KAPLAN PROFESSIONAL AWARDS

Qualification Specification for:

KPA Level 4 Award
In
Cybersecurity for Business (RQF)

Qualification Number: 603/6224/8
Date: 27 July 2020

Version Control

Version number	Date	Updated by	Review date
Launch version v1	27/07/2020	S Tiwary	31/08/2021

Date Submitted to Register: **27/07/2020**
Operational start date: 01/09/2020
Review date: 31/08/2021

Kaplan Professional Awards
179 - 191 Borough High Street London SE1 1HR
Phone: 0207 645 8912

Web: https://kaplanpa.co.uk/
Email: kpaenquiries@kaplan.co.uk
.

Contents

1. Introduction

About KPA

Kaplan Professional Awards (KPA) is a nationally recognised Awarding Organisation which offers high quality accredited qualifications. KPA works with national and local organisations to develop and widen access to high quality and flexible education and learning.

Our mission is to offer the best possible qualifications and resources, and to put these opportunities in the hands of as many people as possible.

KPA Qualifications

KPA Qualifications are developed to ensure they provide a clear measure of the individuals' achievement while highlighting their ability to meet the requirements of the industry in which they wish to operate. KPA work with industry specialists to ensure the qualification modules/units and their assessments are set at a suitable level for the age range and industry requirements.

2. Qualification summary

This specification will provide key information about the KPA Level 4 Award in Cybersecurity for Business (RQF) qualification.

This qualification is regulated by Ofqual and listed on Ofqual's Register of Regulated Qualifications:

Name of qualification	Qualification number
KPA Level 4 Award in Cybersecurity for Business (RQF)	603/6224/8

This qualification has been designed to support an individual's own continuous professional development role in their workplace.

This qualification is specifically designed for middle managers and small business owners, or those advising such businesses, who need to understand what cybercrime and cybersecurity can mean for business.

The aims of the qualification are to ensure that participants:

- Understand the cybersecurity threat environment.
- Appreciate that cybersecurity has its own regulatory environment.
- Can estimate the potential cost to business of a cyber-attack.
- Can examine the extent to which their businesses are secure.
- Can analyse the incident response capability of their businesses.

This qualification provides an opportunity for learners to develop and demonstrate their knowledge and understanding of potential cybersecurity risks on a business.

Upon successful completion, learners will achieve a nationally recognised KPA Level 4 Award in Cybersecurity for Business (RQF) qualification.

The qualification is graded as pass or fail, only.

Qualification Objective

The purpose of the KPA Level 4 Award in Cybersecurity for Business (RQF) is to support managers in understanding the threats posed by cybercrime to business and to identify the steps that can be taken to mitigate against these threats to the workplace.

The objective of this qualification is to give the candidate an overview of the topic, allowing a transfer of knowledge to the workplace and improving employability. This qualification incorporates professional development within the learning of each unit in order to support participants in enhancing their employability options and advancing their careers.

On the successful completion of this qualification, learners will be able to:

- Describe current trends in human behaviour that pose risks to individual and organisational privacy and security.
- Identify network administration management tasks to ensure organisational efficiency, continuity and information security.
- Analyse the security of information systems and related data, and the need for applying secure maintenance practices.
- Implement policies and procedures in accordance with national and international laws to protect information security.
- Distinguish and mitigate vulnerabilities of the various cyber risks and frauds that face businesses.
- Evaluate and describe organisational policies, rules, and norms with security implications.
- Summarise the components of a business continuity plan that ensures minimal downtime and quick recovery in the face of cyber security incidents or natural disasters.

Entry Requirements

KPA qualifications are designed for candidates who are typically 18+ and 19+.

Whilst there are no specific entry requirements to study this qualification, it is recommended that candidates have a good standard of English and Math. It is our policy to ensure qualifications are free from any barriers that restrict access and are available to all who have the capability of reaching the required standard.

Our Centres are required to review, relevant, prior qualifications and experience for each learner and to use that information to decide whether the learner has the necessary foundations to undertake this programme of study.

