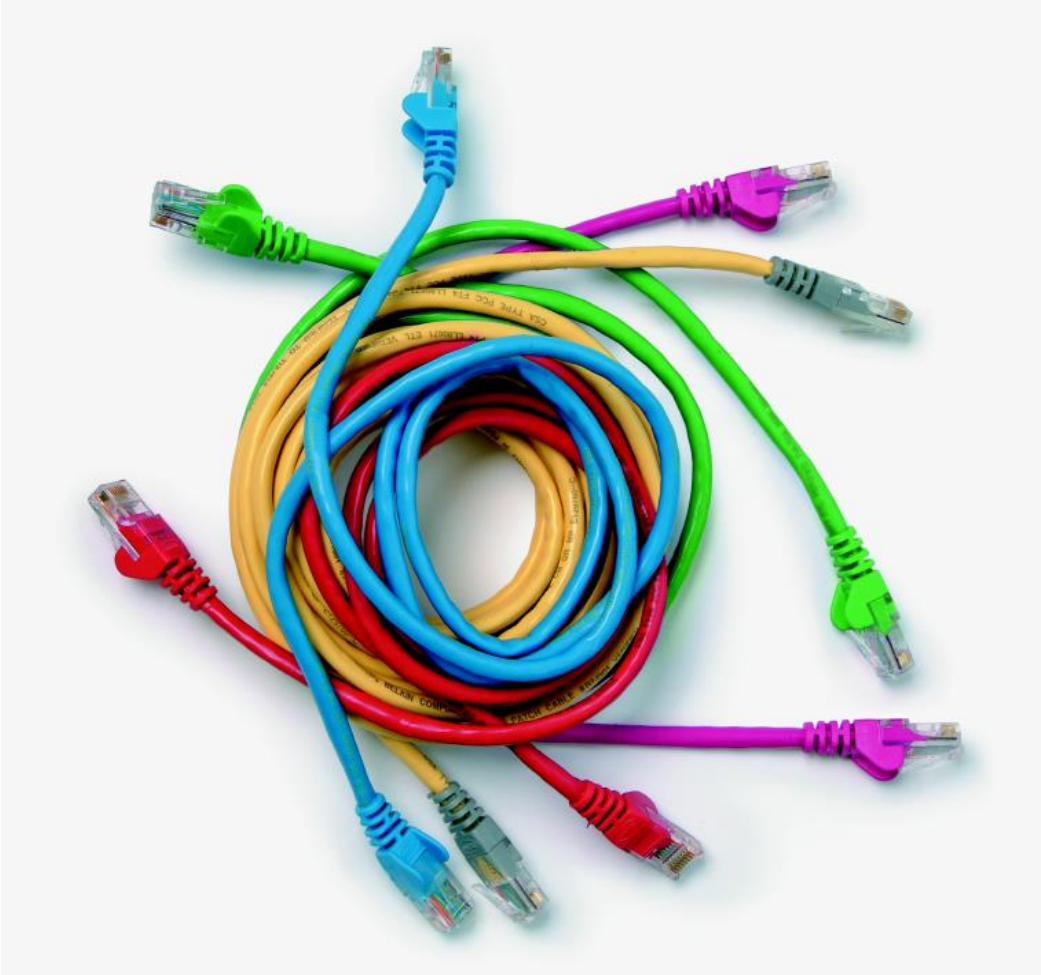
Level 3 Principles of ICT Systems and Data Security

(7540-040/7630-345)

www.cityandguilds.com
September 2017
Version 2.0

Systems and Principles
Assignment guide for Candidates
Assignment B



About City & Guilds

City & Guilds is the UK's leading provider of vocational qualifications, offering over 500 awards across a wide range of industries, and progressing from entry level to the highest levels of professional achievement. With over 8500 centres in 100 countries, City & Guilds is recognised by employers worldwide for providing qualifications that offer proof of the skills they need to get the job done.

City & Guilds Group

The City & Guilds Group includes City & Guilds, ILM (the Institute of Leadership & Management) which provides management qualifications, learning materials and membership services, NPTC which offers land-based qualifications and membership services, and HAB (the Hospitality Awarding Body). City & Guilds also manages the Engineering Council Examinations on behalf of the Engineering Council.

Equal opportunities

City & Guilds fully supports the principle of equal opportunities and we are committed to satisfying this principle in all our activities and published material. A copy of our equal opportunities policy statement is available on the City & Guilds website.

Copyright

Publications

City & Guilds publications are available on the City & Guilds website or from our Publications Sales department at the address below or by telephoning +44 (0)20 7294 2850 or faxing +44 (0)20 7294 3387.

