

June 2008 examination series - Sample script response with commentary
P4 Business Information Systems Auditing - Question 1

- 1 Credit International Group (CIG) offers financial services products to the retail market, including loans, deposit facilities, mortgages and insurance services. CIG conducts a high proportion of its business with customers through the internet. It also has retail outlets in nearly 100 major cities throughout the UK, Ireland and other EU member states.

CIG shares sensitive customer and commercial data with its partners that provide more specialised financial and insurance services for the group's customers. CIG also transfers personal data to a services company that administers the group's payroll and pensions.

CIG has networked computer systems providing for all its customer services and backroom office functions such as procurement, finance and human resources. They also provide email and internet access. The computer systems are hosted at a purpose built facility.

The chief executive has become increasingly concerned by the prevalence of serious information security breaches in other organisations and wishes to minimise the risk of such events at CIG. She has asked the internal audit department to review the effectiveness of the group's computer security and operating arrangements.

As requested by the Chief Internal Auditor, as part of this exercise:

- a Describe** eight controls that would help ensure the confidentiality of sensitive and personal data at CIG. **16 marks**
- b Describe** five controls that would help protect sensitive and personal data transferred between CIG, its commercial partners and the services company. **10 marks**
- c Describe** seven operational controls that you would expect to be in place at the computer systems hosting facility. **14 marks**

"This question covers the controls that ensure the confidentiality of sensitive and personal data and the protection of such data transferred to third parties. It also covers the operational controls provided for a computer systems hosting facility. The question was designed to cover a wide range wide range of controls.

The script is an example of a very successful answer, which gained 34 out of a possible 40 marks. Note that it is well structured, with the volume and detail of each part of the answer matched to the marks available for each part of the question. It has good breadth with a wide range of controls clearly described. It is a full answer having the required number of controls and avoids lists and bullet points, which by their brevity limit the amount of material which can be included in an answer. A good answer plan had been prepared and was submitted with the script."

- a) In order to ensure the confidentiality of sensitive and personal data at CIG there are various controls that would be expected to be in place.
1. Physical security controls - access to CIG's offices should be restricted to authorised personnel. This can be ensured through having an officer manning reception during office hours as well as access cards being required for members or staff to access the building. These could be combined with photographic ID so that an employee's identification could be quickly authenticated in the event of a query.
 2. Once having physically gained access to CIG's offices, there should be another layer of control around access to the computers (ie desktops or laptops) on which the sensitive and personal data is kept. It would be advised to have individual user ID's and passwords for each member of staff. By implementing this level of control the opportunity to access the organisations sensitive information is reduced. It should also enable any inappropriate activity to be traced back to an individual user ID.
 3. Coupled with controls covering access to the organisations networks should be definition of permissions for different users that determine which part of CIG's network each individual user is able to access. Users should have access to the minimum information required commensurate with the requirements of their job. Permissions should be defined for specific groups of users to restrict what information and parts of the organisations network they are able to see.
 4. CIG should have an information security policy that clearly sets out the security requirements of the organisation with respect to the holding, storing, usage and retention of sensitive and personal information. This policy should detail expectations of staff and it should be ensured that all staff are not only aware of, but positively confirm that they understand and will comply with the policy. The policy should be reviewed on a regular basis and updated as necessary.
 5. The information held by the organisation should also be reviewed and classified to ensure that it is clear which information is sensitive. By classifying and labelling all information the organisation can help to ensure that all employees are aware of how data should be treated. This also links in with the earlier controls detailed with regard to the organisations security policy.
 6. There should also be controls around access to and control use of the internet and email. The appropriate uses for these applications may be detailed in the information security policy so that staff are aware of what is permitted, but this should reduce the opportunities for hacking and viruses to be introduced (along with other controls such as firewalls, demilitarised zones, etc).
 7. Personnel controls in the form of reference checking of all new employees should also be introduced. As people are a risk in terms of the dissemination (deliberate or unintentional) of sensitive and personal data, it should be ensured that those employed by the organisation are genuine and have integrity (ie do not lie about qualifications / abilities, etc).
 8. As part of the induction process, training should also be provided to new staff on relevant legislation such as the data protection act, in order to ensure that they are aware of how personal data should be used, obtained, stored, etc.

14 marks awarded out of a possible 16

“A very good answer to part (a) with the required number of valid points clearly described. The answer could have benefited from combining points 7 and 8 by covering induction and training as part of personnel controls. This gives an opportunity to describe one more valid control such as the encryption of all sensitive data.”

