BCS THE CHARTERED INSTITUTE FOR IT

BCS HIGHER EDUCATION QUALIFICATIONS
BCS Level 6 Professional Graduate Diploma in IT

COMPUTER SERVICES MANAGEMENT

EXAMINERS' REPORT

March 2018

General comments on candidates' performance

In general, the answers were well thought out and appropriate to the level of the paper. In some instances, however, there is evidence that the candidates failed to provide sufficient detail and exhibit appropriate knowledge, losing marks as a result.

There were several excellent papers, for which the candidates should be congratulated. The highest marks were given to those who provided comprehensive, relevant, reasoned, structured and detailed answers, and were able to draw upon professional practices and academic material.

Candidates are encouraged to always read the paper carefully before commencing their answers, to ensure they understand what is required. This is particularly the case when questions are multi-part, as the weighting of marks in each section gives a clear indication of the level of detail required in each section in order to score well.

The answer pointers below are for guidance only. Valid alternative answers that were relevant to the question would also attract full marks.

SECTION A

A1.

Due to the growth of your software company, you wish to recruit ten additional software developers who are skilled in the production and maintenance of mobile applications (apps). After advertising the posts, you find that only self-taught developers, with no commercial experience, have applied.

a) Describe FOUR approaches you could take to resolve this situation, stating the potential advantages and disadvantages of each approach.

(16 marks)

b) For ONE of these approaches, create a project plan to show how it will be specified, carried out and monitored.

(9 marks)

Answer pointers

a)

As this is a fairly common situation in the industry at present, candidates may have direct knowledge of those who have experienced it. If this is not the case, candidates should be able easily to comment on the scenario, using their basic knowledge of the industry and the likely options available.

The FOUR options for this scenario will attract up to FOUR marks each and should be sufficiently distinct to warrant the marks awarded, so there should be little or no overlap between them. They could include, but are not limited to, the following:

- Recruit non-commercial coders and train them to professional standards
- Recruit non-coders with suitable parallel qualifications and train them from the ground up
- Re-advertise with better pay and benefits, in order to attract coders who would be immediately effective
- Advertise for conventional programmers (e.g. COBOL, Fortran, C) who wish to retrain for the current development environment
- Train existing non-coding staff who express an interest in professional development

b)

The project plan will attract up to NINE marks. It can be delivered in any appropriate business format, provided it meets the criteria specified in the question.

The plan should convince the examiner that the chosen option is appropriate and workable.

The use of a standard project management methodology will attract suitable marks, depending on the skill with which it is applied.

Examiners' comments

This question was attempted by nearly 70% of candidates and was generally answered very well, with almost 80% of candidates reaching a pass mark.

There is evidence that some of the answers provided showed a welcome level of creativity and engagement; those candidates are to be congratulated.

Candidates who scored poorly often gave the wrong number of approaches in Part a); this limited the number of marks that could be awarded. In other cases, the approaches presented in Part a) were too similar to be marked as separate ideas – again losing marks.

The evidence shows that the project plan proved a weak spot for some candidates. However, those who had thought through the requirement and expressed it clearly scored well.

A2.

Cloud computing is having an impact on the way business organisations manage their data in a global market.

a) Discuss FOUR ways in which Cloud computing demands a new way of evaluating Information Security Management (ISM) for an organisation.
(12 marks)

b) Write a policy document that describes THREE clauses which an organisation should ensure are included in a contract with a Cloud provider.
(13 marks)

Answer pointers

a)

The core factors of Confidentiality, Integrity and Availability are common to both traditional and Cloud information security models.

The FOUR ways which prospective managers should be aware of include, but are not limited to, the following:

- Physical loss of control of the data
- No direct authority over the selection, training or scrutiny of staff employed by the Cloud provider
- No direct control over security policies or procedures at the data centre
- Feedback on security issues is usually limited to contractual reports from vendor, rather than an line-management relationship that would happen in-house
- Data is held in an environment where there is no “loyalty” to the data owner

Each will attract up to THREE marks.

b)

The policy document should be in a standard business format and clearly outline the clauses required to address the THREE issues. The issues should be significantly different, and not have common elements.

