BTEC

Pearson BTEC Level 3 National in Information Technology

Unit 11: Cyber Security and Incident Management

Sample Assessment Materials (SAMs)

For use with Diploma and Extended Diploma in Information Technology

First teaching from September 2017 Issue 3

Pearson

Edexcel, BTEC and LCCI qualifications

Edexcel, BTEC and LCCI qualifications are awarded by Pearson, the UK's largest awarding body offering academic and vocational qualifications that are globally recognised and benchmarked. For further information, please visit our qualifications website at qualifications.pearson.com. Alternatively, you can get in touch with us using the details on our contact us page at qualifications.pearson.com/contactus

About Pearson

Pearson is the world's leading learning company, with 35,000 employees in more than 70 countries working to help people of all ages to make measurable progress in their lives through learning. We put the learner at the centre of everything we do, because wherever learning flourishes, so do people. Find out more about how we can help you and your learners at qualifications.pearson.com

References to third-party material made in this specification are made in good faith, we do not endorse, approve or accept responsibility for the content of materials, which may be subject to change, or any opinions expressed therein. (Material may include textbooks, journals, magazines and other publications and websites.)

All information in this document is correct at time of publication.

ISBN 978 1 4469 5016 6

Contents

Summary of Pearson BTEC Level 3 Nationals in Information Technology Sample Assessment Materials for Unit 11: Cyber Security and Incident Management Issue 3 changes

Part A – Summary of changes made between previous issues and this current issue	**Page number**
It has been made a requirement that Invigilators are compulsory to supervise the monitored assessment: 'Teachers/tutors' have been replaced with 'Invigilators'.	Pages 2, 3, 20 and 21

If you need further information on these changes or what they mean, contact us via our website at: qualifications.pearson.com/en/support/contact-us.html.

Pearson BTEC Level 3 Nationals

Information Technology

Set task: Unit 11 Cybersecurity and Incident Management

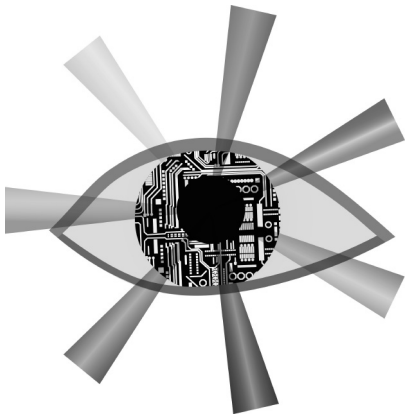
Level 3

Part A

Diploma and Extended Diploma in Information Technology
Sample assessment material for first teaching September 2017

Instructions

- **Part A** will need to have been completed in preparation for **Part B**.
- **Part A** and **Part B** tasks will be submitted together for each learner on completion of **Part B**.
- **Part A** contains material for the completion of the set task under supervised conditions
- **Part A** should be undertaken in 5 hours during the assessment period of one week timetabled by Pearson.
- **Part A** is specific to each series and this material must only be issued to learners who have been entered to undertake the task on a date set by Pearson in the relevant series.
- **Part A** should be kept securely until the start of the 5-hour supervised assessment period.
- **Part B** materials for the set task will be issued prior to the start of the supervised assessment period according to the guidance in the specification.



Paper reference
XXXX/XX
S59204A

1/1/1

S 5 9 2 0 4 A

Pearson

Instructions to Invigilators

Part A set task is undertaken under supervision in a single session of 5 hours in the timetabled days. Centres may schedule a supervised rest break during the session. In order to enable learners to have access to computers a period of 3 days is provided for centres to timetable assessment. Centres should schedule all learners in the same sessions if possible and must release **Part A** to individual learners only for their scheduled sessions.

Internet access is not permitted.

During any break, materials must be kept securely.

All learner work must be completed independently and authenticated by the Invigilator before being submitted to Pearson.

Learners must complete this task on a computer using the templates provided and appropriate software. All work must be saved as a PDF document for submission. Learners must save their work regularly and ensure that all materials can be identified as their work.

The supervised assessment will take place in a timetabled slots. Centres should schedule all learners at the same time or supervise cohorts to ensure there is no opportunity for collusion.

The set task is a formal external assessment and must be conducted with reference to the instructions in this task booklet and the *BTEC Nationals Instructions for Conducting External Assessments (ICEA)* document to ensure that the supervised period is conducted correctly and that learners have the opportunity to carry out the required activities independently.

Learners must not bring anything into the supervised environment or take anything out without your approval.

Centres are responsible for putting in place appropriate checks to ensure that only permitted material is introduced into the supervised environment.

Maintaining security:

- During supervised assessment sessions, the assessment areas must only be accessible to the individual learner and to named members of staff.
- Learners can only access their work under supervision.
- Any work learners produce under supervision must be kept secure.
- Only permitted materials for the set task can be brought into the supervised environment
- During any permitted break and at the end of the session materials must be kept securely and no items removed from the supervised environment

- Learners are not permitted to have access to the internet or other resources during the supervised assessment period.
- Learner work is regularly backed up.
- Learners will save their work to their folder using the naming instructions indicated in each activity.
- Any materials being used by learners must be collected in at the end of the 5 hours, stored securely and handed back at the beginning of the Part B session.

After the session the invigilator will confirm that all learner work had been completed independently as part of the authentication submitted to Pearson.

Outcomes for submission

Each learner must submit the following:

Activity 1 – Risk assessment of the networked system – PDF document

Activity 2 – Cyber security plan for the networked system – PDF document

Activity 3 – Management report – solution justification – PDF document.

Each learner must complete an authentication sheet.

Instructions for Learners

Read the set task information carefully. You should only consider threats, vulnerabilities, risks and protection measures that are implied and/or specified in the scenario.

In **Part B** you will be given a case study. Use this **Part A** booklet to prepare by relating your learning to the specific information given.

Internet access is not permitted.

You will complete **Part B** under supervised conditions.

You must work independently and should not share your work with other learners.

Your teacher may give guidance on when you can complete the preparation.

Your teacher can not give you feedback during the preparation period.

Materials from Part A of the set task must not be taken into or accessed during Part B.

Outcomes for submission

You should submit :

Activity 1 – Risk assessment of the networked system – PDF document

Activity 2 – Cyber security plan for the networked system – PDF document

Activity 3 – Management report – solution justification – PDF document.

You must complete a declaration that the work you submit is your own.

Set Task Information

You are asked to use your cybersecurity and network systems understanding and skills in a given scenario.

Emma's Paintballing Empire (EPE)

Emma Wiltshire's paintballing empire has recently purchased a new concrete bunker for paintballing site number 4 in Hertfordshire. Emma already owns site 1 in Surrey, site 2 in Berkshire and site 3 in Kent.

The company's head office is in a small industrial unit near Slough and consists of two offices and a workshop. Emma works from the head office or from her house, which is situated a few miles away.

