



SECTION A

Question 1 was the most popular question with 59% of the candidates choosing it, followed by question 3 (25%) and the remaining candidates (16%) completing question 2. Disturbingly, about 3% of all candidates attempted to answer all three questions with a few of those completing all the three questions at 'A' standard.

Many candidates used the word "computer" generically to mean "software" or "output devices"; for example "the computer will collect and process the data" rather than specifying the type of software used for such a process. Similarly, some candidates seemed to have little understanding of the difference between the Internet and the World Wide Web with both terms used interchangeably.

In general, candidates tended to answer these question from the limited perspective of desktop computers and tended to display a poor knowledge of processes, products and technologies used by the IT industry, such as xml, asp, portal technologies...

Question 1

- (a) In most cases candidates dealt with the issues of presenting multimedia on the web rather than with the production of the multimedia materials by the owner(s).
- (b) Very few candidates were aware of dynamic data exchange and server site scripting, such as php and asp, to access data from databases and not having to change the website each time the room availability is changed (data in the database is changed and uploaded to the web site using php or asp). It is a concern that no candidate made mention of xml.
- (c) Very few candidates considered other communication technologies such as the telephone. Considerable confusion occurred with describing video conferencing with no candidate making reference to video conferencing technologies being delivered via the public switched telephone network.

Question 2

- (a) See comments for 1b. The need for security for the wholesale purchase of drugs by the chemist was only mentioned by a few candidates.
- (b) A large number of candidates were confused by the difference between a database and a spreadsheet. Few candidates considered specialised database software such as integrated accounting software that can track product sales using barcodes and keep track of stock levels.

Linking the data to promotion activities was discussed by most candidates.

- (c) Although security issues were discussed by most candidates, few mentioned security arrangements on the web, in depth, or only discussed issues familiar to the average technology user, such as firewalls and virus protection. No candidate mentioned the use

of certificates nor encryption options with private and public keys. VPN was mentioned by very few candidates attempting this question.

Question 3

- (a) Most candidates suggested the use of biometric devices for added security. In general this question was done well and better candidates distinguished between the practices that the user can employ and the practices that have to be implemented by governments.
- (b) Most candidates mentioned the use of Database Management Systems without discussing how they work and interact with the data. Data integrity scans and validation systems, based on age of data, were discussed by most candidates.
- (c) This question evoked a varied mixture of poor responses from candidates who merely rephrased the SDLC, and extremely sophisticated responses from candidates attempting to use the frame of the SDLC for the development of a law-enforcement system, around passports.

Section A – Sample Solutions

Question 1

- (a) Video capture card, video editing software, video player plugin. Consider file size, access to web if software needed. Use of compressed video.
- (b) Validation routines in software, or use of an active web that interfaces with the bookings database. Use of mandatory fields. Some organisations use a test website, that is later made live.
- (c) Hardware – networked PC, webcam
Software – Collaboration software – netmeeting, Messenger
Communications – Connection to ISP – modem (analog or digital) – high speed
Application such as outlook – calendar, email
Web browser
Meeting reminders via email.

Question 2

- (a) Stock control software 'flags' the need for new stock.
Need network access, secure network (VPN). Client ID and password, validation of quantities ordered. Select product and quantity. Payment via direct deposit or electronic banking.
- (b) Database or spreadsheet software. Database would provide sales data which could feed into graphing system for trends. This could include sales for each month (over a number of years), order sizes, payment history etc.
Promotion could be by email distribution lists. Presentation software for in-store promotions.
- (c) Business to Business. Set up a VPN and intranet. Centralised database. Standards for transmission.

Provide username/password. Encrypt data during transmission. Use public and private keys. Bandwidth – use ADSL/ISDN. Can use terminal Services. Use VPN.

Question 3

- (a) Have minimum size, expiry, mix of letters and digits, non reuse, explain good password practice.
- (b) Data entry checks – double entry. Scan for inconsistencies / corruptions – integrity tests. Date stamp data. Have a disaster recovery plan which includes offsite storage, hot or cold sites.
Backup techniques.
- (c) plan – collect information about the system from all users and sources – police, customs, passport issuers etc
Design – relationships and procedures – data dictionary. Procedures to collect data and ensure validity for passport issue. Database entry, access, security, searching, forgery management
Develop and implement – code and deploy – phased / cutover
Maintain and review – performance, backup and enhancements such as biometrics

SECTION B

Overall there was quite an even distribution of questions answered by candidates in this section. The least popular questions were 5b and 6c.