Each issue will attract up to THREE marks, with FOUR marks being available for overall style and structure.

It should be noted that this question is NOT a request for a description of the various classes and models of Cloud services. The answers requested are very specific.

Examiners’ comments

This question was attempted by just over 56% of candidates, and the pass mark was almost 66%.

In general, the approach taken to this question was appropriate and well thought out. The evidence shows that candidates who scored poorly either did not provide the number of elements requested in Part a) or spent too long sharing their general knowledge of cloud-based systems. The material requested was precisely defined, and future candidates should take care to observe this.

A3.

The General Data Protection Regulation (GDPR) comes into force in the UK on 25th May 2018.

a) Discuss an overview of the potential impact of the GDPR on a commercial organisation based in the UK which controls and processes personal data.

(10 marks)

b) Explain the distinction between "personal data" and "sensitive personal data". You should describe the different approaches required for the control and processing of each category of data.

(15 marks)

Answer pointers

The advice of the Information Commissioner's Office will be used as the authoritative source for this information.

a)

Current impacts are:

- Need for awareness
- Accountability
- Information audit
- DP impact assessments
- DP Officers
- Establishing lawful basis for processing
- Consent
- Communication with children
- Communicating privacy information
- Rights of individuals
- Subject access rights
- Managing data breaches
- International data transfers

Up to TWO marks will be available for style and format. Up to FOUR marks will be awarded for each of "control" and "processing" of personal data, TEN marks in total.

b)

The categories of "personal data" and "sensitive personal data" were understood by many in relation to the Data Protection Act (1998), but Article 9 of the GDPR modifies the way the categories are defined and intended to operate.

The GPDR now specifically includes genetic data, and biometric data where processed to uniquely identify an individual.

Up to FIFTEEN marks will be awarded for the discussion of "personal" and "sensitive personal" data.

Examiners' comments

The topic of GDPR was chosen as it is likely to continue to impact on the IS/IT community globally for some time to come, having already had much public exposure as a "hot topic" prior to its introduction.

Approximately 25% of candidates attempted this question and the pass rate was only just over 33%. The evidence shows that a number of candidates scored poorly because the material they presented was too limited, too generic or incorrect.

SECTION B

B4

You are the newly appointed Computer Services Manager for a large company that specialises in the design of hospitals and associated medical facilities. The company makes use of leading edge technology and many staff members work from home using mobile devices. Your initial analysis of the company reveals that there are some security issues that need to be addressed.

a) Describe how the use of strong passwords and multi-factor authentication can be used to improve the security of controlled access to the system.
(9 marks)

b) Explain how firewalls can be used to protect computer systems
(4 marks)

c) Describe the operation and benefits of using a Virtual Private Network (VPN) by the staff members who work from home using public networks.
(7 marks)

d) Define the term "ransomware" and list some methods that can be used to counteract it.
(5 marks)

Answer pointers

a) **Strong Passwords** are hard to detect by humans, as they are difficult to guess; this improves the security of controlled access to the system. Passwords are typically case sensitive and a strong password would consist of at least 8 characters which are a combination of upper and lower-case letters, numbers and symbols (such as: +, &, %, $).

Two-factor authentication is a security method by which users obtain access by providing two separate factors to identify themselves; it can be combined with the use of a strong password to increase the security of controlled access to the system.

It is necessary for two different types of factor to be used in two-factor authentication. Three different types of factors that can be used for authentication are:

- Knowledge factor: knowing a password or a personal identification number (PIN)
- Possession factor: owning a membership card or mobile phone
- Biometric factor: a human characteristic such as fingerprint, DNA or voice print

Benefits of using two-factor authentication are:

- Greater security than single factor authentication, which simply uses password protection
- Deterrent, as hackers are more likely to avoid a two-factor authenticated account

(One mark for each key point identified and described - maximum 9 marks)

b) A **firewall** is used to prevent unauthorised requests from hackers attempting to gain access to the network or computer systems via the Internet.