Exemptions and/or Recognition of Prior Learning (RPL)

No prior learning is required. There are no exemptions available towards this qualification.

Delivery Languages

This qualification is available in English only at this time.

Delivery guidance

Mode of Delivery

This qualification can be delivered through synchronous or asynchronous modes and supplemented by additional face to face or online training materials, to complement delivery of this qualification.

The Learning Approach

In delivering this qualification, the units can be divided into an array of topics (each 10-15 minutes duration). Where this qualification is delivered using asynchronous modes, topics have been grouped together, and linked to specific learning outcomes, to form modules. Modules contain in-built knowledge checks to allow the learner to measure and reflect on their progress to date.

Nature of Course Content

The content is practical rather than academic as the content is authored by specialist practitioners who also teach and is contextualised within business scenarios. A narrative approach engages the learner through the real-life story of the impact of the topics on industry.

3. Structure and Content

This KPA Level 4 Award in Cybersecurity for Business (RQF) is composed of three units. The individual must successfully complete the required assessment to obtain the qualification certification.

The Total Qualification Time for this qualification is 23 hours, and the qualification consists of three Mandatory Units, as shown below:

Qualification Structure			
Module/Unit title	Assessment method	Level	GLH
Unit 1 – Understanding cybercrime and its regulatory environment	Computer based exam	4	6
Unit 2 – Cybercrime and the Cost to Business		4	3
Unit 3 – Protecting Your Organisation against Cybercrime		4	6

Rules of Combination

This qualification is composed of three units. The candidate must successfully complete all three units to achieve this qualification.

Offering the Qualification

This qualification is only available through KPA recognised centres. If you would like to find out more about either becoming a recognised centre or working in partnership with a recognised centre please access the 'Become a KPA Recognised Centre' tab under the 'Centres' area of the website or contact KPA on 0207 645 8912.

To become an approved KPA centre you will be required to meet both general and specific requirements to ensure the standard and quality of the qualification delivery is maintained year on year.

All approved centres will be subject to KPA's ongoing quality assurance processes including centre visits which will focus on the internal quality assurance process, management of the qualification delivery and the service provided to the student.

4. Units

How the qualification works

This qualification is made up of unit(s) representing a small block of learning focusing on a particular topic or area of study relevant to the qualification.

Each unit includes the:

1. Level – which indicates the unit difficulty.
2. Credit value – the number of credits awarded to a candidate for the successful achievement of the unit's learning outcomes.
3. Total Qualification Time (TQT) - the total amount of time a typical candidate would take to complete the different activities to demonstrate achievement of the learning outcomes of a whole qualification. TQT includes guided learning hours (GLH) plus tutor directed unsupervised learning and assessment activities.
4. Learning outcome(s) – statement of our expectations of the candidate and what the candidate can expect to know, understand or do as a result of a process of learning. Each learning outcome is linked to a number of assessment criteria.
5. Assessment criteria – descriptions of the requirements a candidate is expected to meet to demonstrate that a learning outcome has been achieved.
6. Indicative content - the scope of knowledge required in order to fulfil the assessment requirements and achieve the learning outcome; it also outlines the technical components of the programme.

Understanding learning outcomes:

There are two main types of learning outcome:

- skills that can be performed.
- knowledge that can be learned.

It's possible that they can cover a combination of the two.

Competence/Skills based learning outcomes:

- linked to a practical skill that can demonstrate competence and/or performance of a specific activity or skill.

Knowledge based learning outcomes:

- reflects evidence that can be recorded in ways other than observation.

Achievement at level 4

Reflects the ability to identify and use relevant understanding, methods and skills to address problems that are well defined but complex and non-routine. It includes taking responsibility for overall courses of action as well as exercising autonomy and judgement within fairly broad parameters. It also reflects understanding of different perspectives or approaches within an area of study or work.