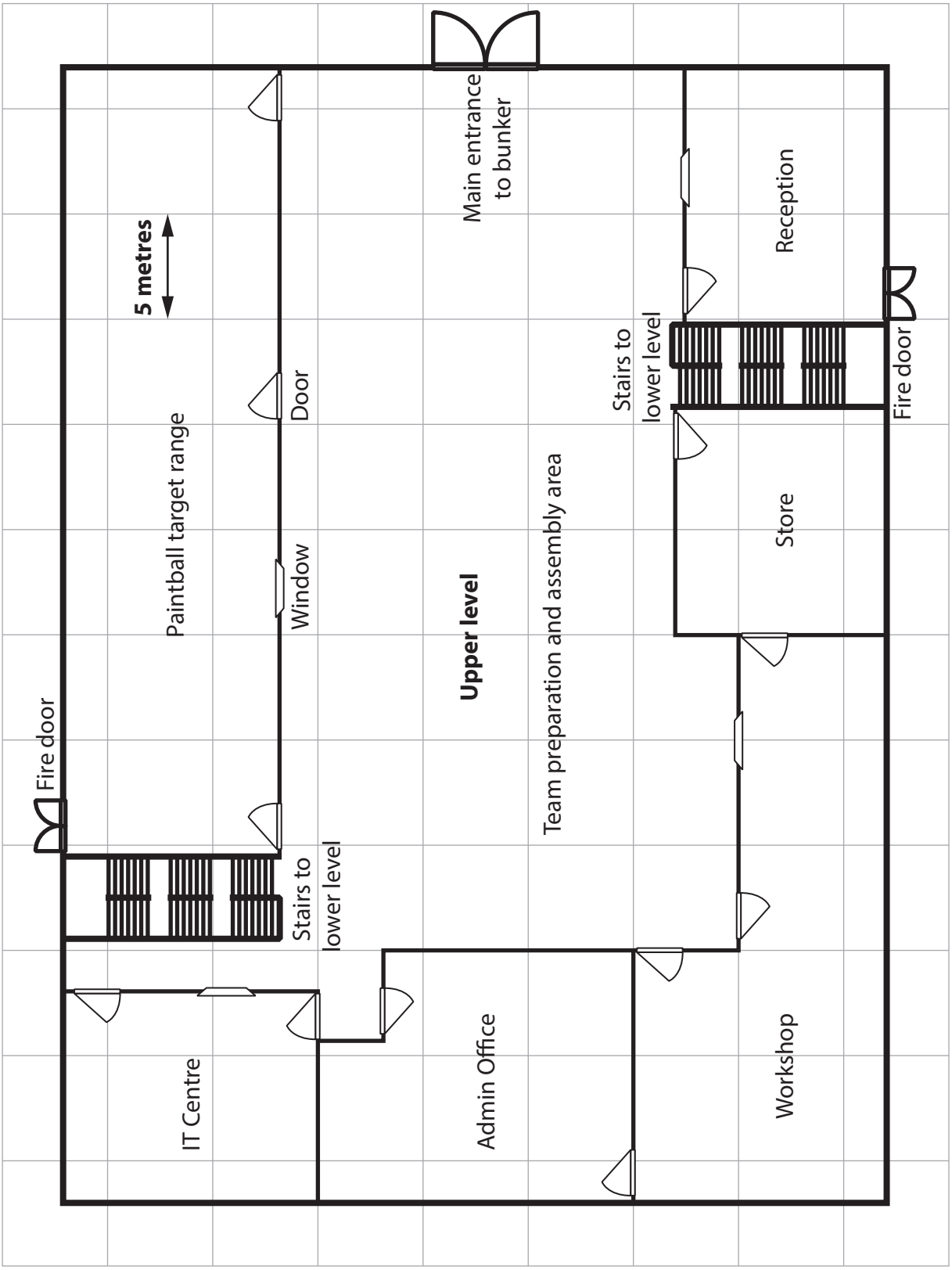
Emma's unique selling point is to provide an enhanced paintballing experience. An enemy base has been constructed at the heart of each location. The enemy base is protected by a large number of automated networked devices that trigger booby traps and automatic paint guns, which the attacking team must avoid. Teams pit themselves against the automated devices (henchmen and women) to capture the enemy base. The idea has proved popular and Emma has improved the productivity of the company by giving employees some administrative control over the paintballing devices. Emma is expanding these aspects of the company.

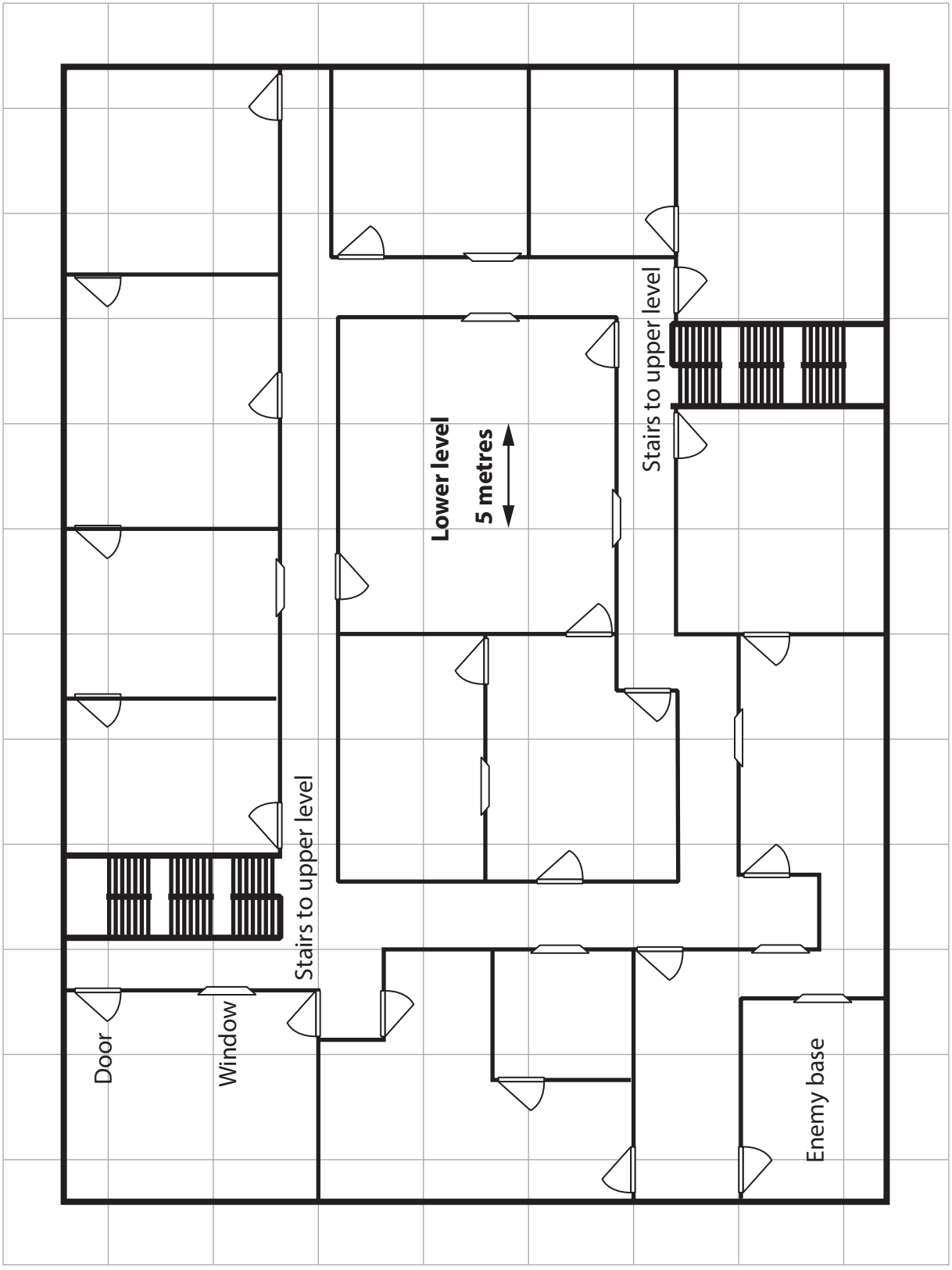
Although the sites have different types of building, they all use the same outline specification for their networks. Emma wants to use the same specification for site 4. The specification states that:

