T-LEVELS | Institute for Apprenticeships & Technical Education

T Level Technical Qualification in Digital Support Services

Occupational specialism assessment (OSA)

Cyber security

Assignment 3

Mark scheme

v1.1: Specimen assessment materials
21 November 2023
603/6901/2

Internal reference: DSS-0013-06

NCFE

T Level Technical Qualification in Digital Support Services
Occupational specialism assessment (OSA)

Cyber Security

Mark scheme

Assignment 3

Contents

Marking guidelines

General guidelines

You must apply the following marking guidelines to all marking undertaken throughout the marking period. This is to ensure fairness to all students, who must receive the same treatment. You must mark the first student in exactly the same way as you mark the last.

The mark scheme must be referred to throughout the marking period and applied consistently. Do not change your approach to marking once you have been standardised.

Reward students positively giving credit for what they have shown, rather than what they might have omitted.

Utilise the whole mark range and always award full marks when the response merits them.

Be prepared to award 0 marks if the student's response has no creditworthy material.

Do not credit irrelevant material that does not answer the question, no matter how impressive the response might be.

The marks awarded for each response should be clearly and legibly recorded.

If you are in any doubt about the application of the mark scheme, you must consult with your team leader or the chief examiner.

Guidelines for using extended response marking grids

Extended response marking grids have been designed to award a student's response holistically for the relevant task or question and should follow a best-fit approach. The grids are broken down into bands, with each band having an associated descriptor indicating the performance at that band. You should determine the band before determining the mark.

Depending on the amount of evidence that the task produces, the grids will either be a single, holistic grid that covers the range of relevant performance outcomes (POs), and will require you to make a judgement across all the evidence, or they will consist of multiple grids, that will be targeted at specific POs, and will require you to make a judgement across all the evidence in relation to that particular grid in each case, therefore making multiple judgements for a single task to arrive at a final set of marks. Where there are multiple grids for a particular task, it is important that you consider all the evidence against each of the grids, as although the grids will focus on particular POs, awardable evidence for each grid may come from across the range of evidence the student has produced for the task.

When determining a band, you should look at the overall quality of the response and reward students positively, rather than focussing on small omissions. If the response covers aspects at different bands, you should use a best-fit approach at this stage and use the available marks within the band to credit the response appropriately.

When determining a mark, your decision should be based on the quality of the response in relation to the descriptors. Standardisation materials, marked by the chief examiner, will help you with determining a mark. You will be able to use exemplar student responses to compare to live responses, to decide if it is the same, better or worse.

To support your judgement, the indicative content is structured in such a way that mirrors the order of the different points within the band descriptors. This will allow you to use the 2 in conjunction with each other by providing examples of the types of things to look for in the response, for each descriptor. In other words, the indicative content provides you with a starting point of possible examples and the bands express the range of options

available to you in terms of the quality of the response. You should apply the standards that have been set at relevant standardisation events in a consistent manner.

You are reminded that the indicative content provided under the marking grid is there as a guide, and therefore you must credit any other suitable responses a student may produce. It is not a requirement either that students must cover all of the indicative content to be awarded full marks.

Performance outcomes

This assessment requires students to:

PO1: Apply procedures and controls to maintain the digital security of an organisation and its data

PO2: Propose remediation advice for a security risk assessment

PO3: Discover, evaluate and apply reliable sources of knowledge

Task 1: security risk assessment

Band	Mark	Descriptor
4	23–30	An **excellent** and in-depth risk assessment that comprehensively identifies a wide range of risks within the scenario provided. A **detailed** explanation of the risks that have been identified, which have been thoroughly risk rated using the provided template. An **excellent** explanation of how the risk could be mitigated through the suggested recommended actions.
3	16–22	A **clear** risk assessment that identifies most of the key risks within the scenario provided. A **good** explanation of the risks that have been identified, which have been clearly risk rated using the provided template. An **appropriate** explanation of how the risk could be mitigated through the suggested recommended actions.
2	8–15	A **satisfactory** risk assessment that identifies some of the risks within the scenario provided. A **sound** explanation of the risks that have been identified, which have been reasonably risk rated using the provided template. A **satisfactory** explanation of how the risk could be mitigated through the suggested recommended actions.
1	1–7	A **basic** risk assessment that identifies a limited range of risks within the scenario provided. A **minimal** explanation of the risks that have been identified, which have been risk rated in a very basic manner using the provided template. A **limited** explanation of how the risk could be mitigated through the suggested recommended actions.
	0	No creditworthy material.

