Qualification Specification
603/4459/3
iCQ Level 2 Certificate in Data Protection and Data Security Principles

Qualification Details

Awarding Organisation : iCan Qualifications Limited
Fees Price List Url : https://icanqualify.net
Qualification Type : RQF
Operational Start Date : 1 May 2019
Offered In England : Yes
Offered In Wales : No
Assessment Language In English : Yes
Purpose : The purpose of this qualification is to enable learners to demonstrate understanding of data security and protection.   The qualification will help learners progress to a work role where data protection and data security knowledge is required.
Total Credits : 13
Min Credits at/above Level : 13
Minimum Guided Learning Hours : 110
Total Qualification Time : 130
Overall Grading Type : Pass
Assessment Methods : Portfolio of Evidence
Structure Requirements : Learners are required to complete all 4 units, totalling 13 credits, to achieve a full certificate.
Age Ranges : Pre-16; 16-18; 19+
Qualification Objective : Learners will: understand current data legislation; understand how organisations protect data; understand how to protect their own data; understand the consquences of not protecting data and systems.

Qualification Specification
603/4459/3
iCQ Level 2 Certificate in Data Protection and Data Security Principles

Rules of Combination (ROC)

Group Name	Mandatory	#Units	Minimum Units	Maximum Units	Minimum Credits	Maximum Credits
M) Mandatory Units	**Yes**	4	4	4	13	13

Group M Mandatory Units

URN	Title	Level	GLH	Credit
A/617/5859	Understanding threats to ICT systems and data	2	30	3
M/617/5857	Understanding data protection legislation	2	35	4
M/617/5860	Understand the consequences of not protecting data	2	20	3
T/617/5858	Principles of organisational data procedures	2	25	3

Unit: A/617/5859 : Understanding threats to ICT systems and data	
Know the common types of threat to ICT systems and data	
Knowledge	
1	Discuss common types of physical threat to ICT systems and data
2	Discuss common types of electronic threat to ICT systems and data
3	List typical areas of vulnerability associated with remote access technology
4	Discuss what is meant by "denial of service attack"
5	Discuss what social engineering is
6	Discuss the following terms in relation to social engineering: - Phishing - Vishing
7	Discuss processes for the reporting of breaches of security or suspicious online activity
Know how to protect ICT systems	
1	Discuss a range of methods for providing physical access control and security for ICT systems and data
2	Discuss a range of methods for providing electronic access control and security for ICT systems and data
3	Explain types of malicious software
4	Discuss the impact malicious software can have on organisations and its data
5	Discuss ways to prevent malicious software
Understand how to protect their own personal data and devices	
1	Discuss potential threats to own personal data
2	Discuss suitable ways to protect your own personal data and information
3	Identify a range of tools and software available to help protect personal data
4	Discuss how to differentiate between trustworthy and untrustworthy sources of information online

Unit: M/617/5857 : Understanding data protection legislation	
Understand the General Data Protection Regulation	
Knowledge	
01	Define the term "Personal Data"
02	Discuss the role of the General Data Protection Regulation (GDPR)
03	In relation to the General Data Protection Regulation (GDPR) define the following terms: - controller - a processor
04	Provide an overview of each of the following 7 principles of the general data protection regulation: - lawfulness, fairness and transparency - purpose limitation - data minimisation - accuracy - storage limitation - integrity and confidentiality - accountability
05	Explain what is meant by a lawful basis for processing personal data
06	Discuss each of the following lawful bases: - consent - contract - legal obligation - vital interests - public task - legitimate interests
07	Explain each of the following individual rights: - right to be informed - right of access - right of rectification - right to erasure - right to restrict processing - right to data portability - right to object - rights related to automated decision making including profiling
08	Explain the role of a Data Protection Officer (DPO)
09	Explain what a Data Protection Impact Assessment (DPIA) is
10	Discuss what should happen in the event of a personal data breach
Understand the purpose of the Data Protection Act	
1	Discuss the purpose of the Data Protection Act
2	Describe the following elements of the Data Protection Act: - general data processing - law enforcement processing - intelligence services processing - regulation and enforcement
3	Compare the Data Protection Act to the GDPR and discuss the differences
Understand the purpose of the Freedom of Information Act	
1	Identify the purpose of the Freedom of Information Act

Unit: M/617/5860 : Understand the consequences of not protecting data	
Understand the potential consequences of not protecting data	
Knowledge	
1	Discuss the potential consequences not protecting data could have on an organisation, including the following: - Legal impact - Reputational impact - Financial impact
2	Discuss the consequences on an individual for not correctly following data protection/data security legislation/regulation
3	Explain the potential consequences of an employee sharing business or customer data
Understand the impact of data breaches on individuals	
1	Discuss the impact on individual if their data or information is shared without consent
2	Discuss the steps an individual can take if they suspect their data has been accessed without consent or stolen

Unit: T/617/5858 : Principles of organisational data procedures	
Understand organisational procedures concerning data	
Knowledge	
1	Discuss procedures an organisation might have relating to: - recording of data - processing of data - storage of data - disposal of data
Understand procedures to maintain data confidentiality and security	
Knowledge	
1	Discuss a range of ways to protect stored data
2	Explain each of the following basic techniques for encrypting information: - Symmetric Cryptography - Asymmetric Cryptography
3	Explain the advantages and disadvantages of each encryption technique
4	Identify a range of security checks an organisation might make before releasing information
5	Explain typical actions to take when an organisation: - encounters a customer whom is unable to satisfy the required security checks - when they suspect an attempt at fraud