Unit title:	**Unit 1 – Understanding cybercrime and its regulatory environment**		
Level:	4	Code	CS01/2020
GLH:	6		
Unit aim	Candidates will understand where cybercrime threats to organisations come from and how they can manifest in the organisation's day-to-day operations. What is the cybersecurity regulatory framework within which companies are operating? Candidates will be made aware of the regulatory environment that ensures companies are not exposed to the risk of fines and penalties from national and transnational bodies.		
Learning outcome	Assessment criteria		
The learner will:	The learner can:		
1. Understand what is meant by 'cybercrime' and potential threats to an organisations' day-to-day operations.	1.1 Describe types of 'cybercrime' threats and the risk they pose to the cybersecurity of a business. 1.2 Describe ways in which to gather intelligence from digital communications and networks. 1.3 Analyse the supply chain risks which can occur via hardware, software, third parties and websites. 1.4 Explain types of hacking methods used to compromise individuals and organisations. 1.5 Outline ways in which to mitigate the effects of cybercrime threats. 1.6 Describe types of social engineering techniques used to manipulate people to circumvent established procedures and policies.		
2. Understand the cybersecurity regulatory environment.	2.1 Outline the operations of cybercrime law enforcement agencies. 2.2 Describe common practices that ensure regulatory compliance. 2.3 Evaluate the risks posed to employees from the inappropriate use of networks and systems.		

Course outline	
Main actors who participate in the field of cybersecurity.	● Types of hackers and their activities (white, grey and black hat; hacktivists; script kiddies; opportunistic; targeted campaign). ● Effects of computer hacking on a business. ● The ways nation state agencies gather intelligence from digital communications and networks and examine its potential impact on individuals, governments and organisations. ● Sources of openly available data and the ways it can be used to leverage personal identification for intelligence gathering.
Scams and risks organisations face including malware attacks and what makes them successful.	● Types of malicious software and the risks to business. ● Ransomware infecting a network or system. ● Supply chain risks which can occur via hardware, software, third parties and websites.
Hacking methods used to compromise individuals and organisations.	● How engaging with phishing can defraud business. ● Recognising fake invoices and examining the procedures to protect business from scamming. ● Practice of phishing and examining how to effectively mitigate the effects of phishing attacks. ● Romance scams and extortion emails and implementing preventive measures against these threats.
Social engineering techniques to manipulate people as individuals and within organisations.	● Risks of employees adopting creative solutions to technological restrictions in a company and steps to mitigate those risks. ● Competitor accessing a company's valuable data and the methods to mitigate the risks of such industrial espionage. ● Stages within a social engineering attack, and what you should look out for in order to stay protected.
Key cybersecurity regulations that are in place in the US and the EU (globally applicable rules and regulations - GAR).	● Cybercrime law enforcement agencies in the UK, Europe and the US and their strategies to shut down cybercrime groups operating on a global basis. ● Cyber-security controls for GDPR compliance. ● Cloud security and mobile technology policies required to ensure regulatory compliance.
Role of law enforcement in the fight against cybercrime and the development of cybersecurity standards and legislation.	● Types of protected data and security provisions which are required under the Health Insurance Portability and Accountability Act (HIPAA) legislation. ● Technical and non-technical measures required to be compliant with the Network and Information Systems (NIS) Directive.

	● Regional regulations and cyber law enforcement (RRCLE). ● NCISS ● PCI DSS
Potential risks from inappropriate use of networks and systems by employees.	● Financial penalties and risks of potential prosecution or imprisonment in cases of the misuse of employee personal data. ● Cloud security and mobile technology policies required to ensure regulatory compliance. ● Development and maintenance requirements for secure systems and card data processing. ● Financial penalties and risks of potential prosecution or imprisonment in case of the misuse of employee personal data. ● GDPR. ● Mobile and cloud storage.