Indicative content

Risk assessment template has been completed including physical, administrative and technical risks. Risks are based on the additional document ‘Company overview’ and can include, but are not limited to:

- physical risks:
  - gate left unlocked
  - dummy cameras being used

  - people using car park not associated with the business
  - door left unlocked
  - fire door left open
  - no alarms
  - windows left open at night
- administrative risks:
  - no procedures for accessing company premises (such as, reception areas, visitors signing in/out, no mantraps to stop tailgating, no biometrics)
  - insufficient or no policies in place (for example, remote access, password, acceptable use, bring your own device (BYOD), insufficient checks at hiring stage for employees)
  - insufficient or no cyber awareness training
  - poor asset management (for example, asset register)
  - reception computer left logged in (requires auto log out of systems if not used for set period)
- technical risks:
  - password policy (such as, recommendations for only changing every 6 months, recommendations for password format rather than policy)
  - local admin rights for software developers installing any software they want to
  - no requirements for anti-virus or firewall as all based on trust
  - service outages
  - system downtime, data loss

Assets, impacts and likelihood contain appropriate explanations, as well as a RAG rating.

Actions are identified with detailed explanations of the actions taken to mitigate these risks. The actions will be linked to the controls detailed below.

Controls should be identified as technical, physical or administrative.

Physical controls could include:

- server room:
  - locked door
  - air conditioned
- physical reception area
- security guard
- door access control, such as key fobs
- Kensington desk locks in hot desk areas
- security alarm on fire door
- close circuit television (CCTV)
- fence/gate in car park

- ID cards

Technical controls could include:

- installation of anti-virus or anti-malware software
- encryption:
  - encrypting file system (EFS) for individual files
  - BitLocker or other disk encryption for laptops
  - BitLocker To Go or removable drive encryption for removable media
- patch management
- removal of unnecessary software or services (hardening)
- configuring file and folder permissions

Administrative controls could include:

- sign in/sign out procedures
- no tailgating policy
- policies – acceptable use policy, password policy, BYOD
- robust procedures in the HR system in relation to staff hiring and management of assets
- security awareness training

Note: The above is not an exhaustive list; credit should be given to other suggestions as appropriate to the scenario in the brief

Task 2: security guidelines recommendations

Band	Mark	Description
4	16–20	An **excellent** explanation and justification for the proposed user and administrative controls to be implemented and **in-depth** reasoning for choosing these controls. An **excellent,** well-written and **comprehensive** description of how each control will be enforced within the business. An **excellent** description of legislation, regulations or standards related to each control. A **detailed** explanation demonstrating a **comprehensive** understanding and justification of the identified considerations for security, manageability and upgradeability in relation to cyber security policies.
3	11–15	A **good** explanation and **appropriate** justification for the proposed user and administrative controls to be implemented and **good** reasoning for choosing these controls. A **good** description of how each control will be enforced within the business. A **good** description of **appropriate** legislation, regulations or standards related to each control. A **good** explanation demonstrating a **good** level of understanding and appropriate justification of the identified considerations for security, manageability and upgradeability in relation to cyber security policies.
2	6–10	A **reasonable** explanation and **some** justification for the proposed user and administrative controls to be implemented and **some** reasoning for choosing these controls. A **satisfactory** description of how each control will be enforced within the business. A **satisfactory** description of **some** legislation, regulations or standards related to each control. A **reasonable** explanation, demonstrating **some understanding** and justification of the identified considerations for security, manageability and upgradeability in relation to cyber security policies.
1	1–5	A **basic** explanation and **vague** justification for the proposed user and administrative controls to be implemented and **limited** reasoning for choosing these controls. A **basic** description of how each control will be enforced within the business. A **basic** description of legislation, regulations or standards related to each control. A **basic** explanation, demonstrating **a vague** understanding and justification of the identified considerations for security, manageability and upgradeability in relation to cyber security policies.

Band	Mark	Description
	0	No creditworthy material.