1) the network has two sub-domains: admin and paintball
2) the paintball sub-domain deals with the live paintball area and must be secure from anything that could affect the automated equipment
3) the admin sub-domain deals with all other aspects of the business
4) both sub-domains are administered from the IT centre
5) there is a backup administration facility in the enemy base.

Each location has its own set of offices on-site. These are connected to the head office via the internet.

Paintballing site 4 has two levels. The layout is shown in these diagrams.




Lower level
5 metres
Stairs to upper level
Stairs to upper level
Door
Window
Enemy base

Workshop

The upper level is built above ground. The IT centre already has an external telephone/internet connection.

The lower level is 10 metres underground and the layout cannot be changed. Emma has had false ceilings installed throughout the lower level to give it a more closed-in feel. The space has been used for any networking cabling and other infrastructure.

Emma employs IT staff at each site but would like some fresh ideas for securing the network at paintballing site 4.

Client brief

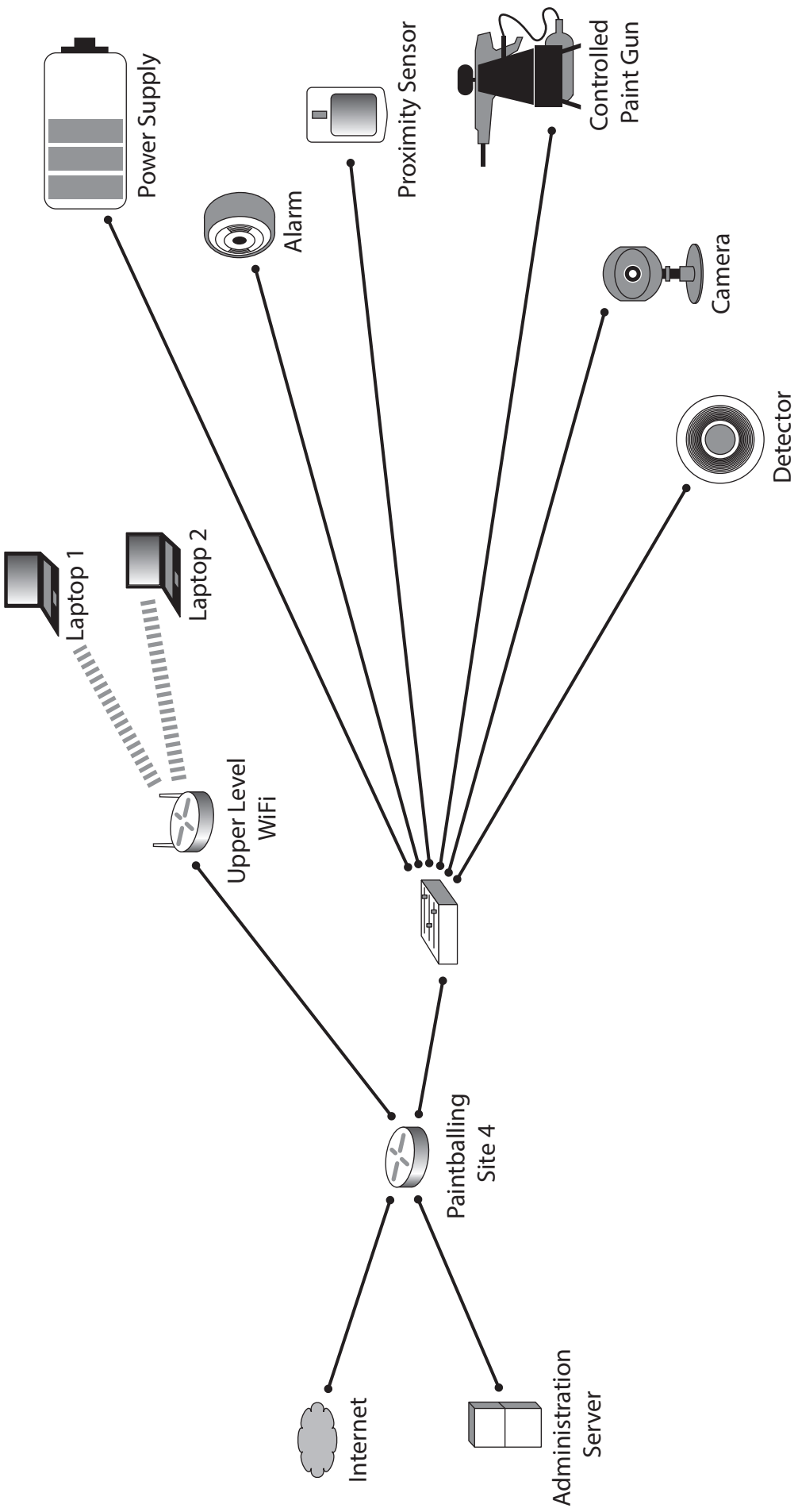
You have been hired to advise Emma on all IT security matters for the project.

Emma is flexible about how the security measures are implemented at paintballing site 4, provided that the networked system is fully secured. During a meeting with Emma, she gives you the following information about paintballing site 4.

1. The system complies with the outline specification.
2. The network in the upper level is mainly connected by Wi-Fi.
3. The network in the lower level is mainly connected by cables.
4. The admin office and reception each have a personal computer (PC) and networked printer.
5. The admin server stores client details, including payment information, which must be kept secure.
6. All of the upper level has network and internet access for mobile devices, including both staff and players.
7. Defence devices such as paint guns may be placed in any part of the lower level and the devices must be kept secure. They must be networked and will often be relocated and adjusted between paintballing sessions. Provision must be made to locate several devices in any room or corridor.
8. Each of the defence devices has a control box and Ethernet (RJ45) port that may be adjusted via internal web pages hosted on that control box. The web pages must be accessible from the IT centre and the enemy base.

The web pages must be accessible from the IT centre and the enemy base.

Logical networked system



The following technical information must be considered in relation to the logical networked system diagram.

