Level 3 Advanced Technical Extended Diploma in Digital Technologies (720) (5220-32)
Level 3 Digital Technologies 5220-042 / 5220-542 (Cyber Security)

November 2017 Version 1.1

Guide to the examination

Who is this document for?

This document has been produced for centres who offer

This document has been produced for centres who offer **City & Guilds Level 3 Advanced Technical Extended Diploma in Digital Technologies (720) (5220-32).** It gives all of the essential details of the qualification's external assessment (exam) arrangements and has been produced to support the preparation of candidates to take the exam/s.

The document comprises four sections:

1. **Details of the exam**. This section gives details of the structure, length and timing of the exam.
2. **Content assessed by the exam.** This section gives a summary of the content that will be covered in each exam and information of how marks are allocated to the content.
3. **Guidance.** This section gives guidance on the language of the exam, the types of questions included and examples of these, and links to further resources to support teaching and exam preparation.
4. **Further information.** This section lists other sources of information about this qualification and City & Guilds Technical Qualifications.

1. Details of the exam

External assessment

City & Guilds Technical qualifications have been developed to meet national policy changes designed to raise the rigour and robustness of vocational qualifications. These changes are being made to ensure our qualifications can meet the needs of employers and Higher Education. One of these changes is for the qualifications to have an increased emphasis on external assessment. This is why you will see an external exam in each of our Technical qualifications.

An external assessment is an assessment that is set and/or marked by the awarding organisation (ie externally). All City and Guilds Technical qualifications include an externally set and marked exam. This must be taken at the same time by all candidates who are registered on a particular qualification. We produce an exam timetable each year. This specifies the date and time of the exam so you can plan your delivery, revision and room bookings/PC allocation in plenty of time.

The purpose of this exam is to provide assurance that all candidates achieving the qualification have gained sufficient knowledge and understanding from their programme of study and that they can independently recall and draw their knowledge and understanding together in an integrated way. Whilst this may not be new to you, it is essential that your learners are well prepared and that they have time to revise, reflect and prepare for these exams. We have produced a Teaching, Learning, and Assessment guide that is you should refer to alongside the present document *(Teaching, Learning and Assessment Guide).* If a learner does not pass the exam at their first attempt, there is only one opportunity to resit the exam, so preparation is essential.

Exam requirements of this qualification

This qualification has **one** pathway. This pathway is assessed by the following examination:

- **Level 3 in Digital Technologies (042/542) (Cyber Security)** – Theory exam (2) (2 hours and 30 minutes).

The exam is graded and a candidate must achieve at least a Pass grade in order to be to be awarded the qualification. (In addition to the exam, a synoptic assignment must also be completed and passed. You can find full details of the synoptic assignment in the *Qualification Handbook* and the *Synoptic Assessment Guide* -please see the links at the end of this document).

When does the exam take place?

The exam is offered on two fixed dates in March and June. The exact dates will be published at the start of the academic year in the *Assessments and Exam Timetable*
http://www.cityandguilds.com/delivering-our-qualifications/exams-and-admin

At the start of the programme of study for each of the two years, in order to effectively plan teaching and exam preparation, centres should know when the exam will be taking place and allocate teaching time accordingly. Section 2 of this document gives a summary of the content that needs to be covered in order to prepare learners for the exam and full details of this are given in the Qualification Handbook.

Form of exam

The exam for this qualification can be taken either on paper or online.

Can candidates resit the exam?

Candidates who have failed an exam or wish to retake it in an attempt to improve their grade, can do so twice. The third and final retake opportunity applies to Level 3 only. The best result will count towards the final qualification. If the candidate fails the exam three times then they will fail the qualification.

How the exam is structured

Each exam has a total of **80 marks** available.

Each exam is made up of:

- Approximately 10-12 short answer questions;
- 1-2 extended response questions.

Short answer questions are used to confirm **breadth of knowledge and understanding**.

The extended response questions are to allow candidates to demonstrate **higher level and integrated understanding** through written discussion, analysis and evaluation. These questions also ensure the exam can differentiate between those learners who are 'just able' and those who are higher achieving.

More details about and examples of question types are given in Section 3 of this document.

