T Level Technical Qualification in Digital Support Services

Occupational specialism assessment (OSA)

Digital Infrastructure

Assignment 1

Mark scheme

v1.1: Additional sample material
17 November 2023
603/6901/2

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

Digital Infrastructure

Mark scheme

Assignment 1

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 a relevant standardisation event 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 (POs)

This assessment requires students to:

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

PO2: Explain, install, configure, test and manage both physical and virtual infrastructure

PO3: Discover, evaluate and apply reliable sources of knowledge

Task 1: planning

(20 marks)

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

Band	Mark	Descriptor
4	10–12	The vulnerabilities and countermeasures have been explored to a very high level with one or more countermeasures provided for each vulnerability. The exploration has been completed to an exceptional level and the mitigation provided would address the vulnerability. Both physical and digital aspects have been covered. The physical countermeasures have been clearly marked on the floor plan with excellent annotation and outstanding thought regarding placement and impact.
3	7–9	The vulnerabilities and countermeasures have been explored to a good level with one or more countermeasures provided for each vulnerability. The exploration has been completed to a good level and the mitigation provided would address the vulnerability. Both physical and digital aspects have been covered. The physical countermeasures have been clearly marked on the floor plan with effective annotation and good thought regarding placement and impact.
2	4–6	Enough vulnerabilities have been identified and countermeasures have been matched to be considered as suitable. The exploration has been completed to a satisfactory level and the mitigation provided could address the vulnerability, but more viable solutions exist. The physical countermeasures have been marked on the floor plan with reasonable annotation and adequate thought regarding placement and impact.
1	1–3	Some basic threats have been identified and some unlinked countermeasures have been provided covering either physical or digital aspects. Limited evidence of annotation on the floor plan and overall the response feels disconnected from the brief.
	0	No creditworthy material.

Indicative content

For bands 3 and 4, students will consider multiple mitigations. For example, they will identify that the room highlighted for the servers will need ventilation to prevent overheating, or the room must always be locked with limited access to only authorised personnel. The building is vulnerable to potential theft and damages, fobbed systems and mantrap doors could be mitigation for any unauthorised access to the office space.

For bands 3 and 4, the threat must be aligned with the countermeasures.

Examples may include, but are not limited to:

- physical:
  - preventative control techniques (for example, managed access, administrative, policies and procedures, technical, security team or mantrap doors)
  - detective control techniques (for example, CCTV, administrative, policies and procedures - such as logs)
  - corrective control techniques (for example, fire suppression, administrative, policies and procedures - for example, standard operating procedure and IT policies)
  - deterrent control techniques (for example, alarm systems, administrative, policies and procedures such as acceptable usage policies and security)
  - directive control techniques (for example, mandatory ID badge display, administrative, policies and procedures such as regular and compulsory staff training)
  - compensating business control techniques (for example, air conditioning, administrative, policies and procedures such as role-based awareness training)
  - disaster recovery planning (for example, backups, administrative, policies and procedures such as business continuity planning
  - types of impacts that can occur within an organisation as a result of threats or vulnerabilities (for example, danger to life, privacy, property and resources, economic, reputation, legal)
- digital:
  - potential vulnerabilities in critical systems (for example, unauthorised access to network infrastructure, single point of failure, system failure, open port access, wireless networks)
  - breach of the Data Protection Act 2018 and GDPR (for example, customer or client data being leaked out of the building for either incorrect storage or being destroyed incorrectly)
- the impact of measures and procedures put in place to mitigate threats and vulnerabilities:
  - measures (for example, recovery time objective (RTO), recovery point objective (RPO), meant time between failure (MTBF), mean time to repair (MTTR))
  - procedures (for example, standard operating procedure (SOP), service level agreement (SLA), and IT policies and agreements)
  - factors involved in threat assessment for the mitigation of threats and vulnerabilities (for example, environmental, man-made, technological, political)
- types of risk response within a digital infrastructure context (for example, accept, avoid, mitigate, transfer)

The annotations on the floor plan should demonstrate suitable placement of physical countermeasures (for example, monitoring systems covering the server room, keypad entry on the server door, preventative action for clients to limit their access and mantrap doors).