About 25% of candidates answered the same scenario for each question (e.g. 4a, 5a, 6a) whereas approximately 60% answered two parts of the same scenario (e.g. 4a,5b, 6a)

Question 4

- (a) This question was answered quite well. Most agreed on the feasibility of a website for each B&B and many candidates suggested that the best idea would be to have a master site for all B&Bs.
- (b) Many candidates gave a positive response to this question but many didn't appreciate the concept of a smart card and assumed the card acted as a link to a database.
- (c) Many candidates assumed a high cost for this proposal and suggested that biometrics would best be used to protect a small number of high security areas as opposed to all areas.

Question 5

- (a) Many candidates suggested that satellite communication was the answer and disregarded dial-up solutions.
- (b) This question was answered quite well with most candidates agreeing with the sentiment of the question. Some students wrote about RFID tags and became somewhat sidetracked.

- (c) Most candidates were not in favour of this idea, especially when they assumed the expert system would be used in isolation rather than in conjunction with a legally trained person. Many objected to the fact that human emotions such as compassion would not be present. Some did not appreciate what an expert system is and assumed some type of "computerised terrorist test"

Some candidates, having little concept of an expert system, discussed an e-judge conducting trials in a remote location.

Question 6

- (a) Most candidates thought this was a good idea and assumed some type of video 'walk through' on a website as opposed to the full VR experience (with goggles etc.) for which they thought there was little benefit.

Candidates generally did not show an understanding of VR and the technology involved, but gave good answers to video/dvd/images on the net.

- (b) Many candidates answered this in a superficial manner and showed no deep understanding of the concepts, especially that of *customer profiling*. Many pointed out problems with tracking due to the fact that customers are not required to identify themselves.

There was some confusion between prescription medicine and over-the-counter medication and the need for identification with one but not with the other.

- (c) Those candidates attempting this question generally answered it quite well although they tended to concentrate on firewalls while ignoring physical security.

Some good answers to outsourcing databases to places like India. One candidate gave a detailed account of the Four Corners program on this topic.

Section B – Sample Solutions

Question 4

- (a) Need somewhere to host it, either their own web server or use a commercial site. They would need to manage the content, so would need some web experience. More likely they would pay someone and would have to pay for hosting the site and for access to the site. Computer equipment costs.
- (b) Its quite possible. An example is the new Medicare smart card. Cards are cheap, readers / writers are common. Data could be recorded at point of sale and when visiting doctor.
- (c) Technologically feasible but more expensive. The equipment is more complex and expensive, and the database would be much larger. Voice, retina, fingerprint. Setup costs.

Question 5

- (a) In Tasmania, internet access is widespread and access can be by dial up, broadband or ISDN in many areas. More remote areas can link via radio, satellite. These technologies make it possible. Cost may be greater for slower access if the volume of access is greater (e.g. graphic and video / sound).
Operators need to be computer literate.
Need to provide alternative booking systems.
Need to carry out cost benefit analysis.
- (b) Stocktaking using wireless technology should be both operationally and economically feasible. A wireless laptop and an access point (few hundred dollars) mean that the stocktake can take place where the items are, without cables. Technologically feasible, but need to be careful about security, although the data travelling will generally be unintelligible.
- (c) Technologically an expert system could be built with much of case law in it. Since much of law is based on precedent, the expert system could guide potential decisions, however a human would still be needed to assess extenuating circumstances. Operationally, there would be a substantial workload in preparing for the electronic judgement. Economically, it may arrive at a decision faster, but an expert would be needed to set up each case.
Costs of courtroom.
Not really practical.