Assessment Objectives

The exams are based on the following set of assessment objectives (AOs). These are designed to allow the candidate's responses to be assessed across the following three categories of performance:

- **Recollection** of knowledge.
- **Understanding** of concepts, theories and processes.
- **Integrated application** of knowledge and understanding.

In full, the assessment objectives covered by the exam for this qualification are:

Assessment objective ***The candidate..***	**Mark allocation (approx %)**
AO1 **Recalls knowledge** from across the breadth of the qualification	20%
AO2 **Demonstrates understanding** of concepts, theories and processes from a range of learning outcomes.	57.5%
AO4 **Applies knowledge, understanding and skills** from across the breadth of the qualification in an integrated and holistic way to achieve specified purposes.	22.5%

Booking and taking the exam

All assessments for City & Guilds Technical Exams must be booked through Walled Garden. There is a deadline for booking exams, synoptic assessments and any other centre marked assessments, please refer to the time line to check these dates.

The exam must be taken under the supervision of an invigilator who is responsible for ensuring that it is conducted under controlled conditions. Full details of the conditions under which the

exam must be taken can be found in the Joint Council for Qualifications (JCQ) document, *Instructions for Conducting Examinations (ICE)*.

Special consideration

Candidates who are unable to sit the exam owing to temporary injury, illness or other indisposition at the scheduled time may qualify for special consideration. This is a post-examination adjustment that can, in certain circumstances, be made to a candidate's final grade. The Joint Council for Qualifications' guide to the special consideration process can be found at www.jcq.org.uk .

To make a request for special consideration, please contact: policy@cityandguilds.com

Access arrangements

Access arrangements are arrangements that allow candidates with particular requirements, disabilities or temporary illness to take assessments, where appropriate, using their normal way of working. The Joint Council for Qualifications document, *Access Arrangements and Reasonable Adjustments* gives full details and can be downloaded here.

For further information and to apply for access arrangements please see:

Access arrangements - When and how applications need to be made to City & Guilds

Applying for access arrangements on the Walled Garden

2. Content assessed by the exam

Level 3 Advanced Technical Extended Diploma in Digital Technologies (720) (5220-32)

The exam assesses:

- **Unit 336: Threats and vulnerabilities**
- **Unit 337: Information availability**
- **Unit 338: Governance and risk management**
- **Unit 339: Ethical hacking**
- **Unit 340: Data encryption**
- **Unit 341: Access control**

Each exam assesses a sample of the content of these units. This means that a single exam will **not** cover 100% of the unit content. The full range of content will be assessed over a number of examination series. Details of the coverage of a particular exam paper will **not** be released in advance of the exam itself. Centres should **not** make assumptions about what will be assessed by a particular exam based on what has been covered on previous occasions. In order to be fully prepared for the exam, learners **must** be ready to answer questions on **any** of the content outlined below.

The table below provides an overview of how the qualification's Learning Outcomes are covered by each exam and the number of **marks** available per Learning Outcome (ie **not** the number of *questions* per Learning Outcome). In preparing candidates for the exam, we recommend that centres take note of the number of marks allocated to Learning Outcomes and to assign teaching and preparation time accordingly.

In preparing candidates for the exam, centres should refer to the Qualification Handbook which gives full details of each Learning Outcome.

The following is a summary of only that qualification content which is assessed by the exam and **not** a summary of the full content of the qualification.

Unit	Learning outcome	Topics	Number of marks
336 Threats and vulnerabilities	LO1 Determine Threats, Vulnerabilities and Countermeasures	1.1 Threats 1.2 Vulnerabilities 1.3 Countermeasures	6 marks
	LO2 Recognise Attack Vectors	2.1 Network Attack Vectors 2.2 Software Attack Vectors	

