BCS THE CHARTERED INSTITUTE FOR IT

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

COMPUTER SERVICES MANAGEMENT

March 2016
Answer **any** THREE questions out of FIVE. All questions carry equal marks.
Time: THREE hours

Answer any Section A questions you attempt in Answer Book A
Answer any Section B questions you attempt in Answer Book B

The marks given in brackets are **indicative** of the weight given to each part of the question.

Calculators are **NOT** allowed in this examination.

General comments on candidates' performance:

The standard of answers was high for this examination, with 75% of those sitting achieving a pass. However, for some candidates there remained areas where improvements could be made. Future candidates should note the following:

- ***Understand the requirements of the question.*** *Candidates are advised to spend time reading and understanding exactly what is required, both in terms of the number of questions to answer and the precise requirement of each question. Failure to do so wastes time and increases the risk of failure.*

- ***Answer all parts of the questions attempted.*** *Some candidates omitted parts of the question. Even if unable to provide a full answer, a partial answer might result in the extra marks that could make a difference between failure and pass.*

- ***Answer the questions set.*** *Some candidates attempted to gain marks by providing answers that were related only vaguely, if at all, to the questions set. Future candidates are advised that no marks are given for such answers.*

Please note that the answer pointers contained in this report are examples only. Full marks were given for valid alternative answers.

Section A

A1.

You have been appointed the Computer Services Manager of a large international Charity that provides disaster relief following natural disasters. After a few days you become worried that the database of subscribers, medical staff and emergency volunteers maintained by the charity is insecure.

After considering all the possible risks to the Charity's information, describe the contents of an appropriate Information Security Policy and the actions necessary to protect this information.

(25 marks)

Indicative answer points:

The description of the charity in the question gave a number of clues to the nature of the organisation, the environment in which it operates and the particular risk profile for information security which results.

The answer to this question could have taken a number of forms but could be formatted into two categories:

- The Information Security Policy (12 marks)
- The actions necessary to protection the information (13 marks)

This provides a structure around which a candidate could develop a response.

Current UK Data Protection legislation provides a good basis for the discussion, augmented by appropriate threads of industry-standard information management policy and procedure.

Particular reference to the rapid-response nature of the charity, its international remit and resulting risk profile was essential in order to gain good marks.

Examiners' comments:

This was a popular question, attempted by around three-quarters of candidates, and was, in general, answered well. Around 80% of those who attempted it reached or exceeded a pass mark.

Most candidates grasped the basic requirements of database security management and how it can be controlled, as well as the specific requirements of an international charity working in this arena.

Those candidates who scored badly generally failed to provide an adequately defined security policy. In some cases, candidates failed to provide descriptions of the actions needed to put the policy into practice and protect the information.

A2.

During a financial audit it was revealed to the Chief Executive of an organisation that it has continued to pay an expensive maintenance contract to support server systems and disk arrays that were actually de-commissioned several years ago.

The Chief Executive has asked you, the replacement IT Services Manager who has just been appointed what steps you intend to take to prevent such expensive and embarrassing situations arising again.

a) Write a report to the Chief Executive outlining the approach you intend to take in bringing matters under control. You should include details of THREE significant relationships with other organisational groups within the company which will be essential to the success of your proposals.

(12 marks)

b) For ONE of these relationships, write an operational document which can serve as a template for your staff in managing the relationship you have described.

(13 marks)

Indicative answer points:

Part a):

3 marks for memo format and style
3 marks for each of THREE significant relationships with other groups

It was important that the candidate provided this answer in the form of a standard business memorandum.

Note that the relationships sought were described as “significant” - so they needed to be closely related to the logic of the question.

Significant relationships expected were likely to include, but were not limited to:

- Internal auditors
- Procurement manager
- WEEE compliance manager
- Financial controller
- IT operations manager

Part b):

3 marks for document style and structure – reflecting the nature of what was requested
5 marks for the extent to which the content dealt with the requirement
5 marks for the completeness of the solution in terms of control

Candidates should note the following:

- The former IT Services Manager had apparently been dismissed for this gross misconduct, so the senior management would be looking closely at your approach.
- The visibility of the issue is such that a complete and auditable solution was required.
- Effective configuration management was likely to be a good start to a longer term approach.
- An integrated workflow managing cradle-to-grave for equipment and service contracts was likely to be the ultimate goal.

Examiners' comments:

This question was attempted by only about a quarter of candidates. While a few very good answers were received, the standard was not high overall, with a pass rate of around 50%.

Many candidates lost marks by not using the document formats required, or not providing the correct number of examples.

Candidates should ensure that they read the question carefully and provide the answer which is requested – and to not provide generic information which might apply to any situation.

A3.

