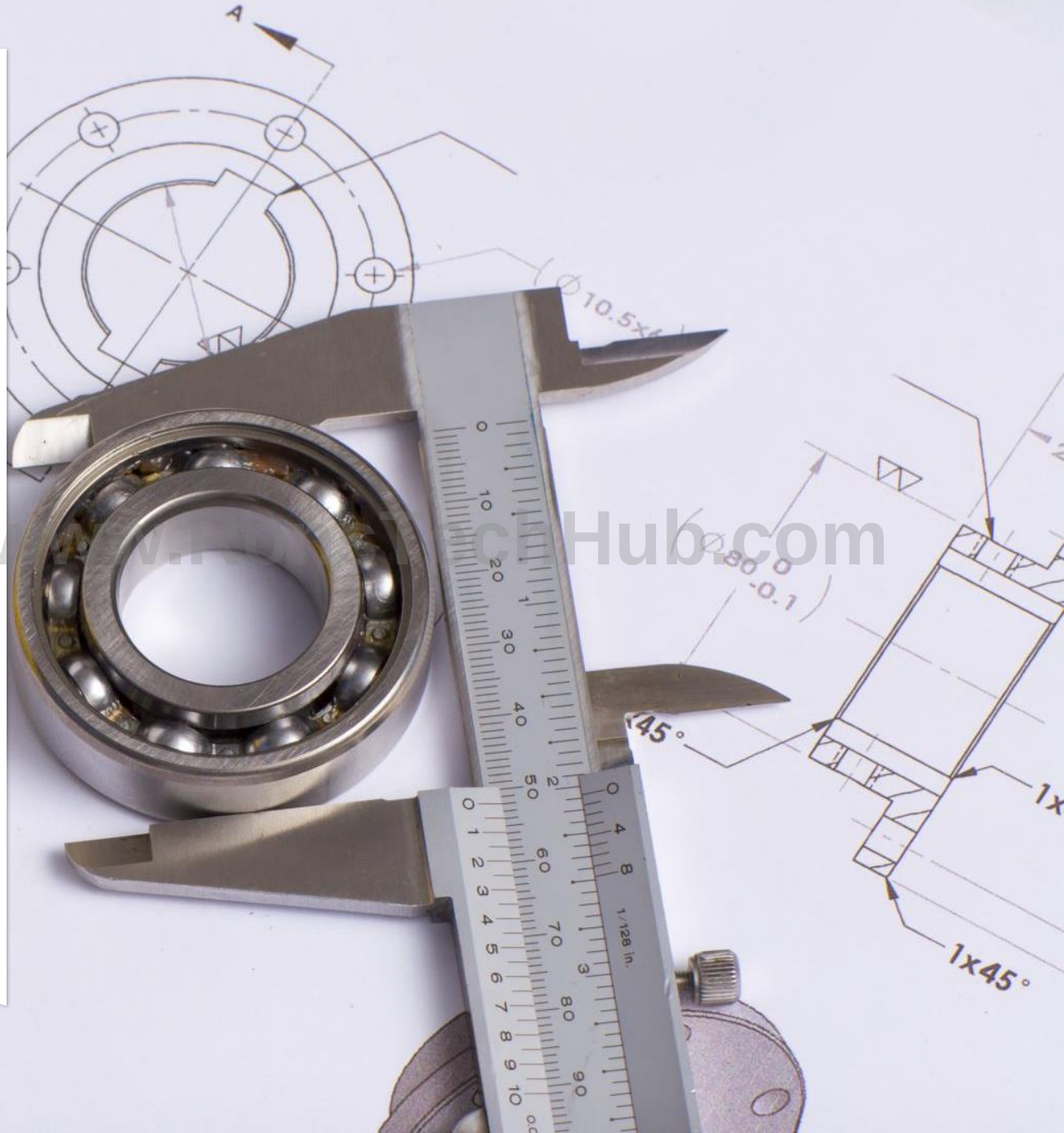
Outline cost-benefit

- How much do you think it will cost to do the fix?
- How much will it cost to NOT do the fix?
- Think of the implications of not doing the fix?
- Simply, is it worth it?

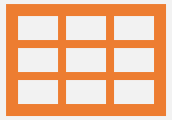


Test Plan

- It does not need to be particularly detailed as the system is hypothetical.
- This is from the examiner's report.
- You test your solution/protection measure.
- There is a table for this.



Activity 3 Introduction



There is NO template.

You will have to create a document yourself.

They do give you pointers to use in the report for Activity 3.

Activity 3

An assessment of the appropriateness of your protection measures.