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

PO2: Explain, install, configure, test and manage both physical and virtual infrastructure

Band	Mark	Descriptor
4	7–8	The project plan and Gantt chart have been completed to a high standard, with suitable activities and durations shown against the requirements of the brief. All information provided in the task has been included and the project completion is within the timeframe required by the brief. The student has covered all phases of planning, design, testing, pre-production, deployment, monitoring and evaluation with activities that match the nature of the project, showing an excellent grasp of the task. The account is highly detailed and accurate covering data security, health and safety and the use of anti-static equipment. The laws selected are appropriate to the brief and have been related back with real confidence and understanding of the task.
3	5–6	The project plan and Gantt chart have been completed to a good standard, with mostly relevant activities and durations shown against the requirements of the brief. Only limited errors in the timing requirements, but the project runs for the timeframe required by the brief. The student has covered most of the phases of planning, design, testing, pre-production, deployment, monitoring and evaluation with activities that mostly match the nature of the project, showing a good grasp of the task. The account is detailed and mostly accurate covering data security, health and safety and the use of anti-static equipment. The laws selected are relevant to the brief and have been related back with a good understanding of the task.

Band	Mark	Descriptor
2	3–4	The project plan and Gantt chart have been completed to a satisfactory standard, with some activities shown against the requirements of the brief, but they are mostly generic activities and unrelated to the brief. Some timings are accurate, however overall, the project does not adhere to the timeframe indicated in the brief. The student has covered some areas of planning, design, testing, pre-production, deployment, monitoring and evaluation with reasonable relation to the brief. The account is sufficient and reasonably accurate covering some aspects of data security, health and safety and the use of antistatic equipment. The laws selected are important, but not always appropriate to the brief and have only partially been related back to the task.
1	1–2	The project plan and Gantt chart have been completed to a basic standard with a limited range of activities that are relevant to the brief. The timings for the task are inaccurate and the project does not adhere to the timeframe indicated in the brief. The student has covered only a few areas of planning, design, testing, pre-production, deployment, monitoring and evaluation and these have little relation to the brief. The account is superficial, covering limited aspects of data security, health and safety and the use of anti-static equipment. The laws selected are inaccurate and have very limited relevance to the task.
	0	No creditworthy material.

Indicative content

Project plan and Gantt chart should be clear and logical.

Clear phases of the lifecycle model should be provided and show suitable activities that align to the requirements of the task. Typical activities include, but are not limited to:

- planning – client requirements, develop project specification, technical specification, project plan, risk assessment
- design – traffic forecasting, storage analysis, access control
- pre-production – virtual machine (VM) development, compatibility test
- deployment – server installation, operating system configuration
- testing – shared folders, network access, security policies

- monitoring – response time monitoring, server logs, storage monitoring
- evaluation – user acceptance, functional requirements, penetration testing and mitigation

Note: In bands 1 and 2, the legal, data and static sections may be generic with limited relevance to the brief

Working with equipment:

- health and safety – manual handling, COSHH, training, electrical safety
- data security – Data Protection Act 2018/GDPR, Computer Misuse Act 1990, backing-up
- antistatic – use of wrist straps, mats, bags
- industrial standards and regulatory compliance for security of IT
- principles of network security
- methods of managing and controlling access to digital systems:
  - mandatory access control
  - discretionary access control
  - rule-based access control
  - biometrics and facial recognition
  - mobile credentials
  - touch screens or keypads
  - fob system
  - visitor management

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: design – servers and storage

(28 marks)

PO2: Explain, install, configure, test and manage both physical and virtual infrastructure

Band	Mark	Descriptor
4	16–20	The student has demonstrated exceptional knowledge and experience of server roles and applications required for the network to fully support the demands of the business. From the server OS, through to the wider roles and applications, the detail provided shows excellent subject knowledge. The judgements regarding the architecture of the servers show a high level of subject knowledge in the generation of the solution, with strong evaluative comments that address the demands of the network. The judgements demonstrate a high level of subject knowledge in the generation of the solution, with detailed and considered evaluative comments. The specification of the server and storage exceeds the technical requirements, both functional and non-functional, and covers the demand for the network to grow. An extremely proficient diagram that clearly considers the requirements of the brief and builds a potential solution that solves the problem to a very high standard.
3	11–15	The student has demonstrated good knowledge and experience of server roles and applications required for the network to function, although not all the required roles and applications have been identified. The essential software and roles have been identified. The approach to the server architecture is appropriate, showing refined technical knowledge and justification with some consideration of alternatives provided. The judgements demonstrate a good level of subject knowledge in the generation of the solution with proficient, evaluative comments. The specification of the server and storage addresses the minimum requirements and shows scope for forward planning and expandability. A proficient diagram that delivers on the requirements of the brief and builds a potential solution that solves the problem to a good standard.

