

Pearson BTEC Level 3 Nationals Diploma, Extended Diploma

Window for supervised period:

Monday 7 January 2019 – Friday 25 January 2019

Supervised hours: 5 hours

Paper Reference **20158K**

Information Technology

Unit 11: Cyber Security and Incident Management

Part A

You must have:

Risk_Assessment.rtf

Security_Plan.rtf

Instructions

- **Part A** and **Part B** contain material for the completion of the set tasks under supervised conditions.
- There are 43 marks for **Part A** and 37 marks for **Part B**, giving a total mark for the set task of 80.
- **Part A** and **Part B** are specific to each series and this material must be issued only to learners who have been entered to take the tasks in the specified series.
- This booklet should be kept securely until the start of the 5-hour, **Part A** supervised assessment period.
- **Part A** will need to have been completed and kept securely before starting **Part B**.
- Both parts will need to be completed during the 3-week period timetabled by Pearson.
- **Part A** and **Part B** tasks must be submitted together for each learner.
- This booklet should not be returned to Pearson.
- Answer all activities.

Information

- The total mark for this paper is 43.

Turn over ►

W61674A

©2019 Pearson Education Ltd.

1/1/1/1/1




Pearson

Instructions to Teachers/Tutors and/or Invigilators

This paper must be read in conjunction with the unit information in the specification and the *BTEC Nationals Instructions for Conducting External Assessments (ICEA)* document. See the Pearson website for details.

Refer carefully to the instructions in this task booklet and the *Instructions for Conducting External Assessments (ICEA)* document to ensure that the assessment is supervised correctly.

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

The 5-hour **Part A** set task must be carried out under supervised conditions.

The set task can be undertaken in more than one supervised session.

Electronic templates for activities 1 and 2 are available on the website for centres to download for candidate use.

Learners must complete this task on a computer using the templates provided and appropriate software. All work must be saved as PDF documents for submission.

Teachers/tutors may clarify the wording that appears in this task but cannot provide any guidance in completion of the task.

Teachers/tutors and invigilators should note that they are responsible for maintaining security and for reporting issues to Pearson.

Maintaining Security

- Learners must not bring anything into the supervised environment or take anything out.
- Centres are responsible for putting in place appropriate checks to ensure that only permitted material is introduced into the supervised environment.
- Internet access is not permitted.
- Learner's work must be regularly backed up. Learners should save their work to their folder using the naming instructions indicated in each activity.
- 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 can only access their work under supervision.
- User areas must only be accessible to the individual learners and to named members of staff.
- Any materials being used by learners must be collected in at the end of each session, stored securely and handed back at the beginning of the next session.
- Following completion of **Part A** of the set task, all materials must be retained securely for submission to Pearson.
- **Part A** materials must not be accessed during the completion of **Part B**.

Outcomes for submission

Each learner must create a folder to submit their work. Each folder should be named according to the following naming convention:

[Centre #]_[Registration number #]_[surname]_[first letter of first name]_U11A

Example: Joshua Smith with registration number F180542 at centre 12345 would have a folder titled

12345_F180542_Smith_J_U11A

Each learner will need to submit 3 PDF documents within their folder, using the file names listed.

Activity 1: activity1_riskassessment_[Registration number #]_[surname]_[first letter of first name]

Activity 2: activity2_securityplan_[Registration number #]_[surname]_[first letter of first name]

Activity 3: activity3_managementreport_[Registration number #]_[surname]_[first letter of first name]

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

The work should be submitted no later than 29 January 2019.

Instructions for Learners

Read the set task information carefully.

Plan your time carefully to allow for the preparation and completion of all the activities.

Your centre will advise you of the timing for the supervised period. It is likely that you will be given more than one timetabled session to complete these tasks.

Internet access is not allowed.

You will complete this set task under supervision and your work will be kept securely at all times.

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

Your teacher/tutor may clarify the wording that appears in this task but cannot provide any guidance in completion of the task.

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

Part A materials must not be accessed during the completion of **Part B**.

Outcomes for Submission

You must create a folder to submit your work. Each folder should be named according to the following naming convention:

[Centre #]_[Registration number #]_[surname]_[first letter of first name]_U11A

Example: Joshua Smith with registration number F180542 at centre 12345 would have a folder titled

12345_F180542_Smith_J_U11A

You will need to submit 3 PDF documents within your folder, using the file names listed.