1. The admin server is within the admin domain, however it will be on its own network segment.
2. The laptops are also within the admin domain, these are in their own network segment.
3. All devices on the lower level switch are 'representative' of the type of automated technologies that will be used. These are all within their own paintballing domain and separate network segment. They will communicate only with the administration server.
4. The paintballing site 4 router will run all firewall and relevant cybersecurity technology to protect the network, both internally and externally.

The router for paintballing site 4 will offer network address translation (NAT) for the network, to the rest of the internet. Your ISP has issued a single IP address for the entire system.
The system should be set up as follows.

1. The Wi-Fi has two service set identifiers (*SSID*), each running its own Wi-Fi Protected Access 2 (WPA2) with a separate key:
   a. one SSID is for visiting customers
   b. the other SSID is for staff laptops.
2. Between the admin server and the laptops, ports 80 (Hypertext Transfer Protocol (HTTP)), 443 (HTTP Secure) and 993 (Internet Message Access Protocol) must be open and visible to the staff laptops.
3. The admin server must not be visible to any other device on the Wi-Fi network. The admin server acts as a controller for the automated devices, and these will only use port 12345.
4. There must be no opportunity for anyone on the Wi-Fi network to connect to the automated devices. This is for safety reasons and to prevent cheating in the paintball matches. The staff administer the automated devices via secure web pages. These web pages are reachable from a PC in the enemy base and from the admin server in the IT centre. The staff use the admin server to administer client details and use local email.

5. The network uses private, Class C, IPv4 addresses.

All devices on the Wi-Fi network can access the internet. This will be set for typical web browsing and email. Ports that are not required for data traffic must be blocked. There must be no opportunity for anyone on the internet to gain unauthorised access to any of the networks in paintballing site 4.

There are no fixed rules regarding setting up security and network addressing, in responding to this scenario you must present reasonable justification regarding the decisions you have made.

Part A of Set Task

You must complete ALL activities in the set task.

Read the scenario carefully before you begin and note that reading time is included in the overall assessment time.

You should only consider threats, vulnerabilities, risks and protection measures that are implied and/or specified in the scenario.

All documents MUST have a header and a footer. The header must contain the activity number. The footer must contain your name, candidate number and centre number.

A minimum font size of 10 should be used in all word processed documents, using a font type suitable for business purposes.

Any diagrams should be large enough for the detail to be read.

Design cybersecurity protection measures for the given computer network.

Emma employs IT staff at each site but would like some fresh ideas for paintballing site 4. You have been hired to advise Emma on cybersecurity and incident management.

Activity 1 – Risk assessment of the networked system

You are advised to spend 1.5 hours on this task.

Using the template given, produce a cybersecurity risk assessment of the given networked system.

Template file name is CS Part A – A1 – Template Risk Assessment.doc.

Save your completed risk assessment in your submission folder as **activity1riskassessment**.

Total for Activity 1 = 8 marks

Activity 2 – Cybersecurity plan for the networked system
You are advised to spend 2.5 hours on this task.

Using the template given, prepare a cybersecurity plan for the computer network using the results of the risk assessment. For each protection measure you must consider:

a) threat(s) addressed by the protection measure

b) action(s) to be taken

c) reasons for the action(s)

d) overview of constraints – technical and financial

e) overview of legal responsibilities

f) overview of usability of the system

g) outline cost-benefit

h) test plan.

Duplicate (copy and paste) and complete the cybersecurity plan using the template given for each protection measure, as appropriate.

Template file name is CS Part A – A2 – *Template Security Plan.doc*.

Save your completed security plan in your submission folder as **activity2securityplan**.

Total for Activity 2 = 20 marks

Activity 3 – Management report justifying the solution
You are advised to spend 1 hour on this task.

Produce a management report, justifying how the proposed cybersecurity plan will meet the security requirements of the scenario. It should include:

- 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.

Save your completed security plan in your submission folder as **activity3managementreport**.

Total for Activity 3 = 12 marks

Total for technical language in Task A = 3 marks

END OF TASK **TOTAL FOR TASK = 43 MARKS**

Set Task Electronic Templates

Activity 1 Template: Risk assessment of the networked system

Risk severity matrix

Probability of threat occurring	Very likely	Medium	High	Extreme
	Likely	Low	Medium	High
	Unlikely	Low	Low	Medium
		Minor	Moderate	Major
	Impact level/value of the loss			

Risk assessment template

Number	Threat title	Explanation of the threat in context	Probability of occurrence	Potential size of loss/ impact level	Risk severity
1					
2					
3					
4					
…					

Activity 2 Template: Cybersecurity plan for the networked system

Use the section headings below for each protection measure.

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

Test plan

Test number	Test Description	Expected outcome	Possible further action following test
1			
2			
3			
4			
…			

Pearson BTEC Level 3 Nationals

Write your name here

Surname	Forename

Level 3

Learner Registration Number

Centre Number

Information Technology

Set task: Unit 11 Cyber Security and Incident Management

Part B

Marks

Supervised hours XX

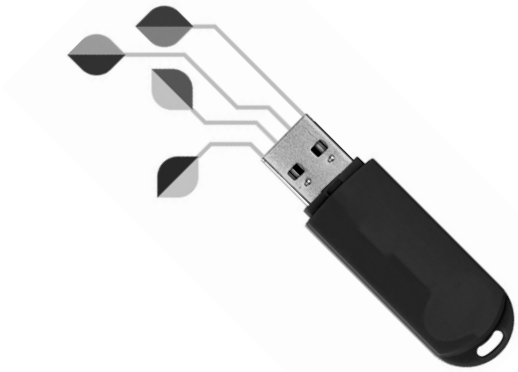
Diploma and Extended Diploma in Information Technology
Sample assessment material for first teaching September 2017

Instructions

- **Part A** will need to have been used in preparation for completion of **Part B**.
- **Part B** booklet must be issued to learners as defined by Pearson and should be kept securely.
- **Part B** booklet must be issued to learners on the specified date.
- **Part B** is specific to each series and this material must only be issued to learners who have been entered to undertake the task in that series.
- **Part B** should be kept securely until the start of the supervised assessment periods.

Information

- The total mark for this paper is 37.



Paper reference
20161K
S59223A

1/1/1/1/1

S 5 9 2 2 3 A

Pearson

Instructions to Invigilators

Part A and Part B set tasks must be completed during the period of three weeks timetabled by Pearson. Part A must be completed before starting Part B.

The five-hour, Part A set task must be carried out under supervised conditions. The set task can be in more than one supervised session.

Learners must complete this task on a computer using the templates provided and appropriate software. All work must be saved as a PDF document for submission. Learners must save their work regularly and ensure that all materials can be identified as their work.

Centres should schedule all learners in the same sessions if possible and must release Part B to individual learners only for their scheduled sessions

Internet access is not permitted.

The set task is a formal external assessment and must be conducted with reference to the instructions in this task booklet and the *BTEC Nationals Instructions for Conducting External Assessments (ICEA)* document to ensure that the supervised assessment is conducted correctly and that learners submit evidence that is their own work.