Unit title	**Unit 2 – Cybercrime and the Cost to Business**		
Level	4	Code	CS02/2020
GLH	3		
Unit aim	The cost of prevention and the cost of recovering from cybercrime have a real impact on any company's bottom line. From this unit, which draws heavily on real-life examples, candidates will gain an insight into the real cost of cybercrime.		
Learning outcome	Assessment criteria		
The learner will:	The learner can:		
1. Understand the potential costs of a 'cyber-attack' to an organisation.	1.1 Estimate the potential costs of a cyber-attack on their businesses. 1.2 Evaluate the different steps to protect against cybercrime disruption to enable informed decision making. 1.3 Estimate the economic impact of incident recovery. 1.4 Analyse the limitations of cyber insurance.		
2. Know the emerging tools, and technologies developed to reduce the risk of a cyberattack.	2.1 Analyse the impact that malware can have on a poorly prepared organisation. 2.2 Evaluate technical solutions to protect a business against cybercrime disruption and enable informed decision making. 2.3 Evaluate the impact of a Ransomware incident on secure computer systems.		
3. Understand the ethical considerations of dealing with cybercriminals.	3.1 Identify the moral and legal implications of paying ransoms to cybercriminals.		

Course Outline

Potential costs to a business of a cyber-attack.	• Steps to protect against cybercrime disruption to enable informed decision making. • Economic impact of incident recovery. • Limitations of cyber insurance. • Mitigation and recovery costs. • Intrusion detection systems (IDS). • Case study: Mondelez insurance.
Emerging tools, and technologies aimed to reduce the risk of a cyberattack	• Impact that malware can have on a poorly prepared organisation. • Technical solutions to protect a business against cybercrime disruption. • Impact of a Ransomware incident on a secure computer system.
Ethical considerations of dealing with cybercriminal	• Moral and legal implications of paying ransoms to cybercriminals.

Unit title	**Unit 3 - Protecting Your Organisation against Cybercrime**		
Level	4	Code	CS03/2020
GLH	6		
Unit description	Ultimately, the role of a manager is to ensure appropriate protections are in place to prevent cybercrime disrupting and possibly destroying the company. This unit looks at implementing "Defence in Depth" or taking a multi-layered approach to protection to ensure a company's people and processes are as secure as the technology. The "Defence in Depth" approach needs to extend to the technological solutions. This unit ensures candidates are aware of the technological protections that any company may need to adopt to mitigate the risk of a cyber-attack.		
Learning outcome	Assessment criteria		
The learner will:	The learner can:		
1. Understand the policies and procedures that examine the cybersecurity challenges affecting business continuity.	1.1 Outline key aspects of an impact analysis of potential cybersecurity risks on an organisation. 1.2 Discuss how a Business Continuity Plan (BCP) can mitigate cybersecurity risks. 1.3 Outline technical and organisational measures used to address IT disaster recovery. 1.4 Identify and address weaknesses in a BCP.		
2. Know the organisation procedures that prepare employees against cyber security threats.	2.1 Explain the need for an action plan to address and effectively manage unexpected cybersecurity incidents. 2.2 Outline the importance for security awareness training against cyber threats.		
3. Be able to protect against internal and external cybersecurity attacks and intrusions.	3.1 Outline the key aspects found in an organisation's technological protections from a cyber-attack. 3.2 Describe the features of different types of encryption and anti-malware software used in the protection, and access restriction of data. 3.3 Explain how elements on a network can be protected from potentially compromised aspects of that network. 3.4 Evaluate the effectiveness of an intrusion detection system to detect the presence of hackers. 3.5 Describe the functions of running a security operations centre alongside staffing requirements.		