Activity 1: activity1_riskassessment_[Registration number #]_[surname]_[first letter of first name]

Activity 2: activity2_securityplan_[Registration number #]_[surname]_[first letter of first name]

Activity 3: activity3_managementreport_[Registration number #]_[surname]_[first letter of first name]

You must complete an authentication sheet before you hand your work into your teacher/tutor.

Set Task Brief

Critically Endangered

Peter Russof is a computer programmer specialising in developing games for PCs. He has written several stand-alone games and has built up a profitable business as an independent game producer. Peter lives in Watford and works from home.

For the last few years Peter has been developing Critically Endangered (CE), a multiplayer, online game. CE is set in a post-apocalyptic world. In CE a plague has caused man to be critically in danger of extinction. Peter's innovative idea was to use real world data such as maps, weather statistics, ecological and geographical information.

Players choose a location in the real world and Peter's algorithms create a 3D play area of that location after the plague. The algorithms take the real world data and integrate it into the game to create a unique play area for each game. At present, Peter can only offer players a few locations as he does not have enough computing power to do any more.

While he was developing CE Peter gave away early versions for nothing and now has an enthusiastic following of several thousand players. He rents server space from a cloud provider to host games. CE has an active online community and several of the players help by running a game forum.

Peter thinks that the next version of CE will be ready for a commercial release. It will require much more storage and processing power. Fortunately, Peter has a cousin, Elana, who runs a web hosting company in Romania, Romwebhost. Peter and Elana have agreed to go into partnership. Peter will produce and support CE while Elana will supply processing and hosting facilities through Romwebhost.

The new version of CE will allow both private and public games.

A player starts a private game by sending a location to the CE server. A play area for that game is then downloaded. Private games may be played offline with no further contact with the CE server. Players with private games may invite friends to join them by linking over the internet.

A player starts a public game in the same way as a private one, the play area is then created and stored on the CE server. Public games must be played online. If a player selects a location that is already being used they will be added to that play area. If public players move beyond the bounds of the existing play areas a new area will be created and stored for anyone to use.

Figure 1 is an outline network diagram, showing how Peter thinks different computers will be linked when the game is running. Figure 2 is a diagram of the CE facilities at Romwebhost.

Peter has already arranged for some of his more dedicated players to act as guides and troubleshooters within the game. They will be given enhanced access to the CE game servers at Romwebhost so that they can modify a play area or a player's character if needed.

Peter is aware that a commercial game system is going to be an attractive target for a cyber attacker. He is particularly concerned about passwords for game access. So far there has been little need for password security, as CE is free for anyone to play and only Peter has administrative access to the existing CE server.

Elana thinks administrative access to the game servers can be protected in a similar way to the web servers that she already runs. However, she is concerned about Peter's idea of having players as guides and troubleshooters within the game. She thinks that the accounts of these players will be a target for people who want to create exploits or manipulate a CE game to give themselves an unfair advantage.

Peter and Elana know that the CE network is vulnerable to attack. You have been hired to advise on cyber security and incident management.

