HM Government

T-LEVELS

Chief Examiner Report

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

Autumn 2025 – employer set project (ESP) Cyber Security

NCFE

Introduction

Autumn 2025 – employer set project (ESP) Cyber Security

Assessment dates: **3 November 2025 to 14 November 2025**

Paper number: **P003023**

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

Raw mark grade boundaries for the series are:

	Overall
Max	76
A*	67
A	58
B	49
C	41
D	33
E	25

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

For further detail on how raw marks are converted to uniform mark scale (UMS), and the aggregation of the core component, 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

The standard of work students produced is consistent with previous assessment windows and follows the same pattern regarding task performance. Tasks 1 and 3, demanding higher-order skills and application of knowledge, proved more difficult for students.

Many students demonstrated confidence in their interviews, although they lost marks from adhering too rigidly to their scripts. Higher-achieving students demonstrated the ability to deviate from pre-planned questions to explore points made by the IT manager, developing a deeper understanding of the security issues involved.

Students are improving their approach to writing for both technical and non-technical audiences, with good analytical thinking evidenced. In Task 3, students demonstrated their ability to apply logical problem solving to complex security challenges, although justifications tended to be less well written and remain an area for improvement.

English and mathematics skills (AO4) assessment marks continue to improve, with many students gaining three to four marks.

Evidence creation

Most students submitted well-structured evidence in appropriate formats. The interview audio recordings for Task 2 were, in most cases, of good quality with participants' voices easy to hear and understand. Unfortunately, some providers did not account for background noise, making some recordings more difficult to assess. In some instances, other conversations could be heard in the background. It is paramount that providers minimise distractions and refrain from making disparaging remarks to students once the interview has concluded.

In some instances, the microphone was placed very close to the interviewee, making it easy to hear their responses; unfortunately, this affected how easy it was to hear the student's questions.

Some students would have benefitted from more attention to completeness in their documentation. Test plans occasionally lacked structure, whilst project proposals sometimes omitted network topology diagrams or comprehensive justifications and costings.

There is no need for students to upload their task briefs or Word versions; correctly named PDFs will suffice, and any additional documentation is a waste of time and effort.

Some students are still including hyperlinks in their documents. Due to the scanning process of student evidence, these links become non-functional. Therefore, adding links should be discouraged, even though no penalty is imposed.

Responses to the external assessment tasks

Task 1: fault-finding investigation report

In this task, students were required to review three control documents (A-C):

- Control Document A – current network set-up.
- Control Document A – network topology diagram.

- Control Document B – problems reported by users.
- Control Document C – virtual private network (VPN) management system.

Once this review was complete, students were required to produce a fault-finding report to help resolve user problems. Unfortunately, some students misunderstood the task and focused on producing a generalised security report for the company, ignoring the three user problems entirely. This resulted in a Band 1 mark because the student did not attempt to provide a solution to the three problems.

Fortunately, most students understood the task and addressed at least one of the three user issues, scoring in Band 2 or 3. On occasion, some students identified one of the faults and thought that this would suffice to solve the other two problems.

Despite this misunderstanding, the cohort averaged Band 2, with a mean mark of 2.96 out of 6 (facility of 49.32%). The discrimination index of 0.66 confirms that this task effectively differentiates the stronger performers from the weaker ones. Students who scored well here tended to adopt a systematic, methodical approach to each of the three helpdesk tickets, addressing User A's VPN access issues, User B's WiFi connectivity problem, and User C's intermittent file and print server unavailability. Band 3 responses typically identified the root cause for each user: the exhaustion of VPN licences due to unauthorised shared administrator credentials, the deliberate separation of the WiFi access point from the corporate network, and the DHCP scope conflict where the file and print server's static IP address (192.168.1.2) fell within the router's dynamic allocation range. Weaker responses often conflated these distinct issues or proposed generic security improvements rather than targeted fault resolution.

Task 1: test plan document

Students are expected to create a test plan that provides a clear, structured approach to verify whether the technical issues raised by the three users have been resolved. The range of tests should cover both functional and security aspects. For example, users without administrative rights should not be able to install software, modify settings, test internal user access to the NAS, use the Ping command to verify connectivity between network devices, or search for inappropriate content on the NAS. Many students scored a Band 2 or 3 mark in this task as their test table design was either good or excellent (following the headings given in the brief), and the content demonstrated a reasonable or limited understanding of the faults and testing process.

Compared to the other tasks, the test plan document is the weakest area of performance, with a mean mark of 5.57 out of 16, which falls below the optimal difficulty range. The task remains effective at differentiating student ability, although many students are not adequately prepared for this component. This is clearly an area where centres are recommended to focus significant effort. To achieve Band 3 or Band 4, students need to demonstrate a structured, logical test plan that includes appropriate fields such as user details, test dates, computer specification, proposed tests, expected and actual outcomes, the ability to record changes based on test outcomes, a record of the investigation leading to a solution, and user acceptance of completed work. Band 4 responses included a wide range of tests directly aligned to each fault, for example: reviewing VPN management system logs to verify licence allocation, confirming administrator credentials are not being shared, checking the WiFi access point configuration against documentation, examining DHCP logs for IP address conflicts, and using Ping to verify file and print server connectivity. Providers should encourage students to think beyond simply listing tests and instead explain the expected outcomes of each test in sufficient detail to demonstrate a comprehensive understanding of the testing process.