Learners must not bring anything into the supervised environment or take anything out without your approval.

Centres are responsible for putting in place appropriate checks to ensure that only permitted material is introduced into the supervised environment.

Maintaining security:

- During supervised assessment sessions, the assessment areas must only be accessible to the individual learner and to named members of staff.
- Learners can only access their work under supervision.
- Any work learners produce under supervision must be kept secure.
- Only permitted materials for the set task can be brought into the supervised environment
- During any permitted break and at the end of the session materials must be kept securely and no items removed from the supervised environment
- Learners are not permitted to have access to the internet or other resources during the supervised assessment period.
- Learner notes will be retained securely by the centre after Part B and may be requested by Pearson if there is suspected malpractice.

After the session the invigilator will confirm that all learner work had been completed independently as part of the authentication submitted to Pearson.

Outcomes for submission

Each learner must submit the following:

- Activity 4 – Forensic incident analysis – PDF document
- Activity 5 – Management report – improvements – PDF document.

Each learner must complete an authentication sheet.

Instructions for Learners

Read the set task information carefully. You should only consider threats, vulnerabilities, risks and protection measures that are implied and/or specified in the scenario.

You have a number of sessions to complete the set task provided by your centre. Plan your time carefully and allow time to produce your outcomes for submission.

Internet access is not permitted.

You will complete this set task under supervision and your work will be kept securely during any breaks taken.

You must work independently throughout the supervised assessment period and must not share your work with other learners.

Outcomes for submission

You should submit:

- Activity 4 – Forensic incident analysis – PDF document
- Activity 5 – Management report – improvements – PDF document.

You must complete a declaration that the work you submit is your own.

Set task Information

You are asked to use your cyber security and incident management understanding and skills in a given scenario.

Emma's Paintballing Empire (EPE)

Emma Wiltshire's paintballing empire has recently purchased a new concrete bunker for paintballing site number 4 in Hertfordshire. Emma already owns site 1 in Surrey, site 2 in Berkshire and site 3 in Kent.

The company's head office is in a small industrial unit near Slough and consists of two offices and a workshop. Emma works from the head office or from her house, which is situated a few miles away.

Emma's unique selling point is to provide an enhanced paintballing experience. An enemy base has been constructed at the heart of each location. The enemy base is protected by a large number of automated networked devices that trigger booby traps and automatic paint guns, which the attacking team must avoid. Teams pit themselves against the automated devices (henchmen and women) to capture the enemy base. The idea has proved popular and Emma has improved the productivity of the company by giving employees some administrative control over the paintballing devices. Emma is expanding these aspects of the company.

Although the sites have different types of building, they all use the same outline specification for their networks. Emma wants to use the same specification for site 4. The specification states that:

1) the network has two sub-domains: admin and paintball
2) the paintball sub-domain deals with the live paintball area and must be secure from anything that could affect the automated equipment
3) the admin sub-domain deals with all other aspects of the business
4) both sub-domains are administered from the IT centre
5) there is a backup administration facility in the enemy base.

Each location has its own set of offices on-site. These are connected to the head office via the internet.

Client brief

You have been working with Emma to secure the networked system on paintballing site 4 and now Emma wants you to investigate a cybersecurity incident at site 2.

Following a visit to paintballing site 2 on 21st May 2016, Emma's antimalware software alerted her to a suspicious file running on her laptop. Emma asked the IT technician at site 2 to examine the file. The technician identified it as being a **keylogging program**, klogX.exe, and deleted the file from the laptop. An internal investigation into how the infection might have happened was inconclusive. Emma has asked you to review the incident and the investigation that followed.

Evidence items from the security incident at paintballing site 2

Evidence items include:

1 anti-malware alert

2 key logger properties

3 incident timeline

4 log of IT processes

5 network diagram

6 cybersecurity document – incident management policy.

Evidence items 1 to 5 are required for Activity 4.

Evidence items 1 to 6 are required for Activity 5.

