T-LEVELS | IfATE Institute for Apprenticeships and Technical Education

Chief Examiner Report

T Level Technical Qualification in Digital Support Services
QN: 603/6901/2

Summer 2025 – occupational specialism (OS) Cyber Security

NCFE

Introduction

Summer 2025 – occupational specialism (OS) Cyber Security

Assessment dates: **19 March 2025 to 30 April 2025**

Paper number: **P002589, P002590 and P002591**

This report contains information in relation to the externally assessed component provided by the chief examiner, with an emphasis on the standard of student work within this assessment.

The report is written for providers, with the aim of highlighting how students have performed generally, as well as any areas where further development or guidance may be required to support preparation for future opportunities.

Key points:

- grade boundaries
- standard of student work
- evidence creation
- responses to the external assessment tasks
- administering the external assessment

It is important to note that students should not sit this external assessment until they have received the relevant teaching of the qualification in relation to this component.

Grade boundaries

Grade boundaries for the series are:

	Overall
Max	250
Distinction	179
Merit	133
Pass	88

Grade boundaries are the lowest mark with which a grade is achieved.

For further detail on how raw marks are scaled and the aggregation of the OS element, please refer to the Qualification Specification.

Administering the external assessment

The external assessment is invigilated and must be conducted in line with our Regulations for the Conduct of External Assessment document. Students may require additional pre-release material to complete the tasks. These must be provided to students in line with our regulations.

Students must be given the resources to carry out the tasks and these are highlighted within the Qualification Specific Instructions for Delivery (QSID) document.

Standard of student work

This is the first series that students have been able to complete the occupational specialism (OS) in Cyber Security. The OS is a synoptic assessment which students undertake in the final year of their T Level qualification.

The OS consists of three assignments which students complete during the assessment period.

Performance for this cohort is in line with what would be expected for an assessment of this type. Students were able to access the various tasks across the three assignments, with some students completing the tasks in greater depth than others.

Evidence creation

There was a range of evidence presented this year across the three assignments for this OS. This included completed reports, screenshots of completed tasks, annotated photographic evidence and risk assessment documents.

The quality of the evidence was generally of a good standard which made it easier for the examining team to understand the steps and processes that students have followed in generating their evidence. It is important that for future cohorts that students continue to be aware that the list of evidence provided in the assignment briefs is the minimum level of evidence that is required. Students can include any additional evidence if they feel that this provides a fair reflection of their skills and knowledge.

Responses to the external assessment tasks

Assignment 1
Task 1

Overall, students performed well in this task. Students were able to undertake research into the three software products that the scenario asked them to.

Students demonstrated a range of performance within their project proposal. Higher performing students were able to make recommendations of two examples of each type of software and why these are relevant to the organisation in the scenario. These students included all the different sections that were requested in the scenario when considering each of the products and they made a contextualised justification of which software the organisation should choose and why this would be the most appropriate for their specific circumstances and needs. These students also were able to consider the legal implications of each piece of software, and they were able to make recommendations on a range of appropriate access controls the organisation should implement.

Students who performed less well were able to make recommendations of the three different types of software for the organisation. These students tended to provide some good detail on some of the areas of comparison but may not have covered all areas or some areas were less well considered. These students did not always include reference to the legal and security requirements of the software and where they did it was more of a brief overview of the relevant laws than an application of what they meant for the organisation in the implementation of the software. Access controls also tended to be either not attempted or more of a description of different controls the organisation could consider.
To achieve well in this task, students need to make sure that they are planning their time effectively so that they are able to attempt all elements of the task. Legal, security and access control requirements were often poorly attempted or not attempted at all. These are key elements of the task, so students need to ensure that they include these within their written proposal. For the three software products it is important that students identify the different factors that they need to research for each product and then

they need to ensure that they are comparing the different products. Students across all levels of performance clearly demonstrated some good knowledge and research on the three software products; they now just need to ensure that they are able to complete all elements of the proposal.

Assignment 1
Task 2

Overall students were able to perform well in this task. Students provided good, annotated evidence which detailed the steps that they had taken from installing the operating system, setting up the required user accounts, installing anti-malware, back-up solutions and full disk encryption and then running tests to ensure that each element of the installation worked.