Task 2: interview

The interview task remains the strongest area of performance, with a mean mark of 3.68 out of 6 which, whilst still within the good range, is the lowest discriminator across all tasks. This is expected, as the

interview format tends to reward baseline communication skills and question preparation, which most students manage competently.

Many students demonstrated confidence in their interview technique, asking relevant questions about security measures, password policies, and remote access procedures. Higher-achieving students deviated from their pre-planned questions to ask follow-up queries based on responses received, developing a more complete understanding of security vulnerabilities. They also give affirmations, paraphrase key points and summarise to confirm understanding.

Most students identified key security issues, including a lack of formal training, the use of shared VPN credentials, and weak password policies. Some students would have benefitted from exploring staff offboarding procedures and access monitoring more thoroughly, as these areas were critical to understanding how former employees might access the network.

Task 2: emails

Communicating the same content to a technical and non-technical audience via email proved more challenging for students. The mean mark was 3 out of 6, indicating that this task effectively separates students who can adapt their communication style from those who cannot. To achieve Band 3, the mark scheme requires sustained application of relevant technical terminology for the technical audience, alongside comprehensive contextualisation for the non-technical audience. Students must also demonstrate an excellent application of analytical thinking and problem solving that identifies a wide range of issues.

Many students adapted their communication style for both audiences. The technical email used terminology such as multi-factor authentication, GDPR compliance, and access control.

Some students clearly distinguished between audiences. Explaining business impact to the HR Director whilst providing implementation details to their Line Manager.

Weaker responses struggled to identify all the security issues uncovered during the interview. Common omissions included:

- personal devices accessing company data
- lack of change management processes
- data protection implications.

Analytical thinking must be demonstrated for a student to earn a Band 3 higher mark.

Task 3: project proposal and mathematics

The project proposal remains the most effective discriminator in the assessment. With a mean mark of 11.50 out of 24, the cohort’s performance was remarkably varied. This task separates those students who can integrate complex technical needs into a coherent, professional proposal from those who simply apply a surface-level approach. The five-band marking grid provides considerable scope for differentiation: Band 5 (20–24 marks) requires comprehensive and highly detailed responses across all four assessment criteria, including network connectivity issues, resolution strategies, equipment and cost judgements, and cyber security mitigations supported by a comprehensive network topology diagram.

Most students identified the fundamental infrastructure weaknesses: the domestic ISP router being inadequate for a 220-employee organisation, Windows Server 2008 reaching end of life, and the flat network topology lacking segmentation. Many recommended replacing the domestic router with an enterprise-grade firewall and managed switches, and the majority produced updated network topology diagrams, although the quality and level of detail in these varied considerably. Higher-achieving students

produced proposals that addressed the full scope of the project requirements outlined in Control Document D. Their responses typically included a clear introduction outlining the current security issues before presenting a structured plan covering network segmentation (separating operational, developmental, and administrative functions), role-based access control to ensure employees only access resources relevant to their role, and properly configured VPN access with dedicated licences for each of the 15 Drone Display teams. Band 4 and Band 5 responses went further, proposing cloud hosting solutions (often referencing Microsoft Azure or AWS as specified in the brief) with geographical redundancy, implementing a Change Advisory Board process for managing network modifications, and providing detailed incident management procedures. These students also demonstrated strong justification skills, explaining why specific equipment was selected and providing cost-benefit analysis for larger purchases. Weaker responses tended to list security improvements without contextualising them to the Shooting Star Drones Ltd scenario. A common shortcoming was proposing generic network upgrades without addressing the specific requirements, such as ensuring all Drone Display teams could download display configurations remotely or providing secure separation between the display creation environment and the operational side of the business. Some students neglected to consider the company's anticipated growth over the next 5 years, proposing solutions that addressed current needs without scalability. Others omitted key elements entirely, such as staff security awareness training, offboarding procedures for leavers, or the WiFi configuration needing to support both staff and guest use securely. Network topology diagrams in weaker responses were often incomplete, missing key components such as firewall placement, VLAN segmentation, or the relationship between cloud services and on-premise infrastructure.

Suggestions for multi-factor authentication and improved VPN configuration were common across most responses. However, several important security considerations were frequently absent. Fewer students addressed encrypted connection protocols for all VPN traffic, mobile device management for the Drone Display teams' corporate devices, or granular password policies to replace the weak administrator credentials ("12345678") identified in Control Document C. The need to disable the shared administrator login and implement individual authenticated accounts for all remote users was a critical security issue that stronger students identified and addressed comprehensively, whilst weaker students overlooked it entirely. Similarly, the data protection implications under UK GDPR and the Data Protection Act 2018, particularly regarding staff using personal devices to access company data, were discussed effectively by higher-achieving students but omitted by many in the lower bands.