ICT systems are constantly communicating with the outside world, which involves connection to public networks and the associated difficulty of effectively policing access to the system.

A firewall is a combination of hardware and software that is designed to check the integrity of incoming messages and requests for service from the system. Where a message or request is dubious, it can be re-routed temporarily until the legitimacy of the message has been established.

(One mark for each key point identified / described, maximum 4 marks)

c) **VPNs (Virtual Private Networks)** are used to create a secure and encrypted connection for the transmission of data across public networks, such as the Internet.
The main characteristics of VPN are:

- VPN technology is a method established to ensure secure access between users linked by public networks, such as the Internet
- Users can safely send and receive data using VPN, as all data is encrypted
- Data travels through secure tunnels in public networks, making it an extension of the private network
- VPN users can access the technology by signing on to their private network; typical authentication approaches are the use of passwords and unique identification methods

Benefits of using VPN are:

- Data Security is increased, as VPN offers encryption security in public wi-fi locations
- User Privacy is increased, as user internet activity cannot be monitored by their ISP
- Site to Site communications: workers can remotely connect to the secure business private network from home or when they are “on the road”

(Seven marks, *some examiner discretion)*

d) **Ransomware** is a type of malware that prevents the user from using their computer or accessing certain files unless a ransom is paid; it sometimes encrypts files so that they cannot be opened. It is often distributed as a trojan or malware disguised as a legitimate file.

The following methods can be used to counteract the ransomware threat:

- Back up your files and store on a completely separate system, so that they can be restored if malware installed
- Be careful not to open unsolicited emails or visit unfamiliar websites
- Do not download programs or applications from an unknown source
- Use an anti-virus program to help prevent ransomware from being downloaded
- Always install updates to software, to prevent any vulnerabilities from being exploited

(Five marks, *some examiner discretion)*

Total marks for Q1 is 25 marks (9 + 4 + 7 + 5)

Examiners' comments

This extremely popular question was attempted by 96% of the candidates, 83% of whom met the required standard.

The evidence shows that part a) was well answered, with most candidates describing the need for, and features of, a strong password. Multi-factor authentication was explained in detail by some candidates and the majority used a range of examples to describe its operation. In part b) most candidates had a good working knowledge of firewalls and gave a range of examples to support their explanation. Part c) was less well answered by the majority of candidates, who demonstrated little understanding of VPN techniques. In some cases, benefits were shown as a list of features relating to teleworking, rather than the benefits to system security. In part d) candidates demonstrated a good awareness of ransomware and gained full marks for their answers.

B5.

In the context of computer services, write notes on the following:

a) Escalation procedures
b) BCS Code of Practice
c) The Software Capability Maturity Model
d) Accounting rate of return
e) Risk management

(5 x 5 marks)

Answer pointers

a) Escalation procedure

The purpose of an escalation procedure is to have formal levels of matching staff from each organisation. If staff from the lowest level are unable to agree resolution of an issue, it is escalated to the next level, and so on. The highest level would be the CEOs of each organisation. For example:

LEVEL	OUTSOURCING COMPANY	ORGANISATION
1	Help desk operator	Operational user
2	Help desk supervisor	User supervisor
3	Support manager	Departmental manager
4	Divisional Director	IT Director
5	CEO	CEO

The purpose of the escalation procedure is to prevent staff at all levels becoming involved in issues that should be resolved by others.

(Five marks – some examiner discretion.)

b) BCS Code of Practice

The BCS Code of Practice describes standards of practice to help BCS members. It provides guidance under the following headings:

- Practices Common to all Disciplines
- Maintain Your Technical Competence
- Adhere to Regulations
- Act Professionally as a Specialist
- Use Appropriate Methods and Tools
- Manage Your Workload Efficiently
- Participate Maturely
- Respect the Interests of your Customers
- Promote Good Practices within the Organisation
- Represent the Profession to the Public
- Key IT Practices
- Practices Specific to Education and Research Functions
- Practices Specific to Business Functions

(One mark for each point raised/explained, maximum five marks.)