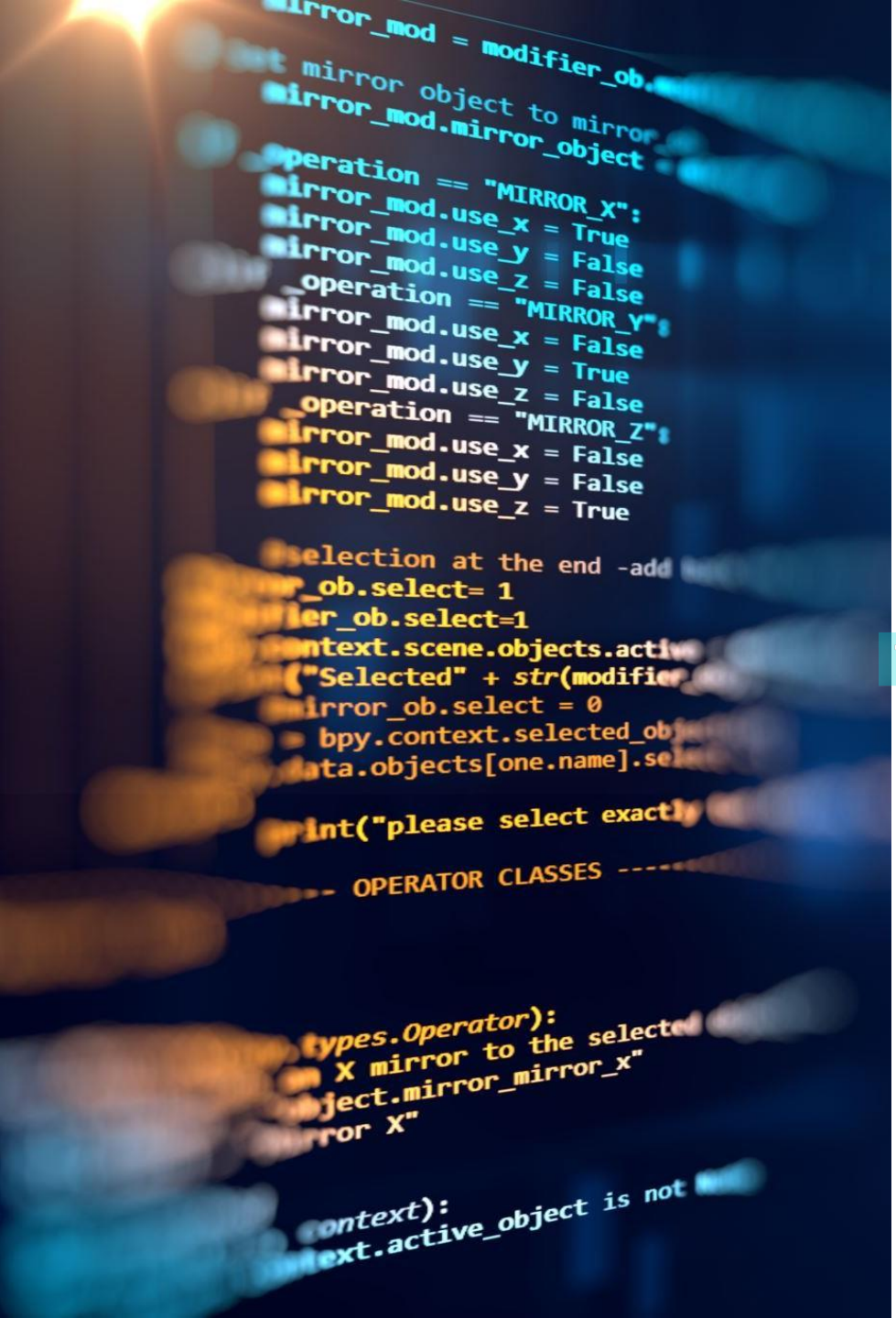
A consideration of alternative protection measures that could be used.

A rationale for choosing your protection measures over the alternatives.

These were copied from the exam paper.

Activity 3
What To Do?

- For each of the previous fixes/protection measures in Activity 2: Assessment.
- You will need to do the three things stated prior.
- Appropriateness.
- Alternatives.
- Rational for choice.



Activity 3 How To Do?

- Very Technical Language?
- Medium Technical Language?
- Low Technical Language?
- For A Dum Dum Like Me?

Activity 3 How To Do?

- Like with everything else it depends.
- The report will most likely be for the person in the brief.
- Tailor your language to suit them.

Tailoring The Language

- If the person is an accountant who simply wants this stuff done, maybe use low level language.
- If the person is an experienced IT practitioner, but not a network specialist, maybe use medium level language.
- If the person is a network specialist who maybe simply needed some help because he/she is understaffed, maybe use high level language.

High Level Language

- They are very much a network person.
- They will understand all the words and phrases you throw are them.
- You use all the technical terms you learnt.
- Example: We will need a firewall and an ACL setup to limit access to sensitive areas.

