L3 Lead Examiner Report 1806

June 2018

Level 3 National in Information Technology.

Unit 11

Cyber Security and Incident Management

Edexcel and BTEC Qualifications

Edexcel and BTEC qualifications come from Pearson, the world's leading learning company. We provide a wide range of qualifications including academic, vocational, occupational and specific programmes for employers. For further information visit our qualifications website at http://qualifications.pearson.com/en/home.html for our BTEC qualifications.

Alternatively, you can get in touch with us using the details on our contact us page at http://qualifications.pearson.com/en/contact-us.html

If you have any subject specific questions about this specification that require the help of a subject specialist, you can speak directly to the subject team at Pearson. Their contact details can be found on this link:
http://qualifications.pearson.com/en/support/support-for-you/teachers.html

You can also use our online Ask the Expert service at https://www.edexcelonline.com
You will need an Edexcel Online username and password to access this service.

Pearson: helping people progress, everywhere

Our aim is to help everyone progress in their lives through education. We believe in every kind of learning, for all kinds of people, wherever they are in the world. We've been involved in education for over 150 years, and by working across 70 countries, in 100 languages, we have built an international reputation for our commitment to high standards and raising achievement through innovation in education. Find out more about how we can help you and your learners at: www.pearson.com/uk

August 2018
Publications Code 20158K _1806_ER

Grade Boundaries

What is a grade boundary?

A grade boundary is where we set the level of achievement required to obtain a certain grade for the externally assessed unit. We set grade boundaries for each grade, at Distinction, Merit and Pass.

Setting grade boundaries

When we set grade boundaries, we look at the performance of every learner who took the external assessment. When we can see the full picture of performance, our experts are then able to decide where best to place the grade boundaries – this means that they decide what the lowest possible mark is for a particular grade.

When our experts set the grade boundaries, they make sure that learners receive grades which reflect their ability. Awarding grade boundaries is conducted to ensure learners achieve the grade they deserve to achieve, irrespective of variation in the external assessment.

Variations in external assessments

Each external assessment we set asks different questions and may assess different parts of the unit content outlined in the specification. It would be unfair to learners if we set the same grade boundaries for each assessment, because then it would not take accessibility into account.

Grade boundaries for this, and all other papers, are on the website via this link:
http://qualifications.pearson.com/en/support/support-topics/results-certification/grade-boundaries.html

Unit 11 Cyber Security and Incident Management

Grade	Unclassified	Level 3		
		P	M	D
Boundary Mark	0	24	40	57

Introduction

Although the overall specification was first examined in 2017, this was the first sitting for Unit 11, Cyber security and incident management.
The examination is based on a scenario and consists of five activities, three in Task A and two in Task B.
Task A involves the production of a risk assessment and cyber security plan for a specified network. Task B involves the analysis of a reported cyber security incident relevant to the specified network.

Introduction to the Overall Performance of the Unit

The number of entries for the examination was low, meaning that analysis of performance is of limited value. However, it was clear from the scripts seen that the majority of learners were able to understand the scenario and produce the required documents.
It was also clear that many learners had read or been taught the Sample Assessment Material and had learned some appropriate, if generic, responses. Unfortunately, some of these responses did not apply to the 1806 paper and some learners scored less well than they might have done because they included irrelevant material.
The ability of learners to perform the two tasks, was surprisingly different, with some giving good answers to one task but seemingly floundering in the other. Although the activities require somewhat different skills, it was expected that learners would perform evenly over the whole examination.

Individual Questions

Task A

Activity 1 – Risk assessment of the networked system

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.

Nearly all the learners managed to fill in the template with estimates of threat probability and size of loss, but a disappointingly large number were, then, unable to use these estimates to look up the correct severity value in the matrix.

The first example shows a poor usage of the template, with an ill-defined threat and vague wording for the size of loss.

Threat number.	1
Threat title.	Unauthorised Physical Access
Probability.	Unlikely
Potential size of loss / impact level.	Generally around either Minor or Moderate. However I'd say more towards moderate, depends on the situation really.
Risk severity.	Low.
Explanation of the threat in context.	Generally speaking this is when a person, who is unauthorised, is able to access secure and confidential data. This could possibly result in a massive loss of data if said person had malicious intentions. This would have a heavy loss on income as well, due to trust lost from customers who would move to another trustworthy company. Again, the threat risk level would be low. Due to the security measures to actually access the building (card scanners at the door) are pretty complex, this would most likely stop an intruder.