1 Figure 1 shows a snapshot of the anti-malware alert.

Figure 1

2 Figure 2 shows a snapshot of the klogX.exe info

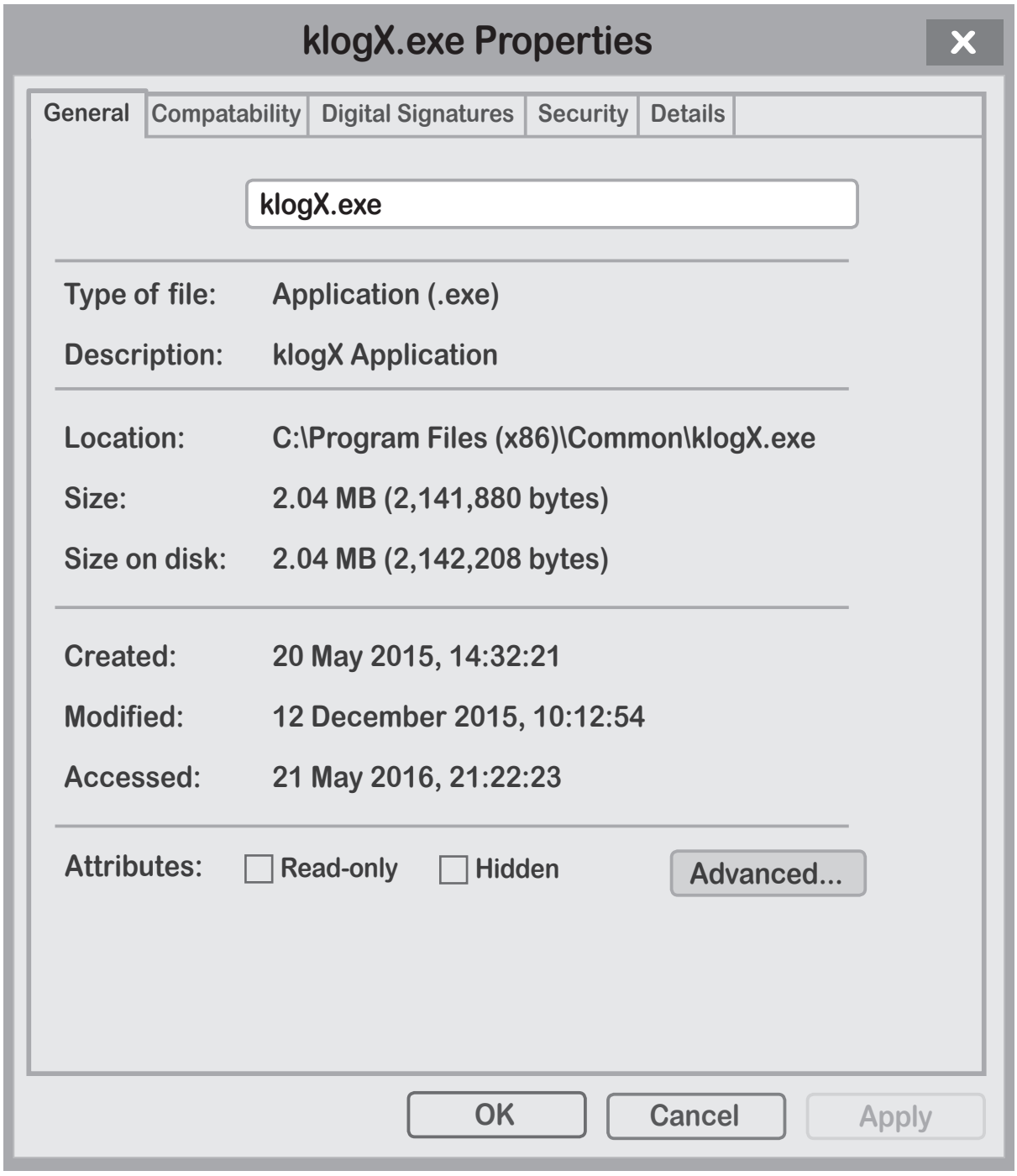


Figure 2

3 Incident timeline

Emma's recollection of events

We've recently started paintball events at paintballing site 2. There had been one the previous evening, 20th May, and a member of staff had taken some photos. I went along on the 21st to have a look at them and select a few to put on the website.

The photos were transferred from the camera to the local drive on the admin office PC, so I logged in to have a look at them. That was at about 4.15 p.m.

I spent about 20 minutes browsing the images and then decided to take a copy of them home with me.

I opened up the laptop to perform the transfer by Wi-Fi but then noticed that there was a flash drive on the desk. I thought that it would be faster to copy the photos onto the drive and then transfer them to my laptop, rather than using the Wi-Fi.

I made the transfer, then logged off from the system at about 5.10 p.m., switched off the laptop and went home.

Later that evening, at about 9.15 p.m., I switched the laptop on again to have another look at the photos. Almost as soon as it started up an alert was displayed. I immediately shut the laptop down again.

Knowing that there was another session being played that evening, I called paintballing site 2 to tell them what had happened. They ran an anti-malware scan immediately but nothing showed up. I took the laptop back there the following day. The same alert showed when the laptop was started up and the technician was able to identify the offending file as being a key logger. The file was deleted and the laptop scanned to ensure there was no further threat.

4 Log of IT processes

Date/time	Event	Event type	Result
Daily/0100	Update anti-malware on site 2 server	Automatic	Anti-malware log shows success from 21st April 2016 to 21st May 2016.
Daily/0200	Anti-malware server scan on site 2 server	Automatic	Anti-malware log shows no alerts for 1st April 2016 to 21st May 2016.
Daily/0300	Off-site backup from site 2 to storage device at site 3	Automatic	Backup logs show success. Backup archives for 14th to 21st May are present.
19th May/1200	Emma's laptop Updates anti-malware signatures and completes a system scan	Manual, following software prompt	Update successful, tracking cookies identified and cleaned.
21st May/1605	Emma's laptop connects to site 2 network via Wi-Fi	Automatic	Server logs show: Wi-Fi connection at 1635 Wi-Fi disconnection at 1710
21st May/1622	Emma logs on to the site 2 network via the admin office PC	Manual	Server logs show: Emma's personal logon at 1612 Emma's logoff at 1708
21st May/2120	Emma restarts her laptop at home	Manual	Anti-malware software displays alert.
21st May/2130	Anti-malware server scan on site 2 server	Manual	No alerts given.
22nd May/0900	Technician investigates suspicious file	Manual	File identified and deleted, no further infection found.

5 Figure 3 shows site 2 with its network.

The network follows the common specification for all of the sites. The admin office and IT centre are in a separate building to the reception and team assembly area and the customers ("paintballers") do not have access.

The enemy base is kept locked unless occupied by a member of staff.

Figure 3 – network diagram for site 2

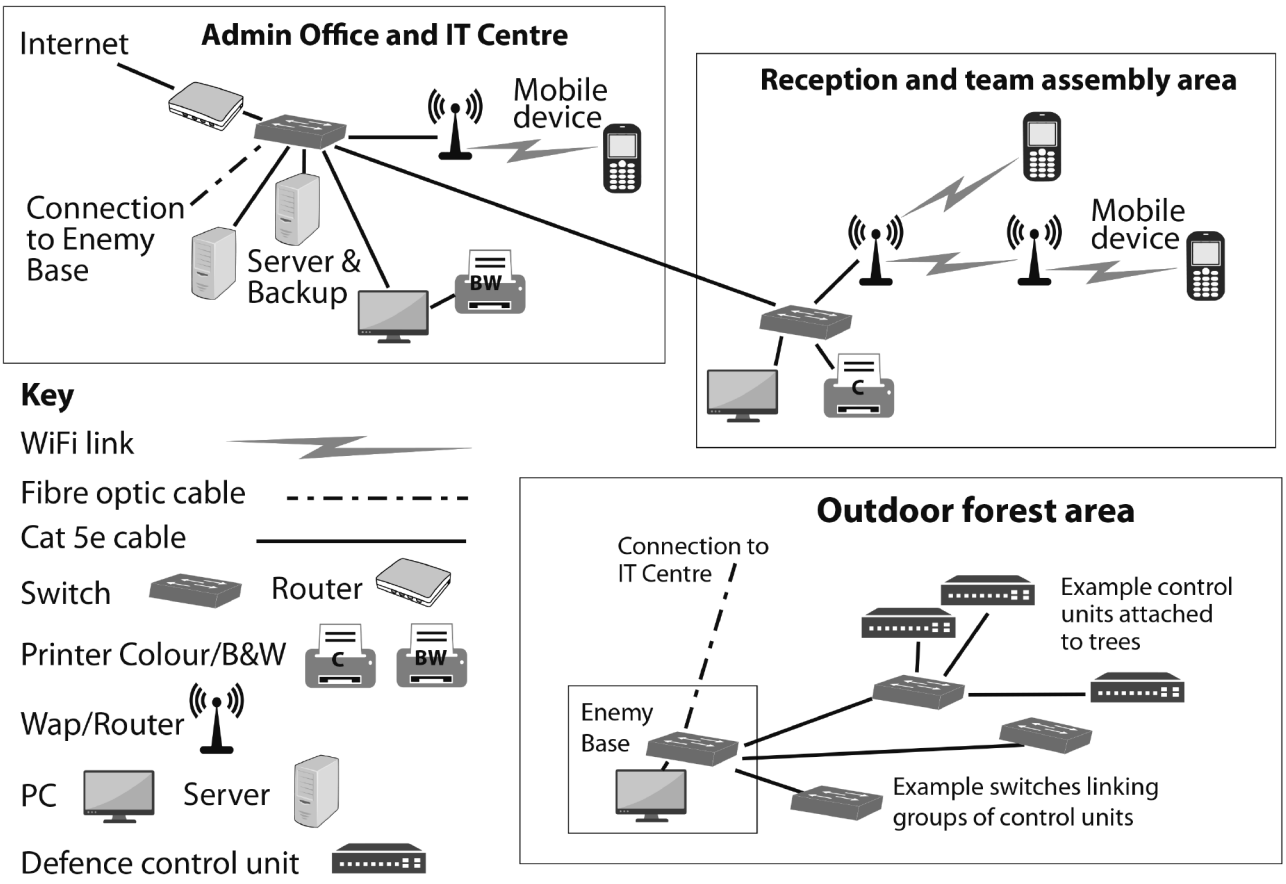


Figure 3

The following evidence item is only required for Activity 5.