- b) As CIG also transfer a lot of personal or sensitive data between themselves, commercial partners and services companies, they also need to be controls in place relating to CIG's communications externally.
1. Encryption should be used for the transfer of data between CIG and its external partners. This provides security in that the information being transferred is protected from interception from CIG to its partners and back the other way. An encrypted message is secure as to be able to access the contents of the message a key is needed. CIG and its partners would have keys to encrypt and decrypt transmissions, but no-one else would have access.
 2. CIG should have detailed contracts or service level agreements in place which clearly specify the requirements for dealing with sensitive and personal information. These documents should be agreed and signed up to by all organisations involved with CIG in terms of sensitive data transfer by someone with appropriate authority. Service level agreements could specify penalties for any security breaches.
 3. In a similar way to the control over internal employees in terms of the checking of references, CIG should review the track record of its external partners in dealing with sensitive information. If security breaches are identified, more rigorous detail may be required in the service level agreement. Even if the company's CIG deals with have been involved with CIG for a significant length of time this exercise is still worthwhile as changes can be made to SLAs periodically.
 4. In terms of the service company, CIG could do periodic checks on the payroll and pensions information held by the services company. This could be a reconciliation between CIG's personnel records and the records held by the services company.
 5. The use of a firewall and a demilitarised zone could also be introduced. This control would help ensure that the information coming in to CIG was valid and free from viruses. It would also assist in preventing hackers from gaining access to the sensitive information held by CIG.

8 marks awarded out of a possible 10

“Part (b) was answered well with the required number of valid points clearly described. The answer could have benefited from the expansion of some points, particularly point 4, such as including reviews of the security arrangements at the service company. The right for CIG to perform such reviews regularly should have been written into the contract and SLA. With regard to secure transmission, examples might have been included such as the use of secure FTP or remote connection by VPN.”

- c) As much of CIG's sensitive and personal data is held on computer, the security and controls in place around the computer systems hosting facility are paramount.
1. It would be expected that access to the facility be controlled through the use of photo ID badges, access cards, etc. The photo ID badges should be required in order to get past reception and access cards configured to allow different members of staff access only to the parts of the facility required for their job. For example, helpdesk staff would not need access to the server room. In addition, there would need to be additional security controls in terms of CCTV which is monitored for unusual activity - especially outside of normal office hours.
 2. In order to ensure that computer systems can be monitored for the back office functions, there should be appropriate detection systems in place at the hosting facility. These should cover fire, temperature, smoke, etc to ensure that any problems which could result in a loss of computer system availability are identified at the earliest opportunity and that appropriate corrective action can be taken, ie power down without loss of information etc.
 3. Appropriate personnel should be employed to operate the facility, this can be ensured by controls around the recruitment process (having detailed job specifications and matching these with qualifications and experience, checking references etc).
 4. Authorisation procedures should be clearly defined and communicated for setting up new users on different parts of the organisations systems. For example, it should not be possible for anyone to be set up with permissions to access HR information without authorisation of the HR manager.
 5. High level passwords, those held by super users with permissions allowing the set up of permissions and other high level tasks should be restricted and monitored by an officer with appropriate authority, for example the Head of ICT. Consideration should be given to use of one time passwords or alternatively passwords should be changed on a regular basis.
 6. A business continuity plan and disaster recovery plan should be developed and tested to ensure that the critical functions of the business can continue in the event of a disaster. As the hosting facility deals with all procurement, finance, HR, and internet and email access the loss of availability of this will have a critical impact on the running of CIG.

7. A further operational control would be around network security. As the hosting facility deals with email and internet access, it should have controls in place such as firewalls and anti-virus checking software. This should reduce the risk of attacks from hackers and reduce the likelihood of the organisations information and data being compromised by infection from viruses. There should also be regular back up of the companies information so that information can be restored should an attack be successful and information is lost.
-

12 marks awarded out of a possible 14

“A good answer to part (c) with the required number of valid points clearly described. The answer shows knowledge of a range of operational controls and did not concentrate on physical and environmental controls to the exclusion of anything else. The answer could have benefited from the expansion of some points. For example, point 3 on having competent operators could have included the requirement for technical training and effective operating procedures. Point 4 could have covered the use of logical access controls to ensure segregation between developers, users and operators, and between development, test and live operating environments.”