Band	Mark	Descriptor
2	6–10	The student has demonstrated satisfactory knowledge and experience of server roles and applications required for a network to function. A range of roles and applications the server and network will require have been identified to a satisfactory level of detail but are not aligned to the demands of the business. The approach to the server architecture is reasonable with some technical knowledge and adequate justification or consideration of alternatives provided, but it does not consider the business or network demands. The servers selected would be viewed as achieving the minimum functional requirements of the task with only storage and operating systems included, but choices are not explored or justified. Some reference to the brief has been included. A satisfactory diagram that mostly addresses the requirements of the brief and builds a potential solution that solves the problem to a reasonable standard.
1	1–5	The student has demonstrated basic knowledge and experience of server roles and applications required for a network to function with gaps evident. Only a few roles have been mentioned in limited detail with little to no consideration for the applications. The approach to the server arrangement is rudimentary with only a basic approach outlined and there is little to no justification related to the brief and alternatives. The servers selected only partially deliver on the functional requirements of the task with only basic storage and operating systems details provided. A functional diagram that addresses the requirements of the brief and builds a solution that could solve the problem with some modification.
	0	No creditworthy material.

Indicative content

The details below will vary based on the approach the student has taken and should be assessed based on the viability to deliver on the requirements of the task.

Server roles and applications:

- the student should select a suitable physical server to purchase with adequate specification to deliver the requirements of the task
- selection of the operating system should be relevant to the task (for example, a network operating system would be more suitable than a client operating system the student must also highlight how a newer server operating system is available
- applications, software and services selected should be suited to the requirements of the task

- examples of software, applications and services may include, but are not limited to:
  - hypervisor
  - server operating system
  - directory services (for example, Active Directory)
  - network services (for example, DNS, DHCP, IIS, FTP)
  - cloud services (for example, Microsoft Azure, Amazon Web Services, Exchange Online)

Server architecture:

- students could recommend one approach or a hybrid approach with some roles virtualised, assess the work based on the technical recommendation and justification
- a case for physical servers with a hypervisor to virtualise the machines, Hyper-V or vSphere are appropriate if the justification is accurate and relevant
- benefits include better hardware utilisation
- failover of virtual machine to another server
- environmental benefits, reduction in heat and power utilisation
- ability to scale out the infrastructure
- consideration to the security and limited access to the server architecture and how a VPN would be required if only a local server was used

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

PO3: Discover, evaluate and apply reliable sources of knowledge

Band	Mark	Descriptor
4	7–8	The sources of information used and the knowledge gained show excellent research skills, utilising sources that are both very reliable and valid, with fully developed comments and consideration of any possible bias in the sources used and how it has impacted on the information gathered. The judgements provided demonstrate an excellent level of critical thinking in the generation of the solution with highly effective evaluative statements.
3	5–6	The sources of information used and the knowledge gained show good research skills, utilising one or more sources that are reliable and valid, with detailed comments including recognition of any bias in the sources of information. The judgements provided demonstrate a good level of critical thinking in the generation of the solution with mostly effective evaluative statements.
2	3–4	The sources of information used and the knowledge gained show moderate research skills, utilising sources that are acceptable in terms of reliability and validity, with a basic comment about the suitability and use. The judgements provided demonstrate a reasonable level of critical thinking in the generation of the solution with some evaluative statements that are partially effective.
1	1–2	The sources of information used and the knowledge gained show only basic research skills, utilising sources that are derived from sites which raise concerns regarding the reliability and validity of the information they contain. Any judgements provided demonstrate a minimal level of critical thinking in the generation of the solution with only limited evaluative statements.
	0	No creditworthy material.

Indicative content

Students can evaluate each source, or all sources combined aiming to justify the sources and validate the quality of the information. For a student to achieve mark band 3 or 4, they should utilise several sources to verify technical data, performance, quality and usability of the devices. The evaluation should be focused on the source and not the information.