NOTE. If candidates become confused with the Code of Conduct, only three marks can be given. The Code of Conduct follows:

General

The Code sets out the professional standards required by the Society as a condition of membership and governs personal conduct as an individual member of the BCS.

Public interest

Work is to be performed with due care and diligence and in the interests of system users. If your professional judgement is overruled, you shall indicate the likely risks and consequences. You shall conduct your professional activities without discrimination against clients or colleagues. You shall reject any offer of bribery or inducement.

Duty to relevant authority

You shall avoid any situation that may give rise to a conflict of interest between you and your relevant authority. You shall make full and immediate disclosure to them if any conflict is likely to occur or be seen by a third party as likely to occur.

Duty to the profession

You shall uphold the reputation and good standing of the BCS in particular, and the profession in general, and shall seek to improve professional standards through participation in their development, use and enforcement.

Professional competence and integrity

You shall seek to upgrade your professional knowledge and skill, and shall maintain awareness of technological developments, procedures and standards which are relevant to your field, and encourage your subordinates to do likewise. You shall not claim any level of competence that you do not possess. You shall only offer to do work or provide a service that is within your professional competence.

(One mark for each point raised/explained, maximum five marks.)

c) The Software Capability Maturity Model is a bench-mark for measuring the maturity of an organisation's software process. It is a methodology used to develop and refine an organisation's software development process by judging the maturity of the software processes used and for identifying the practices that are required to increase the maturity of these processes. There are five CMM levels:

- **Initial.** The software process is characterised as ad hoc, and occasionally even chaotic. Few processes are defined. Success depends on individual effort and heroics.

- **Repeatable.** Basic project management processes are established to track cost, schedule and functionality. The necessary process discipline is in place to repeat earlier successes on projects with similar applications.

- **Defined.** The software process for both management and engineering activities is documented, standardised and integrated into a standard software process for the organisation. All projects use an approved, tailored version of the organisation's standard software process for developing and maintaining software.

- **Managed.** Detailed measures of the software process and product quality are collected. Both the software process and products are quantitatively understood and controlled.

- **Optimising**. Continuous process improvement is enabled by quantitative feedback from the process and from piloting innovative ideas and technologies.

(One mark for each valid point, maximum 5 marks.)

d) Accounting Rate of Return (ARR)

The ARR process is as follows:

- Calculate the total investment for the project
- Calculate the net cash inflows (or savings in expenditure) which will be realised in each period of the project's life
- Calculate the accounting profit over the life of the project
- Divide the total profit by the number of periods and express this as a percentage of the average investment
- The average investment may be calculated on an annual basis or approximated as (initial investment + final investment) ÷ 2

Candidates may also mention advantages and disadvantages.

Advantages
- Simple and uncomplicated
- Comprehensible – gives percentage return
- Relates to financial accounts

Disadvantages
- Ignores the time value of money
- Cannot relate target return to economic objectives
- Suffers from problems of accounting measurement
- Ignores cash flow and the time value of money
- Prefers relative return to absolute return

e) Risk Management

Expected answer points:

- Risk management will consist of the formal consideration of all threats to a computer facility.

- Risks should be ranked in order, based on the combined frequency/severity.

- High frequency/low severity breakdowns may be considered ahead of low frequency/medium severity breakdowns.

- The cost of reducing or transferring the risk should be estimated and compared with the benefits that will arise.

- A formal approach can be used to justify the provision of the resources required.

- A formal approach could also be used as a justification for management to accept the risk.

(One mark for each valid point, maximum 5 marks)

Examiners' comments

This question was attempted by 58% of the candidates, the majority of whom reached the required standard.

The evidence shows that few candidates had full knowledge of all five topics, but most generally had good knowledge of two, perhaps three, of the topics. Escalation procedures, BCS Code of Practice and the Software Capability Maturity Model were generally understood but very few candidates had a detailed knowledge of the Accountancy Rate of Return. The answers for Risk Management were generally limited to a list of risks that can occur in computing, with little or no discussion on how these risks could be quantified and managed.