		2.3 Hardware Attack Vectors 2.4 Social Attack Vectors	
	LO3 Apply effective Countermeasures	3.1 Identify Vulnerabilities 3.2 Implement Countermeasures 3.3 Test Countermeasures	
337 Information availability	LO1 Determine the concepts of Business Continuity	1.1 Business Continuity 1.2 Disaster Recovery 1.3 High Availability 1.4 Planning for Business Continuity	12 marks
	LO2 Plan and Design a High Availability solution	2.1 High Availability Planning 2.2 High Availability Design	
	LO3 Plan and Design a Disaster Recovery solution	3.1 Disaster Recovery Planning 3.2 Topic 3.2 Disaster Recovery Design	
338 Governance and risk management	LO1 Know the concept and purpose of IS Governance	1.1 IS Governance concept and purpose 1.2 The rationale for IS Governance 1.3 Best practice models for IS Governance 1.4 Confidentiality, Integrity and Availability (CIA)	14 marks
	LO2 Understand security roles, responsibilities and documentation management	2.1 Roles and key responsibilities within an IS Governance framework 2.2 IS Governance Documentation 2.3 Third-Party Governance	
	LO3 Understand Risk management	3.1 Risk Management 3.2 Risk Assessment Methodology	

339 Ethical hacking	LO1 Know the role of Ethical Hackers	1.1 Ethical Hacking 1.2 Vetting Ethical Hackers	10 marks
	LO2 Understand a range of Ethical Hacking tools and techniques	2.1 Physical hacking tools and techniques 2.2 Logical hacking tools and techniques 2.3 Social hacking tools and techniques	
	LO3 Plan, execute and report on the process of Ethical Hacking	3.1 Ethical Hacking Processes and Standards 3.2 Develop an Ethical Hacking Plan 3.3 Perform Ethical Hacking	
340 Data encryption	LO1 Understand how data encryption has evolved and the role it plays in business	1.1 Encryption concepts and terminology 1.2 Bodies involved with developing encryption methods	10 marks
	LO2 Understand encryption methods	2.1 Methods of encryption 2.2 Implement data encryption	
	LO3 Understand methods for defeating encryption	3.1 Attack Vectors 3.2 Social engineering methods	
341 Access control	LO1 Know the role and concepts of access control in IT systems	1.1 The purpose of Access control 1.2 Access control categories 1.3 Types of Access Control 1.4 Access control Techniques	12 marks
	LO2 Understand common methods of controlling access to IT systems	2.1 Identify and Authentication 2.2 Good practices for Authentication 2.3 Configure authentication	
	LO3 Understand the limitations of access control	3.1 the limits of Access Control 3.2 Threats to and Vulnerabilities of Access Control	

		Total marks for sections:	62 marks
		Integration across units*:	18 marks
		Total marks for exam:	**80 Marks**

** Integration across units.* These marks relate to Assessment Objective 4). These marks are awarded to differentiate between levels of performance by candidates taking the exam. The marks are given for how well a candidate has applied their knowledge, understanding and skills from across the units that make up the qualification in an integrated way to meet the requirements of the exam questions.

3. Guidance

Vocabulary of the exam: use of 'command' verbs

The exam questions are written using 'command' verbs. These are used to communicate to the candidate the type of answer required. Candidates should be familiarised with these as part of their exam preparation.

The following guidance has been produced on the main command verbs used in City & Guilds Technicals exams.

A more detailed version of this table, which also includes the command verbs used in the assignments is published in *City & Guilds Technical Qualifications Teaching, Learning and Assessment* guide.

Command verb	Explanation and guidance
Analyse	Study or examine a complex issue, subject, event, etc in detail to explain and interpret, elements, causes, characteristics etc
Calculate	Work out the answer to a problem using mathematical operations
Compare (…and contrast) (or ***describe*** the similarities/differences)	Consider and describe the similarities (and differences) between two or more features, systems, ideas, etc
Define	Give the meaning of, technical vocabulary, terms, etc.
Describe	Give a detailed written account of a system, feature, etc **(..the effect of…on…)** the impact, change that has resulted from a cause, event, etc **(..the process..)** give the steps, stages, etc
Differentiate between	Establish and relate the characteristic differences between two or more things, concepts, etc
Discuss	Talk/write about a topic in detail, considering the different issues, ideas, opinions related to it
Distinguish between	Recognise and describe the characteristic differences between two things, or make one thing seem different from another
Evaluate	Analyse and describe the success, quality, benefits, value, etc (of an end product, outcome, etc)
Explain	Make (a situation, idea, process, etc) clear or easier to understand by giving details, **(..how..)** Give the stages or steps, etc in a process, including relationships, connections, etc between these and causes and effects.
Give example(s) illustrate/	Use examples or images to support, clarify or demonstrate, an explanation, argument, theory, etc