Medium Level Language

The person knows some IT.

They can grasp some of the words and terms used.

But making things simpler would be useful.

Example: We will need a firewall and create a list of users who can access certain resources to limit access to sensitive areas.

Low Level Language

- This person knows very little about IT.
- They will most likely understand nothing you say.
- Keep the language very simple and explain what everything means.
- Example: We will need a firewall**(explain this)** and an ACL**(explain this)** setup to limit access to sensitive areas**(explain this)**.

Tailoring The Language

Simply put.

Use words and phrases that you think will allow that person to understand.

Please Note Again

Use the protection measures from Activity 2.

Appropriateness

An assessment of the appropriateness of your protection measures.

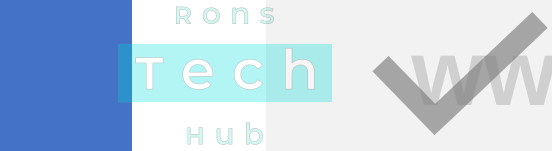
Why is this solution appropriate/suitable for the scenario given?

Why is this good?

Why do you think it would work.

Alternative Protection Measures

A consideration of alternative protection measures that could be used.



I would say no more than 2 or three alternatives.

These are other ways in which the problem could be solved.

Rational For Choice

- A rationale for choosing your protection measures over the alternatives.
- Compared to the alternatives, why was the option you chose better in your estimation?

Protection Measure 1

An assessment of the appropriateness of your protection measures.

A consideration of alternative protection measures that could be used.

A rationale for choosing your protection measures over the alternatives.

With appropriate language.

Protection Measure 2

- An assessment of the appropriateness of your protection measures.
- A consideration of alternative protection measures that could be used.
- A rationale for choosing your protection measures over the alternatives.
- With appropriate language.

Protection Measure 3

- An assessment of the appropriateness of your protection measures.
- A consideration of alternative protection measures that could be used.
- A rationale for choosing your protection measures over the alternatives.
- With appropriate language.

Part A Admin

- You must submit your files as **PDFs**.
- By now you should have 3 documents (rtf, doc, docx etc):
- Risk Assessment.
- Security Plan.
- Management Report.

Part A Admin

You need to export each one as a PDF.

The PDFs are to be submitted to the examiner.

In most cases:

File > Export > Create PDF/XPS

Choose a file name.

Naming Your Files

- The names you should use are on the exam paper.
- You will need the following from your school or invigilator (person in the exam room on the day).
- Registration Number.
- Possibly centre number.

Creating Folder

- My name is KingBoss Ferguson.
- My registration number is 123987 and Centre Number is 000111.
- Instructions: [Centre #]_[Registration number #]_[surname]_[first letter of first name]_U11A.
- My Actual folder Name: 000111_123987_Ferguson_K_U11A.

Risk Assessment Export

- My name is KingBoss Ferguson.
- My registration number is 123987.
- Instruction: activity1_riskassessment_[Registration number #]_[surname]_[first letter of first name]
- Export as: activity1_riskassessment_123987_Ferguson_K.pdf

Security Plan Export

- My name is KingBoss Ferguson.
- My registration number is 123987.
- Instruction: activity2_securityplan _[Registration number #]_[surname]_[first letter of first name]
- Export as: activity2_securityplan _123987_Ferguson_K.pdf

Management Report Export

- My name is KingBoss Ferguson.
- My registration number is 123987.
- Instruction: activity3_managementreport_[Registration number #]_[surname]_[first letter of first name].
- Export as: activity3_managementreport_123987_Ferguson_K.pdf

Show Folder and File Creation

- Create Folder with name: 000111_123987_Ferguson_K_U11A
- Activity 1: activity1_riskassessment_123987_Ferguson_K.pdf
- Activity 2: activity2_securityplan _123987_Ferguson_K.pdf
- Activity 3: activity3_managementreport_123987_Ferguson_K.pdf

Part B Introduction

Part B will have two activities.

Activity 4 Forensic Analysis.

Activity 5 Security Report.

Part B Information

Like Part A, you will need to create a folder and export files.

I will show this process at the end as I did with Part A.

You are **ONLY** given one template for Part B, Forensic Analysis.

An authentication sheet must be completed by each learner and submitted with the final outcomes.

Part B Marks Information

- Part B will have a total of 37 marks.
- 14 marks for Activity 4.
- 20 marks for Activity 5.
- 3 marks in total for use of technical language.

Part B Information

From Exam Paper

- You will be given a new scenario.
- This is an update from the previous task.
- For example the company has now fully moved to the new location.