Indicative content

Student provides recommendations and justifications of potential security controls that could be implemented and their reasons for choosing those controls. This could include but is not limited to:

- password policy:
  - ensuring passwords are hard to compromise and staff understand how best to keep passwords secure
- tailgating:
  - preventing an intruder gaining unauthorised access to the site
- locking screens:
  - preventing unauthorised access of a staff member's account while away from the computer
- encryption of mobile data:
  - ensuring confidential data cannot be accessed in the event of theft or other loss
- mandatory training of staff:
  - reduces user error or social engineering style attacks from giving access to company systems
- installation of firewall, anti-virus or other anti-malware software:
  - reduces risk of malicious malware or viruses accidentally being installed on company computers
- BYOD:
  - details requirements and restrictions when undertaking work activities using personally owned devices

Additional user and administration measures could also include:

- single sign on
- muti factor authentication
- strong password policy
- access control models (for example, mandatory access control (MAC))
- policies and procedures
- zero trust security

Where appropriate students may reference frameworks, standards or regulatory bodies and legislation, such as:

- frameworks:
  - Information Security Management System (ISMS) – used to create policies (for example, information security policy, acceptable use policy) to ensure an organisation is compliant with security and privacy standards

  - Control Objectives for Information and Related Technologies (COBIT) – used in helping organisations to develop procedures and internal frameworks for governance and management of IT systems
  - Service Organisation Controls (SOC 2) – used in assessing an organisation's security, availability, processing integrity, confidentiality and privacy controls
- standards:
  - ISO 27001 information security management – a series of standards to provide best practice for information security management systems
  - National Cyber Security Centre (NCSC) Cyber Essentials – a government backed scheme that supports organisations to protect against cyber attacks and provides accreditation to organisations
- legislation:
  - Data Protection Act (2018)/GDPR
  - Computer Misuse Act
  - Data Protection Policy

Recommended and justified actions and approaches should ensure the most reliable and valid sources are utilised (for example, which sources may or may not be valid and reliable and why).

Note: The above is not an exhaustive list; credit should be given to other suggestions as appropriate to the scenario in the brief

Task 3: disaster recovery document

Band	Mark	Description
4	16–20	An **excellent** explanation and justification for the proposed recommendations in the case of service outages. A **comprehensive**, in-depth explanation of how the actions taken will better protect the company.
3	11–15	A **good** explanation and appropriate justification for the proposed recommendations in the case of service outages. A **good** explanation of how the actions taken will better protect the company.
2	6–10	A **satisfactory** explanation with some justification for the proposed recommendations in the case of service outages. A **reasonable** explanation of how the actions taken will better protect the company.
1	1–5	A **basic** explanation with vague justification for the proposed recommendations in the case of service outages. A **basic** explanation of how the actions taken will better protect the company.
	0	No creditworthy material.

Indicative content

Disaster recovery – focuses on recommendations for what needs to happen to recover the infrastructure in case of a denial of service (DoS) attack.

Business continuity – focuses on recommendations for resuming/maintaining service after a DoS attack leading to a service outage.

An example of a consideration and justification could be:

- all systems are currently housed internally with no redundancy measures visible so the company could consider:
  - moving the infrastructure to a remote site as this would mean that resources and/services are available off site, which would help in the event of a natural disaster
  - the company could introduce a virtualised disaster plan that would create virtual copies of everything, ensuring that there is an option available if the system failed
- by choosing 1 of these 2 options there would be additional resources available that could be used in the event of something happening to the internal network or building

Other things that could be discussed by students include, but are not limited to:

- a network disaster plan that would provide a procedure on how to restore the network and equipment in the event of an incident
- a cloud disaster plan that would consider how data could be backed up off site using cloud services which would allow data to be restored in the event of an incident
- a better back up procedure could be introduced to allow recovery of data in the event of a disaster
- a redundancy server could be introduced to the network so there is a server to fall back on in the event of a failure

Note: The above is not an exhaustive list; credit should be given to other suggestions as appropriate to the scenario in the brief

Performance outcome grid

Task	PO1	PO2	PO3	Total
1	15	0	15	30
2	10	0	10	20
3	10	10	0	20
Total marks	35	10	25	70
% weighting	50%	14%	36%	100%

Document information

The T Level Technical Qualification is a qualification approved and managed by the Institute for Apprenticeships and Technical Education. NCFE is currently authorised by the Institute to develop and deliver the T Level Technical Qualification in Digital Support Services.

Owner: Head of Assessment Design

Change History Record

Version	Description of change	Approval	Date of Issue
v1.0	Post approval, updated for publication		01 June 2023
v1.1	Sample added as a watermark	November 2023	21 November 2023