City & Guilds
1 Giltspur Street
London EC1A 9DD
T +44 (0)844 543 0000 (Centres)
T +44 (0)844 543 0033 (Learners)
F +44 (0)20 7294 2400

www.cityandguilds.com
learnersupport@cityandguilds.com

Contents

Level 3 Principles of ICT Systems and Data Security (7540-040/7630-345)

Assignment B

Level 3 Principles of ICT Systems and Data Security (7540-040/7630-345)

Introduction – Information for Candidates

About this document

This assignment comprises all of the assessment for Level 3 Principles of ICT System and Data Security (7540-040/7630-345)

Health and safety

You are asked to consider the importance of safe working practices at all times.

You are responsible for maintaining the safety of others as well as your own. Anyone behaving in an unsafe fashion will be stopped and a suitable warning given. You will **not** be allowed to continue with an assignment if you compromise any of the Health and Safety requirements. This may seem rather strict but, apart from the potentially unpleasant consequences, you must acquire the habits required for the workplace.

Time allowance

The recommended time allowance for this assignment is **4 hours**.

Level 3 Principles of ICT Systems and Data Security (7540-040/7630-345)

Candidate Instructions

Time allowance: 4 hours

Assignment set up:

This assignment is made up of **three** tasks

- **Task A** – Common types of threat to IT Systems and Data
- **Task B** – Protection of IT Systems and Data
- **Task C** – The application of Cryptography to ICT Systems and Data.

Scenario

You are a final year IT Apprentice in an IT Support Company that has been approached by a publishing house to provide accurate and up-to-date information for a series of articles.
You have been tasked with providing information aimed at Home Users as well as Business and Industry about current threats to IT Systems and Data.

You are required, to provide accurate and up-to-date information in the following areas:

- Common types of threat to IT Systems and Data
- Protection of IT Systems and Data
- The application of Cryptography to ICT Systems and Data.

In keeping with the style of the magazines produced by the publishing house, you should use non-technical language, as far as possible in the information you provide.

You may provide the required information in a format of your choice however you should attempt to provide concise descriptions in each area.

Task A – Describe common threats to IT Systems and Data

Please use the Answer Sheet provided to complete Task A

1	Identify and describe the consequences of **ten** common physical threats to ICT systems and data including hardware damage, loss and theft eg • deliberate damage to hardware or equipment • inadequate physical security • loss or theft due to size or portability of devices • accidental damage to hardware or equipment.
2	Identify and describe the consequences of the following types of malicious code: • Virus • Malware • Spyware • Adware • Trojan • Logic bomb • Worm • Rootkits • Keylogger.
3	Identify and describe the consequences of **seven** other common types of electronic threats to ICT systems and data.
4	Explain **five** security vulnerabilities associated with remote access technologies, including wireless.

Task B – Describe methods of protecting ICT Systems and Data
Please use the Answer Sheet provided to complete Task B

1	Describe the methods of providing physical access control and security for ICT systems including: • locks (hardware locks and entry locks) • biometric controls (fingerprint, voice and retina recognition) • CCTV • fire control systems • shielding (cable screening) • Faraday Cage • Motion detector.
2	Describe methods of providing electronic protection and security controls for any **six** of the following: • firewalls • virtual networks • secure connection/transfer protocols • wireless connection security • login and password protection • access rights and permissions (including limiting data access) • virus, malware and spyware protection • secure remote access • backup and restore systems • monitoring systems (activity logging, access logs and audit logs).
3	Differentiate the following access control methods: • mandatory • discretionary • role based.
4	Describe the characteristics of strong passwords and the methods of attacking password protected systems relating to any **six** of the following: • complexity • length • duration (mandatory changing) • password history • storing (electronic/non-electronic) • dictionary attack • brute force attack • social engineering attack • keyboard attack • 'man in the middle' attack.

Task C – Identify and explain the application of Cryptography to ICT Systems and Data
Please use the Answer Sheet provided to complete Task C

1	Describe the following cryptographic algorithms: • hashing • symmetric • asymmetric.
2	Describe how cryptography can be applied to ICT systems and data security in terms of: • confidentiality • integrity • authentication • non-repudiation • access control.
3	Explain the operation of Public Key Infrastructure (PKI).
4	Explain the concepts of the Key Management and Certificate lifecycles.

When you have finished working:

- Sign each document above your name and label all removable storage media with your name.
- Hand all paperwork and removable storage media to your assessor.

If the assignment is taken over more than one period, all paperwork and removable media must be returned to the test supervisor at the end of each sitting.

End of assignment

Published by City & Guilds
1 Giltspur Street
London
EC1A 9DD
T +44 (0)844 543 0000 (Centres)
T +44 (0)844 543 0033 (Learners)
F +44 (0)20 7294 2400
www.cityandguilds.com

City & Guilds is a registered charity established to promote education and training