Course Outline	
Test and prepare for a cybersecurity attack.	• Business impact analysis to identify (disaster?) cybersecurity risks. • Elements of Business Continuity Plan (BCP) to mitigate the risks identified in a Business Impact Analysis. • Technical and organisational measures to address the recovery requirements as set out in the BCP. • Structure and steps of a BCP to identify weaknesses and address them appropriately. • IT disaster recovery planning.
Practice procedures and processes that prepare employees for various cyber security threats.	• Manage unexpected cybersecurity incidents (incident response plan). • Security awareness training for staff to enable them to apply the preventive measures and protect an organisation. • Selecting internal or external IT support for cyber security issues. • Third party independent assessments of an organisation cyber security posture and know how to manage such a process.
Technological protections required to test and prepare for a cybersecurity attack.	• Organisation's technological protections from a cyber-attack. • Protecting data and restricting data access to unauthorised individuals. • Features of anti-malware software applications • Organising of personal and business-related data files and evaluating secure data storage solutions. • Encryption, Anti-virus, Data loss prevention
Technical solutions to protect personal and business data.	• Protecting a network from external intrusion. • Protecting a network from potentially compromised aspects of that network. • Intrusion detection system to detect the presence of hackers. • Techniques for neutralising detected threats. • Firewalls; network segmentation; intrusion prevention systems.
Anti-virus software for business and commercial use.	• Role of a security operations centre. • Security operations centre running alongside staffing requirements. • Password and authentication discipline. • Security information and event management.

Core reading

Blau, A. (2019) Cybersecurity: The Insights You Need from Harvard Business Review (HBR Insights Series).

Sanchez, F. and Duan, Z. (2012). "*A Sender-Centric Approach to Detecting Phishing Emails*," International Conference on Cyber Security, Washington, DC, 2012, pp. 32-39, doi: 10.1109/CyberSecurity.2012.11.

Trautman, L.J. and Ormerod, P. (2019). *Wannacry, Ransomware, and the Emerging Threat to Corporations.*

Web sources

ISO, ISO/IEC 27001 *Information Security Management*, https://www.iso.org/isoiec-27001-information-security.html (20/07/20)

IT Governance, *Cyber security solutions ISO 27001*, https://www.itgovernance.co.uk/iso27001 (20/07/20)

NIST (National Institute of Standards and Technology), *Cybersecurity Framework* https://www.nist.gov/cyberframework (20/07/2020)

5. Quality Assurance Processes

Assessment

KPA has in place a system of QA which allows it to maintain a high level of control over the development, delivery and awarding of the qualification. In particular it will require centres to meet the particular requirements for each type of assessment. KPA External Quality Advisor's will be responsible for ensuring centres meet the approved centre requirements relating to specific types of assessment and/or examination delivery.

Centre Resources

KPA approved centres are required to provide the right human and physical resources needed to ensure the quality of the learner experience. Centres must ensure that staff have the appropriate level of subject knowledge, practical experience of the sector and are normally qualified to at least a degree standard. It is desirable that staff have a teaching and/or assessing qualification.

The physical resources required will vary depending on the style of delivery. Where distance or blended learning is used, KPA expects centres to have appropriate learning support materials, infrastructure and technology in place to meet student needs.

Certification

On completion of the qualification, KPA will confer upon the candidate the award of

KPA Level 4 Award in Cybersecurity for Business (RQF)

Fees

The exam fee for this qualification is £60.00.

6. Access arrangements and Reasonable adjustments

KPA complies with the Equality Act 2010 and Ofqual general conditions of recognition regarding fair assessment. Students are asked to notify KPA on registration so that their needs may be considered.
Candidates are able to request alternative access due to short-term or long-term indispositions. Applications must meet the relevant deadlines as laid out in the Access Arrangements for Examinations policy. Students who have been granted access arrangements must inform KPA immediately if the circumstances related to their access arrangements change prior to the sitting of the examination in question.

Access arrangements

Access arrangements allow candidates with specific needs; such as special educational needs, disabilities or temporary injuries, to access an assessment without changing the demands of the assessment. The purpose behind an access arrangement is to meet the particular needs of an individual candidate without affecting the integrity of the assessment. Access arrangements are agreed before an assessment and are the principal way in which awarding bodies comply with the duty under the Equality Act 2010* to make 'reasonable adjustments'.

Reasonable Adjustments

KPA will make reasonable adjustments for a candidate with a disability, as defined in the Equality Act 2010*; who would be at a substantial disadvantage in comparison to someone who is not disabled.

An adjustment to be considered reasonable will depend on a number of factors, which will include, but are not limited to the:

- needs of the disabled candidate;
- effectiveness of the adjustment;
- cost of the adjustment;
- likely impact of the adjustment.