The Computing Services group, for which you work as the Helpdesk Manager, provides support for some five hundred office workers on a single site in a major city.

You are concerned about the high level of turnover of front-line helpdesk support staff in your section, which you believe may be contributing to a poor incident clear-up rate and growing dissatisfaction among the customers.

a) Write a memorandum to the Head of Computing Services describing the problem. You should discuss THREE techniques you propose to use to address the problem of high staff turnover.

(12 marks)

b) With reference to ONE of your proposals, write a formal project plan which will allow you to design, implement and monitor the technique you intend to use. You should state any assumptions which you make regarding the organisation and its infrastructure.

(13 marks)

Indicative answer points:

Part a):

Candidates should have used a memo format as requested. Failure to do so resulted in a loss of marks, as the aim was to reflect a standard business environment. This included the use of correct forms of address

In answering the question, candidates should have sought to build a realistic picture of the problem and determine reasons for high turnover.

These factors may have included, but were not limited to, pay and conditions, work environment, poor training, lack of opportunity for learning or advancement, attitude of customers, quality and usability of information systems available, lack of variety in the work.

The memo needed to show that the staff have been consulted and involved and that the issues have been understood.

Many techniques were available for addressing the problem, but they could have included asking the staff members themselves what was going wrong, reviewing all the concerns, showing them how management were seeking to address the issues, showing practical steps towards permanently solving the problems.

Up to 3 marks for style and format.
Up to 3 marks for each of THREE techniques.

Part b):

The use of a standard formal format for project planning was preferred in the answer to this section – the choice of this would naturally vary according to the experience of the candidate.

Candidates needed to note the use of the terms “design, implement, monitor” in the question. This gave a hint as to what is expected as the basis for structuring the response from the candidate.

The list of assumptions provided by the candidate was required in order to describe to the examiner the picture the candidate had of the environment.

Up to 4 marks for project plan format.
Up to 3 marks for each of design, implementation and monitoring aspects.

Examiners' comments:

This question was attempted by around 60% of candidates. The question was answered well in the majority of cases, with close to 80% of those attempting it reaching or exceeding a pass mark.

Part a) provided the majority of marks for many candidates and the quality of the material offered was generally high, with good, cogent examples being given by many.

Part b) was less well attempted in the majority of cases, with many candidates losing marks by not providing the answer in the form requested or giving an answer which was too vague or generic. A "formal project plan" was requested and, while credit was given for the use of any appropriate methodology or format, many answers were anecdotal and not fit for purpose.

Section B

B4.

You are the newly appointed Information Security Manager for a group of sports and leisure centres. Using wireless technology, members are permitted to use their own devices at the leisure centre to access the internet at the club. A recent risk analysis revealed that there were some security issues based on members' use of the system.

a) Describe the content of an Internet Acceptable Use Policy for the use of leisure centre members.

(10 marks)

b) Explain the term "two-factor authentication" and why it might be used to improve the security of controlled access to the system.

(5 marks)

c) Describe the techniques which might be used to gain unauthorised access to systems and the measures that can be taken to prevent these risks.

(10 marks)

Indicative answer points:

a) Internet Acceptable Use Policy

An internet acceptable use policy (AUP) will define the extent to which a member might use the leisure centre internet facilities for personal purposes, to define appropriate browsing behaviour and to specify the directives necessary to protect the IT network infrastructure.

Typical structure of the leisure centre AUP could be:

Acceptable internet usage

- Fully comply with legislation including the Data Protection Act, Computer Misuse Act and the Copyright, Design and Patents Act.
- The internet must be used in an acceptable way.

Unacceptable behaviour

General and System Activities

- The introduction of malicious programs onto the network or server
- Attempting to access unauthorised data on the server or other members' accounts
- Executing network monitoring with the intention of intercepting data
- Downloading pirated software

Leisure Centre Interactive Services

All messages posted in chat rooms, on bulletin boards, and in blogs or other social media MUST BE:

- Genuinely held member opinions
- Correct and simply keeping to facts

All messages posted MUST NOT:

- Promote activities that are illegal
- Promote material that is violent, sexually explicit or discriminatory
- Contain material that is obscene, inflammatory or offensive
- Be used to misrepresent or impersonate a person
- Be used to threaten, annoy or invade another person's privacy.

Email and Communication Activities

- Members must not use the leisure centre Wi-Fi facility to send unsolicited email messages or "junk" mail.

Web Monitoring Software

The leisure centre will control and monitor the usage of its Wi-Fi facility using web monitoring software to ensure that members of the gym adhere to the internet acceptable use policy (AUP).

This software will also be used to filter and block websites that are considered to be unsuitable and unacceptable for members.