Task 3: mathematics

Mathematical skills in this task were weaker than usual. The mean mark of 0.79 out of 2 indicates that many students struggled with accurate costings. The AO4 mathematics mark scheme requires accurate calculations with appropriate units for Band 2. Students who achieved full marks typically included detailed cost breakdowns with VAT calculations, whole-life support costs, and cloud service estimates. Weaker responses often omitted VAT entirely, presented round-number estimates without justification, or failed to include support costs over the lifetime of equipment.

Task 4: sample satisfaction survey

Students were required to create a satisfaction survey to measure user responses to the implemented security improvements. The mean mark was 2.58 out of 6. This suggests that whilst many students grasped basic survey design, fewer demonstrated the comprehensive and highly detailed approach required for Band 3.

Most students demonstrated a reasonable understanding of survey design, including questions that assessed ease of use, network security confidence, and access to resources. Higher-achieving students designed professionally formatted surveys with a balanced mix of question types: Likert scales for measuring satisfaction levels (for example, rating network performance from 1 to 10), yes/no questions for confirming specific functionality (such as whether users could access the network remotely), and

open-ended qualitative questions to capture detailed user feedback. These stronger responses also included questions that gathered contextual information about the respondent, such as their job role and self-assessed technical ability, which would help interpret the survey results meaningfully. Weaker responses tended to rely heavily on one question type, often producing a list of closed yes/no questions that would provide limited insight into the effectiveness of the implemented solution. Some students failed to format their surveys professionally for a non-technical audience, using overly technical language that would not be appropriate for distribution to all staff at Shooting Star Drones Ltd.

The mark scheme required surveys that could comprehensively measure the effectiveness of the solution. This means systematic coverage across multiple areas: system performance improvements, confidence in the new security measures, accessibility of network resources, remote connectivity for the Drone Display teams, and the adequacy of any new training provision. Band 3 responses achieved this breadth of coverage whilst maintaining a professional, user-friendly format. Band 1 and Band 2 responses typically focused on only one or two of these areas, often concentrating solely on general satisfaction without probing the specific security improvements that were central to the project.

Task 4: project summary

This task required students to provide a project summary that included the original network issues, the solutions implemented, the security mitigations applied, and a self-evaluation. The mean mark of 2.82 out of 6 demonstrates that the task effectively identifies students who can synthesise and reflect on their project work. The mark scheme for Band 3 requires an excellent understanding of key issues, supported by the sustained application of relevant technical terminology, alongside an excellent, highly detailed self-evaluation.

Most students provided a reasonable overview of the project, identifying the key issues from the original network: VPN access problems caused by shared administrator credentials and insufficient licences, IP address conflicts between the file and print server and the DHCP scope, security vulnerabilities arising from the lack of network segmentation, and the inadequacy of the domestic ISP router. Students generally summarised their proposed solutions, including network segmentation, improved authentication, infrastructure upgrades, and adoption of cloud services. Higher-achieving students structured their summaries using a relevant reflective cycle, such as Gibbs' reflective cycle, to provide a coherent framework for their evaluation. These students used sustained technical terminology appropriate for their line manager (a technical audience), referencing specific technologies and configurations from their Task 3 proposal. Band 3 responses also demonstrated a clear link between the issues identified, the proposed solutions, and the implemented security mitigations, presenting a cohesive narrative rather than a disconnected list of points.

The self-evaluation component proved problematic for many students. A significant number produced generic statements about “working harder” or “managing time better” rather than critically evaluating their actual project decisions and outcomes. Good responses demonstrated genuinely reflective analysis, discussing specific strengths in their approach (for example, the effectiveness of their network segmentation strategy or their cost-benefit analysis) alongside honest acknowledgement of weaknesses (such as areas where their proposal lacked detail or where their costings could have been more thorough). The strongest self-evaluations identified concrete areas for improvement, such as developing deeper knowledge of cloud hosting pricing models, improving the level of detail in network topology diagrams, or conducting more thorough research into equipment specifications. These students articulated clear lessons learned that would inform their approach to future projects, demonstrating the kind of professional reflection expected in a workplace cybersecurity role.

Weaker self-evaluations remained superficial, offering general observations without critically analysing their own decision-making process or project outcomes. Some students simply restated what they had done in Task 3 without evaluating how well their proposals addressed the brief's requirements. Providers should encourage students to engage meaningfully with reflective practice, focusing on the quality and

appropriateness of their technical decisions rather than generic commentary about effort or time management.

Tasks 2, 3 and 4: English skills (AO4)

English skills were assessed holistically across written work in Tasks 2, 3, and 4. The cohort achieved an average of 2.83 out of 4 marks, with approximately 70% of available marks, indicating consistently strong literacy performance.

Most students demonstrated good spelling, punctuation, and grammar accuracy throughout their submissions. The majority achieved Band 3 or Band 4 marks, demonstrating mostly accurate or fully accurate technical communication, with an appropriate professional tone and coherent organisation.

Higher-achieving students maintained professional standards across all written outputs, including emails, technical proposals, and reflective summaries. These students adjusted language appropriately for different audiences whilst maintaining clarity and accuracy throughout.

Document information