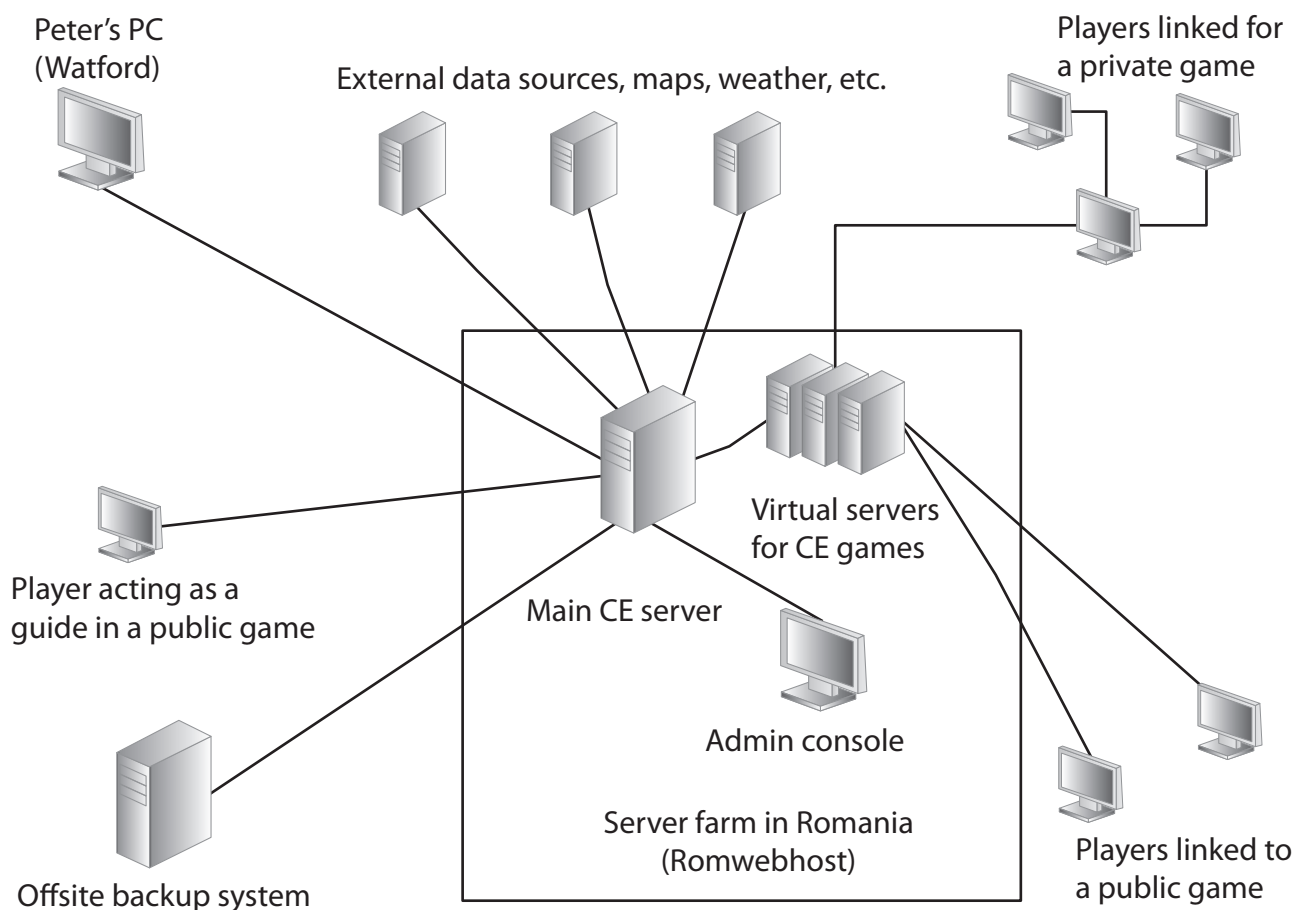


Figure 1

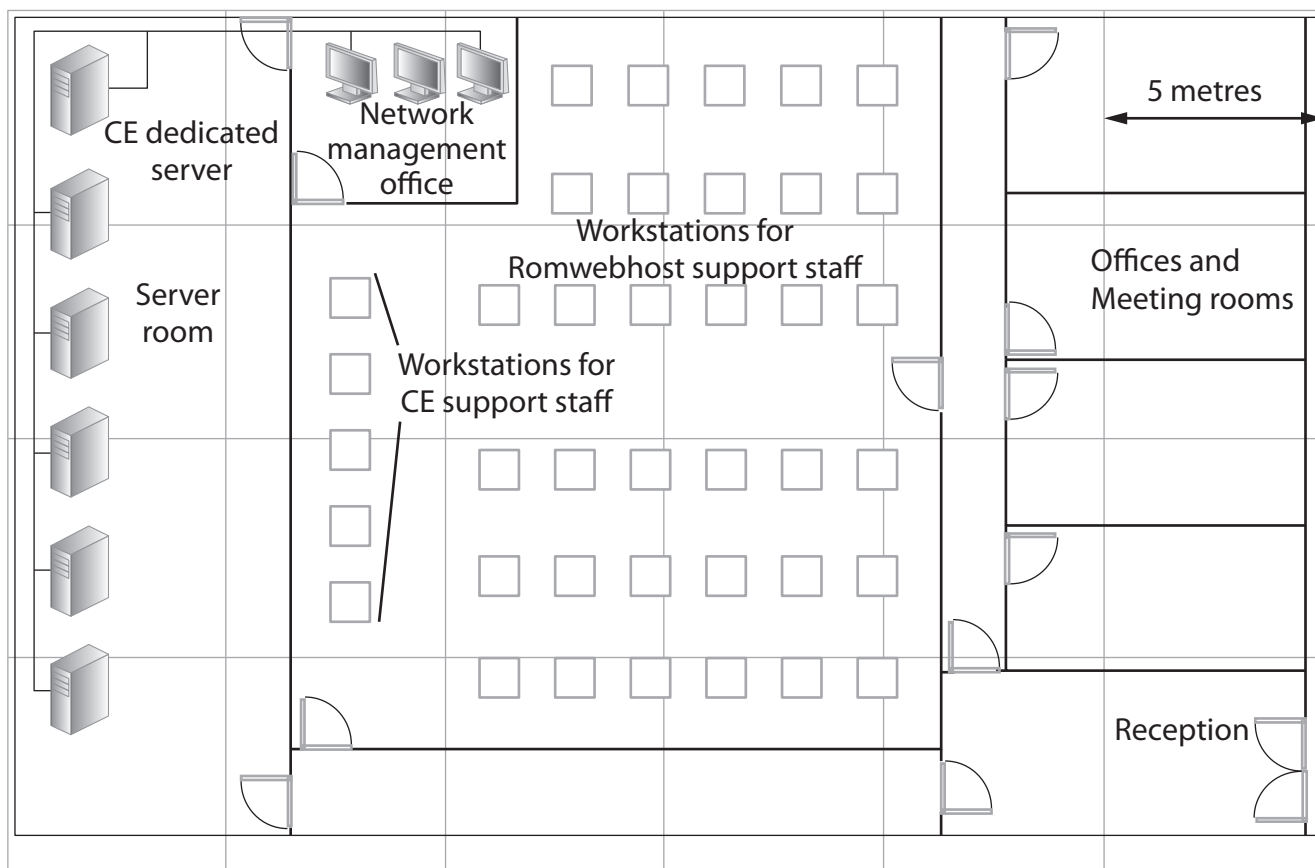


Figure 2

Development plan

During a video conference with Peter and Elana you agree these points on the development of the CE system at Romwebhost.

1. The network will conform to Peter's outline network diagram (**Figure 1**).
2. Romwebhost's staff will create a CriticallyEndangered.com website.
3. The game forum will be moved to the new website and the players who run the current forum will be asked to administer it.
4. The website will have a section for taking payments, using common online payment methods.
5. Peter, Elana and some of Romwebhost's technical staff will have full administrative access to both the website and the CE server.
6. Peter will be responsible for maintaining the program that creates CE play areas. This includes maintaining any accounts required for accessing external data sources.
7. Romwebhost's technical staff will use the backup system that is currently employed in the web hosting business to make regular backups of the CE server.
8. Players' game accounts will be held on the CE server and additional capacity will be added as required.
9. After a player logs on to their account and joins a public game, their connection will be transferred to a virtual server.

10. Private games will involve a one-time download, public games will involve frequent two-way data transfer between the players and the CE server.
11. Players with private games may invite friends to join them by linking over the internet.

Part A Set Task

You must complete ALL activities in the set task.

Read the set task brief 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 set task brief.