Higher performing students were able to provide detailed step by step evidence of each stage of the different installations, with a commentary that explained what they were doing and why. These students were able to demonstrate clear evidence that all of the installed software functioned and that the user accounts they created were operational.

Students that performed less well were able to demonstrate that they were able to install the software and set up the user accounts. The evidence tended to be less comprehensive and, in some instances, simply showed each piece of software functioning; however, they did not detail the installation process which is a vital component of this task. It is clear that all the students in this cohort have the skills and knowledge needed to undertake this task effectively; they just need to focus on ensuring that they provide the evidence to demonstrate this.

To achieve well in this task, students need to make sure that they are including a screenshot of each stage of the installation process. This does not need to be every screen that they see within the process, but it should provide a good overview of each step taken, what the student did and how that resulted in a successful installation.

Assignment 2
Task 1

Overall, students were able to perform well in this task. Students were able to research whether the issues being faced in the scenario were software or malware related. Students were then able to investigate the issues with the three emails and make recommendations on which are likely to have caused the issues being faced. Students were then able to make recommendations for remedial actions that should be taken to resolve the issues.

Higher performing students were able to provide a comprehensive overview of the different issues that could be causing the issues with the device, providing a contextualised justification of what they think may be the issue. These students have then provided a detailed overview of the investigations they have undertaken of each email, their findings and which email they felt was behind the issue. They were then able to suggest remedial actions that the organisation should take and why these would resolve the issue and prevent similar issues in future.

Students that performed less well were able to provide good research on what the problem may be with the device; however, they may have focussed on the malware or software issue more. The justification of what could be causing the issue also tended to be less well developed. These students were able to investigate the emails they were provided with and make recommendations on what they think was causing the issues with the device, though this was not always as developed. They were able to suggest potential remedial actions that could be taken to resolve and prevent the issue.

To achieve well in this task, students need to make sure that they are giving equal consideration to both potential issues in Part (a) and that they make a decision on what they believe is causing the issue in the

scenario. Students are encouraged to attempt this in the format that they find is most effective for them but should ensure that they are providing a discussion. Using a comparison table for example is a valid approach to presenting the evidence; however, care should be taken to ensure that the student includes the right level of depth in their response, which some students using tables tend to struggle with.

In Part (b) it is important that students are considering the scenario in relation to the emails they have been provided with and that they are considering the impact that the email could have on different operating systems. The scenario does not specify which operating system the organisation is utilising so it is important that students are considering how the issues identified may affect the main operating systems they are familiar with, including Windows and Linux. In this series the virtual machines (VM) utilised Linux as the operating system which meant that when some students were reviewing the emails and identified malware, they did not always consider how the issues could affect Windows systems as well. This meant that some students did not fully consider the impact the identified malware would have as they had discounted the issue as not affecting a Linux system. They need to consider the impact of the emails on different operating systems as these are phishing attempts so could affect many users. Therefore, it is recommended that where a situation like this arises, that students do add some commentary around the fact that whilst it may not impact the current operating system, that if the device were to be running Windows, it would pose significant issues and then describe how they would resolve this.

In Part (c) there is no requirement that students implement the remedial actions. There was some good evidence provided by some students that demonstrated their approach to implementing the software they were recommending and why. Students should ensure that they read the task carefully and respond to the task fully. If they then have additional time left and wish to also implement the controls suggested, then they are able to, but this should only be when they are confident all other elements of the tasks are complete.

Some students opted to combine Part (c) with Assignment 2 task 2. Where possible, students should ensure that these are two separate tasks. Whilst there is some crossover in the actions that could be utilised it is important that remember that Part (c) is about resolving the immediate issue and an outline of future recommendations, whereas task 2 focuses more on what actions should be taken for ongoing maintenance. This separation will make it easier for the examining team to award marks for both tasks as there will be a clear justification for each recommendation.

Assignment 2
Task 2

Overall, students were able to perform well in this task. They were able to recommend a wide range of actions that the organisation could take to ensure the network and systems remain safe.
Higher performing students were able to provide a well thought out and structured set of recommendations. These recommendations considered software, policies and procedures, training required and other appropriate actions as well as what upgrades might be needed to implement this. Each of the recommendations included a contextualised justification of how it would prevent similar issues in the future.