6 Cybersecurity documentation – incident management policy

Incident management team

The owner of the paintballing sites is Emma Wiltshire. The incident lead and associate members will be selected by Emma, dependant on the location and nature of the cybersecurity incident.

Incident reporting

Any member of staff who considers that an IT-related security incident has occurred must report it as soon as possible to the Computer Security Incident Response Team (CSIRT) leader. Initially, it may be reported verbally but this must be followed up by an email. It is the responsibility of the CSIRT to maintain detailed documentation on the incident from first report to final resolution. Security incidents may include:

- theft of IT equipment
- theft of company data
- unauthorised access to company IT systems
- infection of company IT systems with malware
- physical incidents such as fire, flood, terrorist attack etc.

Incident response procedures

a) Theft of IT equipment

- Theft of IT equipment is a very serious issue. Any theft must be reported at once to the CSIRT leader. Initially, a verbal report must be made followed up by email, providing as much information as possible (location and type of equipment, when it was last seen etc.).
- CSIRT team leader must ascertain if the item has actually been stolen (or if it is just missing).
- If the item is confirmed as stolen, the CSIRT team leader must inform the police and contact the finance department so they can inform the insurers.
- CSIRT must prepare a report on the theft to the directors and if needed justify the finances required to replace the stolen item.

b) Theft of company data

- Theft or loss of company data may occur in a number of different ways.
- Any loss of company data must be reported at once to the CSIRT team leader, initially a verbal report must be made followed up by email.
- The CSIRT must investigate the loss and identify exactly what data has been lost or stolen and when the incident occurred.
- Having identified what has been lost or stolen and when, the CSIRT must retrieve backups and restore the data as soon as possible.
- The CSIRT should review the incident and implement procedures to prevent future losses.

c) Infection of company IT systems with malware

- Any member of staff who suspects that any IT system has been infected with malware must report it at once to the CSIRT team leader, initially a verbal report must be made followed up by email.
- The infected system should be shut down as soon as possible
- The CSIRT will investigate the infection and take appropriate measures to resolve the infection and restore the system.

d) Unauthorised access to company systems

- Any member of staff who suspects that there has been unauthorised access to any company IT system must report it at once to the CSIRT team leader, providing as much detail as possible (which system, how access was obtained). Initially, a verbal report must be made followed up by email.
- The CSIRT will thoroughly investigate the incident and identify how the unauthorised access was obtained.

The CSIRT will take whatever action is required to prevent future occurrences (e.g. change passwords).

Set Task

You must complete ALL activities in the set task.

Read the scenario carefully before you begin and note that reading time is included in the overall assessment time.

All documents **MUST** have a header and a footer. The header must contain the activity number. The footer must contain your name, candidate number and centre number.

A minimum font size of 10 should be used in all word-processed documents, using a font type suitable for business purposes.

Any diagrams should be large enough for the detail to be read.

You have been working with Emma to secure the networked system on paintballing site 4 and now Emma wants you to investigate a cyber security incident at paintballing site 2.

Activity 4 – Forensic incident analysis

You are advised to spend 2 hours on this task.

Analyse the forensic evidence, including how the evidence was obtained, for the cybersecurity incident at paintballing site 2.

Consider possible causes of the incident and come to a conclusion about the most likely cause of the incident.

Refer to evidence items 1–5 inclusive.

Template file name is *CS Part B – B4 - Template Forensic Analysis.doc*.
Save your completed forensic incident analysis in your submission folder as **activity4incidentanalysis**.

Total for Activity 4 = 14 marks

Activity 5 – Management report on security improvements

You are advised to spend 2 hours on this task.

Review the incident. Suggest improvements and explain how they would prevent a similar incident in the future. Areas for improvement are:

- adherence to forensic procedures
- the forensic procedure and current security protection measures
- the security documentation.

Read the scenario and evidence items 1–6 inclusive when answering the question.

Save your completed management report in your submission folder as **activity5managementreport**.

Total for Activity 5 = 20 marks

Total for Technical Language in Task B = 3 marks

END OF TASK

TOTAL FOR TASK = 37 MARKS

Unit 11: Cyber Security and Incident Management – Sample marking grid

General Marking Guidance

- All learners must receive the same treatment. Examiners must mark the first learner in exactly the same way as they mark the last.
- Marking grids should be applied positively. Learners must be rewarded for what they have shown they can do rather than penalised for omissions.
- Examiners should mark according to the marking grid not according to their perception of where the grade boundaries may lie.
- All marks on the marking grid should be used appropriately.
- All the marks on the marking grid are designed to be awarded. Examiners should always award full marks if deserved. Examiners should also be prepared to award zero marks if the learner's response is not rewardable according to the marking grid.
- Where judgment is required, a marking grid will provide the principles by which marks will be awarded.
- When examiners are in doubt regarding the application of the marking grid to a learner's response, a senior examiner should be consulted.

Specific Marking Guidance

The marking grids have been designed to assess learner work holistically. Rows within the grids identify the assessment focus/outcome being targeted. When using a marking grid, the 'best fit' approach should be used.

- Examiners should first make a holistic judgement on which band most closely matches the learner response and place it within that band. Learners will be placed in the band that best describes their answer.
- The mark awarded within the band will be decided based on the quality of the answer in response to the assessment focus/outcome and will be modified according to how securely all bullet points are displayed at that band.
- Marks will be awarded towards the top or bottom of that band depending on how they have evidenced each of the descriptor bullet points.

Part A, Activity 1 – Risk assessment of the networked system

Assessment focus	Band 0	Band 1	Band 2	Band 3	Max mark
Activity 1: Risk assessment of the networked system	**0**	**1-3**	**4-6**	**7-8**	**8**
	No awardable content	Demonstrates superficial understanding of security threats. Risk assessment shows limited interpretation of the scenario, using generic reasoning to identify some obvious and/or common threats. Risk assessment provides generally unreasonable and/or unrealistic judgements of: • risk severity • risk probability • size of potential loss.	Demonstrates sound understanding of security threats. Risk assessment shows reasoned interpretation of the scenario, using some logical chains of reasoning to identify an adequate range of threats. Risk assessment provides mostly reasonable and realistic judgements of: • risk severity • risk probability • size of potential loss.	Demonstrates in-depth understanding of security threats. Risk assessment shows perceptive interpretation of the scenario, using logical chains of reasoning to identify a comprehensive range of threats. Risk assessment provides consistently reasonable and realistic judgements of: • risk severity • risk probability • size of potential loss.	