The next learner gives a good estimate of the risk but does not clearly identify the threat, although, in this case, the explanation makes up for the weakness of the threat title. It would be better to title it something such as 'an SQL injection attack via the internet connection'. This learner has also put much of the explanation of the threat in the 'Potential size of loss' box.
An inability to complete the template correctly is likely to impinge on the Technical Language mark and may also lead to poor planning for subsequent activities.

Threat number.	1
Risk severity.	Medium
Threat title.	A database is used to store information on freelance trainers and assessors.
Probability.	Likely
Potential size of loss / impact level.	Moderate as this database doesn't contain information of payment details. However, without the information stored on this database, the BCTAA won't be able to operate. This breaches the data protection act as BCTAAA failed to protect information. This also leads to a financial loss, as fines may have to be paid. People are likely not to trust this company as much which will lead to a reputation loss.
Explanation of the threat in context.	Attack via an internet connection, for example an SQL injection attack, will enable the attacker to gain access to the database, which will become a target as it contain a lot of important information.

The final example shows correct usage of the template and is worthy of band 3.

Threat number.	1
Threat title.	Attack via Wi-Fi connection
Probability.	Very likely
Potential size of loss / impact level.	Major
Risk severity.	Extreme
Explanation of the threat in context.	The office is placed on the 19th floor of a 20 storey building with a restaurant and coffee bar above the office and a bar-café on the roof. There is also a gym and art gallery on the lower floors. This results in many visitors that will be walking around the company offices. An unauthorised user or hacker, can connect to the company Wi-Fi and use automated scanners to find any open ports or software vulnerabilities in the network. The unauthorised user or hacker will use open ports to connect to the network where he can access company files or plant malware such as spyware. This will grant the hacker full access to the BCTAA network where he can cause permanent damage to the company.

Another common error was the identification of non-cyber security threats such as burglary or fire. These threats are not penalised in the marking but learners who identified several such threats tended to get lower marks because they (a) spent valuable time on them and (b) usually only identified a small number of actual cyber security threats as they had already filled a page or two with the non-cyber threats.

Activity 2 – Cyber security plan for the networked system

This activity requires learners to produce a cyber security plan based on their risk assessment from Activity 1. A template is provided for learners to complete.

As with Activity 1, the great majority of learners used the template correctly. Those who could not or would not do so were likely to gain lower Technical Language marks.

Although the threats dealt with Activity 2 should be the same ones that are risk assessed in Activity 1, marking of Activity 2 is independent of Activity 1. This means that an erroneous estimate of threat severity or overemphasis on generic risks does not directly affect the marking. Although having a number of non-cyber security threats was disadvantageous for the reasons given for Activity 1.

Activity 2 requires that the learner demonstrate an understanding of the threats that they have identified. They also must tailor protection measures and testing to meet those threats.

Top band answers do not need to be perfect but a good answer such as the one below uses all the headings in the template and give sufficient detail to demonstrate understanding of the threat and how it can be countered.
Where one of the constraints has little or no relevance, learners should say so rather than leave the heading out. This indicates that the learner has considered the matter and not simply ignored it.

Threat(s) 2, Misconfigured SSIDs
Action to Take: Check the SSIDs of the network and reconfigure them to what is needed, taking measures to not show the staff one to the public (visitors), or even using MAC addresses to only allow devices approved by the network to be connected to the staff network.
Reasons for Action: If the staff network is visible to the visitors, this can cause a

potential threat as it would allow people to try gain access to the network via attacks or password infiltration, for which if the staff network is not visible to the public it would mean that scanners may not be able to pick up the network and would only see the visitor one, which even if accessed won't allow people into the staff only section of the network. Normally routers would come with a default username and a strong password however in some cases old routers may not have that and may have weaker passwords which could be easier to crack.
Constraints:
- Technical: Minimal technical constraints as most routers come with settings to configure MAC addresses for the network, along with the internet being available to provide help to the user, however sometimes there can be a limit to how many MAC addresses can be entered (may not be enough for all staff)
- Financial: Minimal, if router MAC address limit is reached within router, contact ISP to find out cost for more.

Legal Responsibilities: None, data is not affected during this protection measure.
Usability of System: Minimal changes made to the system itself, system still should be used as normal.
Cost-Benefit: The benefits outweigh the costs in this protection measure.