The following points should be considered when marking:

- the sources selected are appropriate and provide valid technical information
- in bands 3 and 4, websites have a higher degree of reliability
- manufacturer forums can be included but the comments must be scrutinised
- reseller customer comments should only be considered for bands 1 and 2, for example, Amazon

Suitable brand websites may include:

- Buffalo
- Dell
- Fujitsu
- HP
- IBM/Lenovo
- Linux (Derivatives)
- Microsoft
- QNAP
- Supermicro
- Synology
- Western Digital

Review websites for corroborating brand information may include:

- CNET
- IT PRO
- PCMag
- TechRadar
- Trustpilot

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: design – communication equipment

(28 marks)

PO1: Explain, install, configure, test and manage both physical and virtual infrastructure

Band	Mark	Descriptor
4	4	The security aspect of the relevant equipment required by the brief is excellent, with a range of modern approaches and techniques that would ensure threats are minimised. The approach is in line with current best practice and shows a high degree of subject competence.
3	3	The security aspect of the relevant equipment required by the brief is good and covers a range of approaches and techniques focused on security. The points raised have been related back to the brief and combined with a technically adept justification.
2	2	The security aspect of the relevant equipment required by the brief is satisfactory and covers a few approaches and techniques focused on security. Some attempt has been made to relate the method back to the brief, but this is technically weak and lacks justification.
1	1	The security aspect of the relevant equipment required by the brief is minimal with only one element of security covered and little or no relevance to the brief.
	0	No creditworthy material.

Indicative content

This task should be marked focusing on the security of the network rather than each device. A range of security technologies should be considered but are not required to cover each area equally.

WiFi security would cover encryption and authentication of users, for example, domain username and password, separate VLAN network isolating from main network traffic.

Managed switches, for example, Cisco, Dell, HPE products that support segmentation, VLAN and advanced security management should be expected.

A good case could be made for running WiFi on a separate physical network so long as the justification was detailed enough.

The selection of security measures should be contemporary and aim to use current best practice, for example, WPA2-Enterprise, MAC address filtering, and directory service authentication. Legacy approaches, for example

WEP or WPA, would not be appropriate for mark bands 3 and 4 as they are less effective or robust in a commercial setting.

To show understanding of cloud portability and moving between different cloud providers, responses may include:

- limited portability between cloud providers, for example, because of lack of industrial standards, dependencies on proprietary for custom-built solutions
- security – other cloud providers may not support the same security technologies
- multi-regional compliance and legal issues

For security, responses may include:

- apply effective system monitoring (for example, traffic, service performance, memory, processor utilisation, database performance, establishing responsibilities, managing access control)
- develop routine testing methodology, for example, pen tests
- continually review access requirements
- maintain and manage data encryption, maintain sufficient data deletion policies
- ensure effective data back-up and recovery
- ensure effective border controls (for example, firewalls, signature management, access control lists, resource visibility, employee training, CERT-UK, OWASP)

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

PO2: Explain, install, configure, test and manage both physical and virtual infrastructure

Band	Mark	Descriptor
4	13–16	Excellent understanding of the problem with a selection of fully compatible components that will deliver an advanced solution. The plan shows meticulous annotations to enable full visualisation of the approach taken. Advanced subject knowledge has been shown with strong use of technical terminology and reasoning in the selection of the components. The justification is very strong, showing multiple benefits to the business using effective evaluative statements.
3	9–12	A good understanding of the problem with a selection of compatible components that will deliver an advanced solution. The plan shows effective annotations to enable visualisation of the approach taken. Effective subject knowledge has been shown with good use of technical terminology and reasoning in the selection of the components. The justification is sound, showing a number of benefits to the business using some effective evaluative statements.
2	5–8	An adequate understanding of the problem with a selection of mostly compatible components that will deliver a functional solution. The plan shows a suitable level of annotation to enable some degree of visualisation of the approach taken. Acceptable subject knowledge has been shown with satisfactory use of technical terminology and reasoning in the selection of the components. The justification is functional at best with few benefits shown and few evaluative statements.
1	1–4	A basic understanding of the problem with a selection of components that are relevant to the task but would not result in a viable solution. The plan shows a functional level of annotation which enables only limited visualisation of the approach taken. Little subject knowledge has been shown with rudimentary use of technical terminology and very basic reasoning in the selection of the components. There is a lack of any form of justification other than selection and equipment.
	0	No creditworthy material.

Indicative content

Any devices selected should mirror current practices, avoiding technology that would be considered end of life or untested in a commercial environment.

When marking, the approach and selection of equipment would naturally vary, but the solution should deliver the requirements of the brief.

The approach to the technical proposal may include consideration of design documentation, for example:

- parent schema, cloud design object, information object, persons type of actor object, external system type of actor object, resources object, context object, components object

Some sample devices and further information have been provided as a guide for the selection of equipment, serving as a guide for a medium level solution.