Give a rationale	Provide a reason/reasons/basis for actions, decisions, beliefs, etc
Identify	Recognise a feature, usually from a document, image, etc and state what it is
Justify	Give reasons for, make a case for, account for, etc decisions, actions, conclusions, etc, in order to demonstrate why they suitable for or correct or meet the particular circumstances, context
Label	Add names or descriptions, indicating their positions, on an image, drawing, diagram, etc
List	Give as many answers, examples, etc as the question indicates (candidates are not required to write in full sentences)
Name	Give the (technical) name of something
Propose	Present a plan, strategy, etc (for consideration, discussion, acceptance, action, etc).
Select	choose the best, most suitable, etc, by making careful decisions
State	Give the answer, clearly and definitely
Summarise	Give a brief statement of the main points (of something)

Question types

The following explains, and gives examples of, types of questions used in City & Guilds Technical exams. In preparing candidates to take the exam, it is recommended that you familiarise them with the requirements of each question type so that they can be effective and make best use of the time available when sitting the exam.

- An effective candidate will gauge the type and length of response required from the question and the number of marks available (which is given for each question on the exam paper).
- Short answer questions may not require candidates to write in complete sentences. Extended response questions will require a more developed response.
- Candidates should read the exam paper before attempting to answer the questions and should allocate time proportionate to the number of marks available for each question or section.

Question type:

Short answer questions (restricted response)
These are questions which require candidates to give a brief and concise written response. The number of marks available will correspond to the number of pieces of information/examples and the length of response required by the question.

Example question:

Mark scheme:

Identify **two** High Availability (HA) solutions. (2 marks)

Answer:
Accept any of the following or any other reasonable answer

- Standby server(s) (1)
- Concurrent processing (1)
- RAID storage (1)
- Duplicate networks (1)
- Application failover (1)
- Centralised server administration (1)
- HA clustering software (1)

One mark for each HA solution identified, maximum of two marks.

Test spec reference: 337 1.3	**Total marks: 2**

Question type:

Structured Response Questions

These are questions that have more than one part (eg a), b), etc.). The overall question is made up of linked, short answer questions which move the candidate through the topic in a structured way. For example, the question will usually start with a 'recall'/'state'/ 'describe' question followed by an 'explain' to draw out understanding of the topic. They usually have a shared introductory 'stem', and the number of marks may increase through the question.

Example question:

Mark scheme:

a) State **two** logical tools that an Ethical Hacker may use to test an organisation's security. (2 marks)

b) Explain how **each** tool in Question a) can be used by hackers to identify weaknesses in the logical security of information systems.

(4 marks)

Answer:

a) Accept any of the following or any other reasonable answer

- Port scanners (1)
- Packet sniffer (1)
- Password crackers (1)
- Vulnerability scanners (1)
- Wireless detection applications (NetStumbler) (1)
- Web testing applications (BurpSuite) (1)

One mark for each tool stated, maximum of two marks.

Answer:

b) Accept any of the following or any other reasonable answer

Port scanning is a process that sends client requests to a range of port addresses on a host (1), with the goal of finding an active port with a listening service (1).

Packet Sniffer is used to capture traffic flowing to and from a host in real time (1). Allowing it to be analysed and unencrypted packets identified (1).

Two marks for each explanation, maximum of four marks.

Test spec reference: 339 2.2	**Total marks: 6**

Question type:

Extended response questions

Extended response questions are those that require the candidate to write a longer written response using sentences and paragraphs. These usually require candidates to discuss, explain, etc. a topic in some detail. The question is often based on a short case study, scenario or other prompt. The level of detail should be gauged from the question and the number of marks available.

Example question:

Mark scheme:

A small insurance company has recently experienced a failed attempt to hack their client database. They are currently reviewing how they ensure the security of their customer's data.

Discuss internal threats that could result in security breaches and how they could be mitigated.