The test plan should of course match the identified threat. It does not need to be particularly detailed as the system is hypothetical and learners cannot be expected to know the exact set up. It should however consist of relevant tests that could reasonably be carried out as shown in this example.

Test No	Test description	Expected outcome	Possible further action following test
3	Set a weak password	Weak password should be denied and user should be asked to set strong password.	If this does not happen, reconfigure the section and try again
4	Scan for networks	Only visitor network should be visible, staff should be hidden.	If staff is visible, reconfigure to make sure staff network is invisible, and try again.

The next example although addressing a reasonable situation, power failure, shows a weak understanding of the scenario as it is unlikely that a company occupying some offices in a multi-story building would be allowed to turn the power off on an entire floor. The test is therefore much less reasonable and in this case, the possible further action does not really follow from the expected outcomes of the test.

Test No	Test description	Expected outcome	Possible further action following test
1	Turn the power off on the floor and let the backup power turn on to open the doors	The backup power should allow the door to open	Have the power work for the system and keep it running so it can take a complete save

Activity 3 – Management report justifying the solution

The result of this activity should be a Management Report, justifying the solution presented in the previous activities.

Learners are told that:

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.

Learners should also be able to analyse the information from the scenario to determine at what level to pitch the report. They were told:

Your contact is Baljinder Singh. He is an experienced computer user and is responsible for the current network, but he admits that the current system is "a bit cobbled together" and "just had stuff added when we thought it was needed".

This, together with other information in the scenario indicates that Baljinder is unlikely to be an IT professional and that the language should be accessible to a non-specialist.

It is expected that a top band report would be laid out correctly, including; a title, a summary or introduction, a main body split into sub-titled sections or bullets, and a section with conclusions or recommendations. Although this final section could be integrated into each of the ones in the main body.

The Technical Language trait is assessed over the whole of Task A, but the ability of a learner to use an appropriate report format and to pitch the language at a suitable level for the target audience will certainly influence the mark awarded.

Task B

Activity 4 – Forensic incident analysis

In this activity learners must analyse both the Task B scenario and the evidence items that are presented. The scenario will be related to the one from Task A but will be shifted in time, location, or both. In this case the Task B scenario occurs a few weeks later than the Task A scenario, when the company involved, Black Country Training and Assessment (BCTAA), has moved to new premises.

The learners are given a template to copy and complete for each piece of evidence that they consider. Most candidates managed this successfully, although many did not do anything about the evidence contained in the Client Brief and Set Task Brief. An inability to complete the template correctly is likely to impinge on the Technical Language mark for Task B.

The weakest part of learners' answers, even for those with higher band marks, was Method of acquiring the evidence.

With some items of evidence, such as Evidence item 2. Summary of a meeting with the block management company. The method of acquiring the evidence would not require much description, e.g. *Jalpinder's notes from the meeting*. Other items such as Evidence

item 3. Annotated door access control log, give more opportunity for learners to display some technical knowledge. e.g.:

> *There are regular logs that are kept everyday of who enters the private area of the building. The logs can be held as a printout or on a database in a graph. Information such as the time and the card number who has entered is shown.*
>
> *The evidence was provided by accessing the card reader software and looking at the log which is recorded. The log contains information such as;*
>
> - *Card number – Each person has a unique card number which allows the person who entered to be easily identified.*
> - *Date-Time – Time and Date the person entered or exited the office.*
> - *In/out – Did the person entered or exited the office*
> - *Note – detail about who entered such as cleaning staff, security check and incidences.*

Weaker answers were along the lines of, *this evidence was acquired from the log.*

The template calls for a conclusion to be drawn from each individual piece of evidence as well as an overall conclusion. Learners need to understand that individual pieces of evidence may not lend themselves to any particular conclusion and any one piece of evidence taken by itself is unlikely to give the full picture. Learners who omitted the overall conclusion tended to be restricted to lower band marks.

Most learners realised that the incident hinged on the door entry cards. Unfortunately, the majority then went on to say that the cards must have been stolen / pick-pocketed, despite the fact that no cards are reported as being stolen in the scenario.

In conclusion I believe that the most likely explanation is that while the BCTAA party was taking place on the 20th floor at the restaurant and bar where there had been reports of thefts and pickpocketing in the same day, is where the senior manager had his card pickpocketed. After his card was pickpocketed, the thieves used it to gain access past the controlled doors into the informal seating and work area where the devices were unprofessionally left out.