Switches:

- various approaches to the selection and positioning of the switches exists, one single large switch or separate switches for different meeting rooms and the CCTV, the approach should be considered on its viability and suitability
- there is no requirement to address how the switches will connect back to each other, but bands 1 and 2 should be considered if this has been addressed

WiFi:

- possible features to explore are encryption, power over ethernet (POE), wireless specification, for example, AC
- the WiFi equipment is at least AC speed and running on a separate network or VLAN (for example, Cisco Catalyst 9100 Access Points, Dell EMC Networking Ruckus R720)

IP Cameras:

- possible features to explore are connectivity, management, lens POE
- the IP cameras have been suitably placed with good coverage, ideally with a 360 degree lens but this is not essential (for example, students may identify Cisco video surveillance 3520 IP camera, AXIS M3024-LVE network camera)
- a suitable network-attached storage (NAS) drive has been purchased with enough storage to hold all the video footage (for example, Synology DiskStation NVR DVA3219)

NAS:

- possible features to explore are storage capacity, upgradeability, connectivity, operating system features
- the selection of older specifications, for example, an access point that only supports 802.11N would not be viewed as favourably as a WiFi AC device
- the approach should be structured (for example, POE for the security cameras, a separate VLAN for WiFi, CCTV cameras and core network traffic)
- a separate NAS drive should be placed in the server room, storage for the CCTV cameras should be on OnPrem unless sufficient justification can be made for offsite storage, otherwise no credit can be given

Cloud recommendation:

- consider and apply the most suitable service features in the developed prototype based on business case needs
- performance features (for example, auto-scaling, redundancy, global infrastructure, networking, content and delivery services)
- security features (for example, security groups, access control lists, users, roles, policies and permissions)

- monitor and logging features (for example, CloudWatch, EC2, monitoring, auto scaling and elastic load balancing, alarms, logs, metrics and events)

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

PO3: Discover, evaluate and apply reliable sources of knowledge

Band	Mark	Descriptor
4	7–8	The sources of information used and the knowledge gained show excellent research skills, utilising sources that are both very reliable and valid, with fully developed comments and consideration of any possible bias in the sources used and how it has impacted on the information gathered. The judgements provided demonstrate an excellent level of critical thinking in the generation of the solution with highly effective evaluative statements.
3	5–6	The sources of information used and the knowledge gained show good research skills, utilising one or more sources that are reliable and valid, with detailed comments including recognition of any bias in the sources of information. The judgements provided demonstrate a good level of critical thinking in the generation of the solution with mostly effective evaluative statements.
2	3–4	The sources of information used and the knowledge gained show moderate research skills, utilising sources that are acceptable in terms of reliability and validity, with a basic comment about the suitability and use. The judgements provided demonstrate a reasonable level of critical thinking in the generation of the solution with some evaluative statements that are partially effective.
1	1–2	The sources of information used and the knowledge gained show only basic research skills, utilising sources that are derived from sites which raise concerns regarding the reliability and validity of the information they contain. Any judgements provided demonstrate a minimal level of critical thinking in the generation of the solution with only limited evaluative statements.
	0	No creditworthy material.

Indicative content

Students can evaluate each source, or all sources combined aiming to justify the sources and validate the quality of the information. For a student to achieve mark band 3 or 4, they should utilise several sources to verify technical data, performance, quality and usability of the devices. The evaluation should be focused on the source and not the information.

The following points should be considered when marking:

- the sources selected are appropriate and provide valid technical information
- in bands 3 and 4, websites have a higher degree of reliability
- manufacturer forums can be included but the comments must be scrutinised
- reseller customer comments should only be considered for bands 1 and 2 (for example, Amazon)

Suitable brand websites may include:

- Cisco
- Dell
- Foscam
- NETGEAR
- Smonet
- Synology

Review websites for corroborating brand information may include:

- CNET
- IT PRO
- PCMag
- TechRadar
- Trustpilot

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 (PO) grid

Task	PO1	PO2	PO3	Total
1	12	8		20
2		20	8	28
3	4	16	8	28
Total marks	16	44	16	76
% weighting	21%	58%	21%	100%

Document information

The T Level Technical Qualification is a qualification managed and approved 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	Additional sample material		01 September 2023
v1.1	Sample added as a watermark	November 2023	17 November 2023