Part A, Activity 2 – Cyber security plan of networked system

Assessment focus	Band 0	Band 1	Band 2	Band 3	Band 4	Max mark
Activity 2: Cyber security plan for the networked system	**0**	**1-5**	**6-10**	**11-15**	**16-20**	**20**
	No awardable content	Report identifies limited measures that provide little or no protection against few threats. Report includes reasons for actions that demonstrate a limited understanding of the function of each protection measure in relation to the threat(s). Report demonstrates a limited understanding of the protection measure in relation to the threat(s) covering: • constraints • legal responsibilities • usability • cost-benefit. Test plan is limited and includes few relevant tests and/or actions.	Report identifies some measures that provide basic protection against the most common threats. Report includes reasons for actions that demonstrate a basic understanding of the function of each protection measure in relation to the threat(s). Report demonstrates a basic understanding of the protection measure in relation to the threat(s) covering: • constraints • legal responsibilities • usability • cost-benefit. Test plan is basic and includes some relevant tests and/or actions.	Report identifies adequate measures that are mostly effective in protecting the system against an adequate range of threats. Report includes reasons for actions that demonstrate a sound and logical understanding of the function of each protection measure in relation to the threat(s). Report demonstrates a sound understanding of the protection measure in relation to the threat(s) covering: • constraints • legal responsibilities • usability • cost-benefit. Test plan is adequate and includes mostly relevant tests and actions.	Report identifies robust measures that effectively protect the system against a comprehensive range of appropriate threats. Report includes reasons for actions that demonstrate comprehensive and in-depth understanding of the function of each protection measure in relation to the threat(s). Report demonstrates a comprehensive understanding of: • constraints • legal responsibilities • usability • cost-benefit. Test plan is comprehensive and includes relevant tests and actions throughout.	

Part A, Activity 3 – Management report justifying the solution

Assessment focus	Band 0	Band 1	Band 2	Band 3	Band 4	Max mark
Activity 3: Management report justifying the solution	**0**	**1-3**	**4-6**	**7-9**	**10-12**	**12**
	No awardable content	Alternative security protection measures, if identified, are likely to be inappropriate. Demonstrates limited understanding of how the security plan would function to protect the networked system, including hardware, software and physical measures. Limited justification that refers to the risk assessment and security plan to address a few of the security requirements.	Appropriate alternative security protection measures are identified for some aspects of the security plan. Demonstrates a basic understanding of how the security plan would function to protect the networked system, including hardware, software and physical measures. Basic justification that refers to the risk assessment and security plan to address some of the security requirements.	Appropriate alternative security protection measures are identified for a range of aspects of the security plan. Demonstrates a sound understanding of how the security plan would function to protect the networked system, including hardware, software and physical measures. Sound and mostly logical justification that integrates aspects of the risk assessment and security plan to address most of the security requirements.	Appropriate alternative security protection measures are identified for a range of aspects of the security plan. Demonstrates a comprehensive understanding of how the security plan would function to protect the networked system, including hardware, software and physical measures. Comprehensive and logical justification that integrates aspects of the risk assessment and security plan to fully address the security requirements.	

Part A, Activity 1-3 – Use of technical language during the task

Assessment focus	Band 0	Band 1	Band 2	Band 3	Max mark
Activity 1-3: Use of technical language	**0**	**1**	**2**	**3**	**3**
	No awardable content	Limited appropriate use of technical language.	Mostly appropriate technical language with some inconsistencies.	Appropriate and consistent technical language used throughout.	

Part B, Activity 4 – Forensic incident analysis

Assessment focus	Band 0	Band 1	Band 2	Band 3	Band 4	Max mark
Activity 4: Analyse the forensic evidence, including how the evidence was obtained, for the cyber security incident and come to a conclusion about the probable cause(s) of the security incident.	**0**	**1-3**	**4-7**	**8-11**	**12-14**	**14**
	No awardable content	Response demonstrates a limited understanding of the forensic procedures and how a few pieces of evidence were obtained. Superficial analysis of evidence, with incomplete links between the pieces of evidence and/or back to the scenario. Conclusion, if present, lacks support or plausibility, with little or no consideration of alternative possibilities.	Response demonstrates a basic understanding of forensic procedures and how some of the evidence was obtained. Reasoned analysis of the evidence, showing generally logical chains of reasoning that link some of the evidence together and back to the scenario. Conclusion is plausible and partially supported, with an unbalanced consideration of alternative possibilities.	Response demonstrates a sound understanding of forensic procedures and how most of the evidence was obtained. Sound analysis of the evidence, showing logical chains of reasoning that link most of the evidence together and back to the scenario. Conclusion is sound and mostly supported, with a generally balanced consideration of alternative possibilities.	Response demonstrates a comprehensive understanding of forensic procedures and how the evidence was obtained throughout. Perceptive analysis of the evidence, showing logical chains of reasoning that comprehensively link the evidence together and back to the scenario. Conclusion is convincing and fully supported, with a balanced consideration of alternative possibilities.	

Part B, Activity 5 – Management report on security improvements

Assessment focus	Band 0	Band 1	Band 2	Band 3	Band 4	Max mark
Activity 5: Review the incident and suggest ways to prevent a similar incident in the future.	**0**	**1-5**	**6-10**	**11-15**	**16-20**	**20**
	No awardable content	Review shows limited analysis, identifying generic weaknesses with incomplete or imbalanced consideration of: • forensic procedures • protection measures • security documentation. Suggestions for improvements are mostly unrealistic in the context of the scenario and would not reduce the likelihood of a similar incident. Justification is limited and lacks support, showing a superficial understanding of the incident.	Review shows basic analysis, identifying a few appropriate weaknesses with imbalanced consideration of: • forensic procedures • protection measures • security documentation. Suggestions for improvements are occasionally realistic in the context of the scenario and would reduce the likelihood of a similar incident. Justification is mostly valid and partially supported with some logical chains of reasoning, showing a basic understanding of the incident.	Review shows sound analysis, adequately identifying appropriate weaknesses with generally balanced consideration of: • forensic procedures • protection measures • security documentation. Suggestions for improvements are mostly realistic in the context of the scenario and would reduce the likelihood of a similar incident. Justification is valid and mostly supported with logical chains of reasoning, showing a sound understanding of the incident.	Review shows perceptive analysis, comprehensively identifying appropriate weaknesses with balanced consideration of: • forensic procedures • protection measures • security documentation. Suggestions for improvements are realistic in the context of the scenario and would greatly reduce the likelihood of a similar incident. Justification is valid and fully supported with logical chains of reasoning, showing an in-depth understanding of the incident.	

Part B, Activity 4-5 – Use of technical language during the task

Assessment focus	Band 0	Band 1	Band 2	Band 3	Max mark
Activity 4–5: Use of technical language	**0**	**1**	**2**	**3**	**3**
	No awardable content	Limited appropriate use of technical language.	Mostly appropriate technical language with some inconsistencies.	Appropriate and consistent technical language used throughout.	

For more information about Edexcel, BTEC or LCCI qualifications visit qualifications.pearson.com

Pearson Education Limited. Registered in England and Wales No. 872828
Registered Office: 80 Strand, London WC2R 0RL
VAT Reg No GB 278 537121

ISBN 978-1-4469-5016-6