The answer is still possible, but it would require the thieves to have replaced the cards after using them.

A better answer is that the cards were skimmed / cloned and the thieves used these clones to gain entry.

On the other hand, another way in which they potentially gained access of these cards was due to using cloning NFC cards, providing them with all the information they would need.

Activity 5– Management report on security improvements

The result of this activity should be a Management Report. As with Activity 3, the report should look like a report and be written at a level suitable for the target audience.

It is expected that a top band report would be laid out correctly, including; a title, a summary or introduction, a main body split into sub-titled sections or bullets, and a section justifying the conclusions or recommendations. Although this final section could be integrated into each of the ones in the main body.

Learners are told that:

Areas for improvement are:
• adherence to forensic procedures
• the forensic procedure and current security protection measures
• the security documentation.

Although Activity 5 is marked independently of Activity 4, there is inevitably a close link between them, since learners who were unable to reach at least plausible conclusions in activity 4 would be hard pressed to identify and combat the weaknesses inherent in the scenario.

Good answers concentrated on the mistakes made.

Mistakes that were made
1. Laptop and phones had been left out and plugged in, instead of being securely out of sight.
2. Insurance claim was not made.
3. Serial numbers of laptops and phones were not taken/recorded as well as IMEI identifiers of smartphones.
4. No realisation of what other items may be missing until a search for the laptop took place.
5. No attempt at asking for witnesses and their statements from anyone in the area including security, maintenance workers and cleaners.
6. Leaving employee cards out of sight, making it easier to steal.
7. No checks to see if employees still possess their cards.
8. No check on card system to see if there is abnormal activity
9. No checks with security to see if they saw anything strange, while checking the premises.
10. No check on network to see if access could've been granted this way
11. No police investigation such as forensics and foot/fingerprint took place, to catch potential suspects.
12. Data was not remotely wiped from the laptop using Find My Device software, even though the tool offers this facility.
13. Laptop was not remotely password locked using Find My Device software, even though the tool offers this facility.

Less good answers had a mixture of mistakes, statements about the system, and possible solutions.

Mistakes made
1. All devices should have been checked before everyone left
2. The person with card 26 shouldn't have let everyone out
3. The missing items were used for meetings in the informal seating and work area.
4. There weren't any strong username and passwords to login to the devices.
5. CCTV was inconclusive which means there needs to be more cameras and the quality needs to be improved.
6. They didn't make any claims on the devices which means they would have to purchase these devices again.
7. The button which allows people to leave needs to be removed. So if someone enters the building and they use the button they could be blamed for incidents as its not on the log that they left the building just that they entered.
8. All the networks are on the main switch which links the guest and staff network.
9. There should have been an alarm system put into place when the devices have left the

building.

In the security documentation section, good answers both identify the weakness and give a suggested replacement or additional text to be used.

The policy also gives out no instructions about preserving evidence or securing the scene of an incident, which would aid the investigation regarding the incident. This must be included in the policy. For example, for each procedure, there should be instructions such as:
Hardware theft
1. Ensuring CCTV footage is analysed and downloaded if possible.
2. Take up eye witness accounts and statements from staff and people who were near the location.
3. Keep staff and visitors away from the incident location.
4. Ensure that tracking software on the devices is immediately turned on and remotely locked and wiped, to prevent data theft and unauthorised access.

Summary

Based on their performance on this paper, learners should:

- *learn how to use the templates before the examination date. The templates are fixed and will be used for every examination*
- *learn how to set out a formal report, The suggested sub-sections are fixed and will be asked for in every examination*
- *read the scenario carefully, looking for specific mentions of security threats, and worries or concerns of the people involved*
- *avoid the pre-planning of answers based on the sample assessment material or previous examinations. Although many of the threats will be similar, the context will be different*
- *ensure that the risk severity is plausible and that related threats such as attacks on two different WiFi systems don't have wildly different risk analyses*
- *look at all the evidence. This includes the scenario as well as the individual evidence items*
- *look at each evidence item separately to draw a conclusion for that evidence item*
- *look at all of the evidence holistically to come to an overall conclusion. This may contradict an individual conclusion*
- *refer to specific sub-sections / pieces of text when discussing changes to the Incident Management Policy*

For more information on Edexcel qualifications, please visit
http://qualifications.pearson.com/en/home.html

Pearson Education Limited. Registered company number 872828
with its registered office at Edinburgh Gate, Harlow, Essex CM20 2JE