(One mark per relevant content point / not necessary for answers to be in context - maximum 10 marks.)

b) Two-factor authentication

Single-factor authentication (SFA) is where the user can obtain access to an account or service using one factor. The risk with using SFA is that, if the same password is used for multiple applications, they are all vulnerable if the password gets hacked. Using a unique password for each application will minimise this risk.

Two-factor authentication is a security method by which users obtain access by providing two separate factors to identify themselves. 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 just 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 5 marks.)

c) Techniques used to gain unauthorised access to systems and prevention measures

Access techniques include, but are not limited to the following:

- Cracking Passwords
- Phishing
- Pharming – route traffic to a fake website
- Network sniffing – monitoring network traffic for passwords
- Playing middleman – to intercept two communicating groups
- Viruses or worms – software loaded with the aim of causing damage
- Trojan horse – malicious program that appears innocent or helpful
- Spoofing – access gained by impersonating a legitimate IP address

Preventative measures include, but are not limited to, the following:

- Firewall - used to prevent unauthorised requests from hackers to gain access to the network or computer systems via the Internet.
- Intrusion detection systems (IDS) - designed to monitor the computer system for malicious activities and report the incident to the network management.
- Anti-malware /anti-virus software - searches the computer system for viruses / spyware programs and deletes them once detected.
- Encryption - used to make stored data more secure, by making it unreadable to people who do not have the key to decode it.

(One mark for each technique / measure described - maximum 10 marks.)

TOTAL: 10+5+10=25

Examiners' comments:

This was an extremely popular question that was answered by nearly all of the candidates, many of whom passed.

Part a) was well answered, with many candidates listing the types of unacceptable behaviour and the need to limit the bandwidth of the leisure centre members. Few candidates mentioned the need for the policy to contain references to the web monitoring of members to detect misuse and / or inappropriate behaviour.

In Part b) most candidates had a good working knowledge of two-factor authentication and gave a range of examples to support their answers. A minority of candidates did not understand the term and confused the use of a username and password as two factors whereas the factors should be any two from a knowledge factor, a biometric factor and a possession factor.

Part c) was generally well answered with a range of techniques that could be used to gain unauthorised access to the system and the associated preventative measures that could be used.

B5.

As Computer Services Manager for a large financial organisation, you have been asked to investigate the adoption of a cloud computing approach.

Discuss the responsibilities of the organisation with respect to the 1998 Data Protection Act and the steps you would take to ensure compliance with this Act.

(25 marks)

Indicative answer points:

Outline of the Data Protection Act

DPA Principles:

1. Personal data should be obtained and processed fairly and lawfully
2. Personal data can be held only for specified and lawful purposes
3. Personal data should be adequate, relevant and not excessive for the required purpose
4. Personal data should be accurate and kept up-to-date
5. Personal data should not be kept longer than necessary
6. Personal data must be processed in accordance with rights of the data subject
7. Appropriate measures must be taken against unauthorised access
8. Personal data cannot be transferred to countries outside the E.U. unless the country has similar legislation to the Data Protection Act.

DPA Responsibilities:

1. Data Controller
2. Data Subject
3. Information Commissioner

(One mark for each item outlining DPA legislation - maximum 10 marks.)

DPA Cloud Compliance Actions and Checks

Discussion could include but not limited to the following:

Risks

- List personal data held and how it will be processed
- Check reputation of cloud provider

Confidentiality

- All communication encrypted
- Cloud provider response to security vulnerability
- Cloud provider compliance with third party security assessment
- Does cloud provider delete all data securely if you withdraw from cloud contract?
- Ensure that your data is not shared with other services delivered by the cloud provider

Integrity

- Audit trails to monitor data access
- Data provided from the cloud in a usable format
- Time for cloud provider to restore data from backup in the event of a major data loss

Availability

- Does cloud provider have capacity to cope with high demand
- Could the actions of other cloud users impact the quality of service
- Would a major outage at the cloud provider impact your business

Legal

- Location where data is processed and safeguards in place to ensure the rights and freedoms of the data subject are protected
- In what circumstances will data be transferred to other countries?
- Limit the transfer of data to countries appropriate to the DPA
- Ensure a written contract is in place to listing the full details of the service
- How will the cloud provider communicate changes to the service agreement?

(One mark for each action / check discussed - maximum 12 marks.)

Report format and presentation – maximum 3 marks.

TOTAL: 10+12+3=25

Examiners' comments:

This was a popular question attempted by many of the candidates, the majority of whom reached the required standard.

Several candidates misunderstood the question and simply described the role of cloud computing in business, with little or no reference to compliance with the Data Protection Act.

However, the majority of candidates produced a discussion that:

- *Demonstrated their working knowledge of the DPA principles*
- *Gave an overview of the cloud computing approach and the associated risks to data*
- *Discussed some security actions that could be taken by the cloud provider to mitigate these risks.*