- **You advised Baljinder Singh of BCTAA on security matters for the move to the new location.**
- **Now, a few weeks later, he has called you in to review the investigation of a cyber security incident.**

Part B Information

- There has been a few incidents since we last met Singh.
- We now need to go in, assess and give some advice.

- The information you will get is forensic evidence, **not a murder case.**
- Simply issues that have arisen since last we spoke to Singh.

Activity 4

You will need to go over all the evidence provided to you.

It might not be obvious how this all happened.

You will make educated guesses.

For example, in 2018 paper.

There were multiple reports of people being pickpocketed.

Activity 4 Notes

- Read the evidence and highlight or write down things you think are important.
- I would do this for each piece of evidence.
- Then bring it all together at the end.

Activity 4 – What To Do?

- Look over all the evidence.
- If you think it is important, make some notes on why.
- What stood out to you.
- I made notes on all of them (not all were needed).

Activity 4 – Evidence 1

- Singh's account of events.
- Listed missing items, this is not often checked.
- Phone blocked.
- Laptop tracked.
- No sensitive information on the file server.

Activity 4 – Evidence 2

- Meeting with Management Company.
- Cleaners and other EH staff are unlikely to steal.
- Pickpockets were on the roam on Friday.
- BCTAA and Recruitment agent had no break ins but had thefts.
- Phantom charges on people's cards, not a system error.

Activity 4 – Evidence 3

- Door Access Control System Log.
- 19630 00029, 18420 00775, 19630 00010 and 19630 00035 are the cards that tried to gain entry.
- All people reported not remembering using the card or NOT using the card.

Activity 4

Evidence 4

Network diagram is the same as before.

No visible updates present.

Activity 4 – Evidence 5

- Laptop Tracking Software.
- Detected the laptop in: Nairobi, Kenya when connected to a network.
- Date: 09.04.2018.
- Time: 11:22:41.

Activity 4 – Evidence 6

- Cyber Security Documentation.
- Details what people do in the event of:
- Theft of IT equipment.
- Theft of data.
- Infection of company IT systems with malware.
- Unauthorised access to BCTAA systems.

Activity 4 – What To Do?

- You need to think about all the evidence.
- The brief.
- The scenario.
- Put together what you think happened.

Activity 4 Template

- You get a template for part 4.
- Forensic Analysis.rtf.

Set Task Electronic Template – Unit 11

Task B - Activity 4 Template: Forensic Incident Analysis

*Use the section headings below to structure a response for **each** evidence item.*

Evidence item:
Method of acquiring the evidence:
Evidence detail:
Evidence reliability:
Conclusions:

After all the evidence items, provide an overall conclusion.

Activity 4 Template Explained

- The template will have five headings.
- Evidence Item.
- Method of Acquiring Evidence.
- Evidence Detail.
- Evidence Reliability.
- Conclusion.

Activity 4 Template Explained

You make use of all the headings for each piece of evidence.

2018 had 6 pieces of evidence.

Copy and paste the headings 5 more times.

You are NOT done.

Conclusion x 2

- After you fill in the table for each piece of evidence.
- You will STILL need to conclude overall.
- This conclusion will give overall thoughts again on what happened.
- You should add how and why you think it happened.

Activity 5 Introduction

A Management Report will be the end result.

Tailor the language for the person who is your contact.

Back in Activity 3, I said Singh was about a medium.

Activity 4 and 5 are linked of course, you will refer to the evidence items again.

Activity 5, What To Do?

- Analyse the policies they had in place.
- Look at the actions taken that led to the incident.
- Compare the actions taken to the policy which is in place.
- Highlight where individuals went wrong or strayed from the policy.
- Then how can we improve upon the policy?

Activity 5, What To Do?

- The exam paper summed it up better than I did.
- Review the incident.
- Was the procedure in place followed.
- Suggest improvements and explain how they would prevent a similar incident in the future.

Security Report Areas For Improvement

- Adherence to forensic procedures.
- The forensic procedure and current security protection measures.
- The security documentation.
- Taken from the exam paper.

Security Report

- This was taken from the examiner's report.
- For the top band marks, the document needs to be laid out ligically.
- A Title.
- A Summary or Introduction.
- A Main Body (with subsections if necessary).
- Justification or Recommendations.

Activity Step By Step – 1

- Make a list of all the mistakes made by the parties involved.
- Look at the procedure that deals with that specific activity.
- Leaving the phones and laptops out probably links to:
- a) Theft of IT equipment.
- b) Thet of data.
- d)) Unauthorised access to BCTAA systems.

Activity Step By Step – 2

Say how the procedures were NOT adhered to/followed.

For example, the phone and laptop should have been locked away with the other devices.

This would have ensured they were out of sight and possibly out of reach.

Activity Step By Step – 3

- What can be done to improve the system.
- On the policies.

- On the individuals.
- This is your recommendation.