Students that performed less well were able to make a range of recommendations, but they were not always contextualised to the organisation in the scenario. There were also some recommendations that might be deemed high importance such as training, updating policies, scheduled back-ups and scans that were not included in the report.

To achieve well in this task, students need to make sure that they understand the current issues that are facing the organisation in the scenario and that they have a clear understanding of the physical, technical and administrative measures that they could utilise to address this and also that they are

providing a justification of how each measure will help to prevent the issue occurring again. Students also need to ensure that they are including the implementation approach, any upgrades that might be needed and if they are able to locate costs whilst researching, that they include these. Inclusion of costs is not a requirement but where students find it as part of their overall research, it may help students to justify the benefits of the methods for the organisation.

Assignment 3
Task 1

Overall, students were able to perform well in this task. Students were able to complete a risk assessment for the organisation based on the company overview they had been provided. Students were asked to consider the physical, technical and administrative risks, considering what the risk was, what issue it posed, the level of risk, what assets were at risk and how the organisation could resolve the risk.

Higher performing students were able to identify a wide range of the risks. These students considered a comprehensive range of risks in each of the categories they had been asked to consider, and their risk assessment was detailed. They were able to discuss why it was a risk to the organisation and the assets that it would impact, why it is important that the organisation addressed the risk and how they could achieve this. They were also able to justify the level of risk that they felt each risk posed to the organisation.

Students that performed less well were able to consider a range of risks. Many students considered a comprehensive number of risks, though this may have had an impact on the depth in which they were then able to consider the risks. These students were able to consider each of the three categories of risk, though they often tended to address one of the categories in more detail than the others. They were able to describe the risks, the risk it posed and how the organisation could reduce or remove the risks.

To achieve well in this task, students need to make sure that they consider each of the three categories of risk in similar depth. Students should ensure that they are striking a balance of quality and quantity of the risks. Having a good range of risks is important but it is as important that the students are providing the explanations of how the risks affect the organisation and how they can mitigate these.

Assignment 3
Task 2

Overall, students were able to perform well in this task. Students were asked to create a report considering controls to include within information security policy.

Higher performing students were able to create a comprehensive report which considered a range of controls and the frameworks that the organisation would need to adhere to when implementing each control. These students were able to provide justifications of how these controls would help the organisation to manage information security incidents.

Students that performed less well were able to consider a number of elements of the report but there were often some gaps. These students were able to provide a range of user and administrative controls, though these may not have considered all the relevant controls. These students tended not to consider the frameworks and standards or where they had, it was more what the framework is rather than how it applied. They also tended not to consider how it would manage information security incidents, and how they would update policies.

To achieve well in this task, students need to make sure that they are including all the information that they are asked to within the report. Students do not need to consider all possible controls, instead they should consider the controls which are most relevant to the organisation’s needs.

Assignment 3
Task 3

Overall, students were able to perform well in this task. Students were asked to create a disaster recovery document to support the organisation in ensuring that they are able to have a fully operational network within 24 hours of any major incident. Students were also provided with healthy sized budget to enable them to make recommendations to support their plans.

Higher performing students were able to create a comprehensive and well-structured disaster recovery document. These students were able to provide a range of recommendations of what the organisation would need to implement. They also were able to provide a detailed budget of the costs of their recommendations.

Students that performed less well were able to provide a disaster recovery document. They were able to provide a range of recommendations of how the organisation can recover their network, though these were not always considered in relation to the 24-hour requirement provided in the scenario.

To achieve well in this task, students need to make sure that they read the scenario and consider what they are being asked to do. Where there is a timescale, it would be beneficial if students had a timeline of what actions would be taken when and what outcome this would have. This would help the students to provide a more robust recovery plan. Where students are provided with a budget it is recommended that students are utilising a large percentage of the budget for their solution. This does not necessarily need to all be utilised in the first year, it may be students opt to provide for ongoing support for a few years; however, in this series many students only utilised around 10% of the budget. Students could also factor in the cost of downtime in their budget based on their suggested recovery plan which may help them to have a better utilisation of the budget provided.

Document information

The T Level Technical Qualification is a qualification approved and managed by the Institute for Apprenticeships and Technical Education.

NCFE is authorised by the Institute for Apprenticeships and Technical Education to develop and deliver this Technical Qualification.