(9 marks)

Answer

Indicative content

- Internal threats, criminal activities, disgruntled employees, complacency
- Impact of internal threats, disclosure of sensitive information, legal penalties
- Methods of mitigating internal threats, user authentication, two-factor authentication, rights and permission

0 – No awardable material

Band 1:
1– 3 marks

The response demonstrates a limited understanding of the processes and technologies involved and is mostly a statement of facts which are not developed. The approach to the task is inconsistent. Statements may be occasionally incorrect and the use of precise technical language is sparse.

Band 2: **4 – 6 marks** The candidate has produced a discussion that expands on the factual knowledge but lacks detail in some areas. They show an adequate understanding of the processes and technologies involved including some reasons for their selection. They have provided some valid reasons for their choices. The response is structured and presented in a logical order. **Band 3:** **7 – 9 marks** The candidate has produced a thorough discussion in a logical and professional manner. They show a thorough understanding of the processes and technologies involved and have covered these in the correct logical order, including reasons behind the processes and technologies, the factors that need to be considered and the impact these factors may have on the implementation. They have clearly understood how all of the processes and technologies link to one another in terms of order and importance. They have provided valid reasons for their choices. The response is clear, coherent and all information has been presented in a logical order.	
Test spec reference: **336: 1.1, 1.2, 1.3, 2.2, 2.4, 3.1, 3.2** **337: 2.1** **338: 1.1, 1.2, 1.3, 1.4, 2.1, 2.2, 3.1** **339: 2.1, 2.2, 2.3, 3.1** **340: 1.1, 1.2, 3.2** **341: 1.1, 1.2, 1.3, 1.4, 2.1, 2.2, 3.1, 3.2**	**Total marks: 9**

Band 1

1– 3 marks

Example band 1 response

The first step would be to use the system and security logs to view the activities and identify any trends that have been occurring. Once these have been identified the system polices can be altered to prevent them from reoccurring. They should also ensure that any antivirus software and system patches are up-to-date.

There are various types of internal threats that may be encountered these range from social engineering to disgruntled employees these can be mitigated by educating the end users so that they are aware of the issues.

Another threat is the loss of data on portable devices, portable devices should be encrypted so that no one can access the data if the device is lost. If the systems do not have anti-virus software installed then malware could be installed, which could lead to data being lost.

If an organisation does not comply with the relevant legislation then they will be prosecuted.

Band 2

4 – 6 marks

Example band 2 response

Security audit can be used to identify any potential vulnerabilities that could be exploited, this could include using System and security logs built in to the Operating Systems (OS). It could also look at common areas of human behaviour such as leaving their systems logged on while they are away from their desks, which could result in people seeing information that they should not.

Disgruntled employees may disclose sensitive information or physically destroy the data to take revenge on the organisation for a preserved wrong. This could be addressed by deactivating their account as soon as their employment has been terminated.

If the systems do not have up to date anti-virus definitions they will not be able to detect the latest threats, which could result in malware being installed on the system and data being corrupted.

The threats and risks discussed can be mitigated in various ways, for instance using permissions to allow access to files and ensuring that the systems are patched and up-to-date. User education also plays an important part in mitigating threats as it raises users' awareness and helps to reinforce good practices.
If an organisation fails to comply with the relevant legislation they may be prosecuted and face financial penalties. This could lead to a loss of reputation and business.

Band 3
7 – 9 marks

Example band 3 response

The starting point would to conduct a security audit to identify any potential vulnerabilities that could be exploited, this could include using System and security logs built in to the Operating Systems (OS). They could be used to identify suspicious activities such as users logging on after working hours or trying to access information that they do not have permission to access. It would also look at common areas of human behaviour such as writing user names and password down. By writing down their passwords the user is potentially providing an unauthorised user with the opportunity to gain the information required to logon.

Other methods used that can be used to gain access to a system include social engineering, for instance you receive a phone call from someone pretending to be an IT Technician asking you for your logon details so that they can check if your system has had the latest software patch installed.

If the systems policies are not configured to prevent software being downloading and installation without requiring an administrator account, could lead to malicious codes being downloaded and installed without anyone being aware. This issue can be addressed by ensuring the latest patches are installed and the systems policies are configured to allow only system administrators to install software.