Design cyber security protection measures for the given computer network.

Activity 1: Risk assessment of the networked system

Duplicate (copy and paste) and complete the risk assessment using the template given for each threat.

Produce a cyber security risk assessment using the template **Risk_Assessment.rtf**

Save your completed risk assessment as a PDF in your folder for submission as **activity1_riskassessment_[Registration number #]_[surname]_[first letter of first name]**

You are advised to spend 1 hour and 30 minutes on this activity.

(Total for Activity 1 = 8 marks)

Activity 2: Cyber security plan for the networked system

Using the template **Security_Plan.rtf** produce a cyber security 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 cyber security plan using the template given for each protection measure, as appropriate.

Save your completed security plan as a PDF in your folder for submission as **activity2_securityplan_[Registration number #]_[surname]_[first letter of first name]**

You are advised to spend 2 hours and 30 minutes on this activity.

(Total for Activity 2 = 20 marks)

Activity 3: Management report justifying the solution

Produce a management report, justifying how the proposed cyber security plan will meet the security requirements of the set task brief.

The report 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 management report as a PDF in your folder for submission as **activity3_managementreport_[Registration number #]_[surname]_[first letter of first name]**

You are advised to spend 1 hour on this activity.

(Total for Activity 3 = 12 marks)

TOTAL FOR TECHNICAL LANGUAGE IN PART A = 3 MARKS

TOTAL FOR PART A = 43 MARKS