If employees copy data to portable storage devices such as USB hard drives to store data there is a risk that the device may be lost or stolen, resulting in the disclosure of sensitive data or if there is no copy of the data on the system the most up-to-date information will not be available to the organisation. Where information is not stored in a safe manner the organisation may be prosecuted and receive a financial penalty, another result of the information being disclosed could be damage to the reputation of the organisation resulting in a loss of revenue. The disclosure of information could be prevented by using encryption to render the data unreadable if unauthorised access was attempted.

The threats and risks discussed can be mitigated in various ways, one of which is education for instance making employees aware of social engineering tactics used by hackers to gain information. Raises awareness and makes people think twice before giving out information.

Access to system resources can be controlled by using Group policies to grant access to perform specific functions, these can range from performing administrative tasks such as creating users accounts to enabling users to create files and store them in a specific area. Applying system policies can help to restrict the access to data and is oftener based on the role that an individual holds within and organisation and the level of access they require.

Written polices also have a role in mitigating the risks and threats mentioned as they act as a set of guide lines for individuals using systems within the organisation.

Examination technique

Candidates with a good understanding of the subject being assessed can often lose marks in exams because they lack experience or confidence in exams or awareness of how to maximise the time available to get the most out of the exam. Here is some suggested guidance for areas that could be covered in advance to help learners improve exam performance.

Before the exam

Although candidates cannot plan the answers they will give in advance, exams for Technical qualifications do follow a common structure and format. In advance of taking the exam, candidates should:

- be familiar with the structure of the exam (ie number and type of questions).
- be aware of the amount of time they have in total to complete the exam.
- have a plan, based on the exam start and finish time for how long to spend on each question/section of the exam.
- be aware of how many marks are available for each question, how much they should expect to write for each question and allow most time for those questions which have the most marks available.

At the start of the exam session

At the start of the exam, candidates:

- should carefully read through the exam paper before answering any questions.
- may find it helpful, where possible, to mark or highlight key information such as command words and number of marks available on the question paper.
- identify questions which require an extended written answer and those questions where all or part of the question may be answered by giving bullets, lists etc rather than full sentences.

Answering the questions

Candidates do not have to answer exam questions in any particular order. They may find it helpful to consider, for example:

- tackling first those questions which they find easiest. This should help them get into the 'flow' of the exam and help confidence by building up marks quickly and at the start of the exam.
- tackling the extended answer question at an early stage of the exam to make sure they spend sufficient time on it and do not run out of time at the end of the exam.

Candidates should avoid wasting time by repeating the question either in full or in part in their answer.

Candidates should **always** attempt every question, even questions where they may be less confident about the answer they are giving. Candidates should be discouraged however, from spending too long on any answer they are less sure about and providing answers that are longer and give more detail than should be necessary in the hope of picking up marks. This may be mean they have less time to answer questions that they are better prepared to answer.

Extended answer questions

Before writing out in full their answer to extended questions, candidates may find it helpful to identify the key requirements of the question and jot down a brief plan or outline of how they will answer it. This will help clarify their thinking and make sure that they don't get 'bogged down' or provide too much detail for one part of the question at the expense of others.

Towards the end of the exam

Candidates should always set aside time at the end of the exam to read back through and review what they have written in order to make sure this is legible, makes sense and answers the question in full.

If a candidate finds they are running out of time to finish an answer towards the end of the exam, they should attempt to complete the answer in abbreviated or note form. Provided the content is clear and relevant, examiners will consider such answers and award marks where merited.

Further guidance on preparing candidates to take the exam is given in the City & Guilds publication, Technical Qualifications, Teaching, Learning and Assessment which can be downloaded free of charge from City & Guilds website.

4. Further information

For further information to support delivery and exam preparation for this qualification, centres should see:

City & Guilds

Qualification homepage: http://www.cityandguilds.com/qualifications-and-apprenticeships/it/it-professional/5220-technicals-in-digital-technologies#tab=information *which includes:*

- *Qualification handbook*
- *Synoptic Assignment*
- *Sample assessments*

Technical Qualifications, Resources and Support:
http://www.cityandguilds.com/techbac/technical-qualifications/resources-and-support

Joint Council for Qualifications

Instructions for Conducting Examinations: www.jcq.org.uk/exams-office/ice---instructions-for-conducting-examinations