Question 6

- (a) Technologically, it is possible to use virtual reality experiences to show an environment and to have limited interaction (touch, motion, see and hear). Operationally it would take a great deal of work to set up the experience, and the tourist would have to be in a location where the specialised hardware was present. The experience wouldn't work well over the internet. Economically, the cost of development would outweigh the actual experience.
- (b) The technology is there to do this. However, actually tracking purchases would be a problem as customer is currently not required to identify themselves. They could also get others to make the purchases on their behalf. Privacy prevents this. Pharmacists have to do the work which adds to their costs. Cost of equipment to record the data.
- (c) It isn't economically practical to totally secure all government websites and databases. A value must be placed on the data and a reasonable level of security implemented. It is technologically possible to have highly secured sites (physically and by firewall). This can include optical only communication (military). Many attacks on data come from inside – so need an access system that provides only limited access by each user. Encryption may help deter data theft.

Outsourcing will require a lot of knowledge transfer to the service providers so that they can build and maintain the systems. But more people have access to data.

SECTION C

In general there tended to be a failure to read questions clearly to identify exactly what was required. This was worse for part a of each of these questions. In Q8(a) candidates tended to address the needs of the tourist instead of the B & B operator.

In Q8(a) and Q9(a) the scatter gun approach was also frequently used. "Write down as many pieces of hardware and software I know and I must hit the correct ones and get credit for these" These same candidates often failed to address the money transfer and the security required. A number of candidates also launched into a feasibility study, using up valuable time.

The sending/use of videos was often neglected.

In general, candidates did not understand the small and personal nature of B & Bs and planned systems that would have better suited large motel chain complexes.. Many candidates nominated age and/or birthdate as required data from a potential customers prompting unanswered questions such as: - Will I be banned if I am over 65? Is there concern I might die in one of their beds? ...

A significant number of candidates attempted at least one of Q8(a) or Q9(a) and often both. Students who attempted the other parts tended to be more focussed in their answers although it seems the there are only two ways to protect the database Q8(c); firewall and encryption though others were mentioned further on in the paper.

In summary, the majority of candidates gave satisfactory answers to this section, but high quality answers were few and far between.

Subject teachers should remind students that their writing needs to be clear and relatively easy to read by ageing markers.

Section C – Sample Solutions

Question 7

- (a) Data compression involves representation of data in a more compact way. A common technique is to identify long sequences of the same pattern and store these as a number followed by the pattern. When decompressing, the number determines how many times the pattern will be regenerated.
- (b) Client server refers to one process which provides information or some process (the server) for another process (client). Often the client and server are on separate computers and operate over a network. A good example is a database server (server) that provides information to a request from a client computer.
- (c) A firewall is software (or hardware) that examines each packet entering a system to determine if it satisfies some specific criteria. These may involve addressing or content. Usually configured with a set of rules which determine if a packet will pass or not.

Question 8

- (a) Hardware can be a simple terminal with web interface, running a secure session. It is normal to have a magnetic card reader for reading credit card details and carrying out transaction. Software will be web based secure payment system for transactions using credit card details – encryption. Need a network connection such as phone / modem, ADSL, ISDN.
- (b) Barcodes – single number in binary format used as an id. for a product line. Read optically using a scanner.

E-tag – identifies a single item. Read electronically, has storage on them for data. Can be read without physical or visible contact.

- (c) Firewalls – hardware and software, private IP addresses, biometric devices, encryption, password security and authentication procedures.

Question 9

- (a) Need a network throughout building, server with web connectivity and database software. Rooms would have touch screens. Regional attractions could be from in-house intranet with links to internet for specific provider's information. Email needs 'post office' software. Video needs some sort of digital video system to select, capture / compress, or feed video from a digital source. Telephone could use a voice over IP system.

- (b) An expert system could give guidance on side effects. Patient reaction database would be helpful also.

A VPN across the internet would allow electronic prescriptions, but validation of the doctor would be needed (digital signature).

There are many web sites with drug information and chemists could make their prices available on the internet (although they often like to keep this information from their competitors). Shopping bots.

- (c) Can be optical (infrared) which covers only a small area and is relatively safe (but slow). More likely radio based, and others outside may gain access because of the wider coverage area. Security such as WEP and WPA along with MAC filtering. Coverage - number of devices versus throughput?

SECTION D

Question 10

Most candidates answered parts (a) and (b). Better candidates discussed the people issues and the ethical issues associated with the term rather than merely defining the terms. For example: National Privacy Principles are the guidelines that both gov't and private sectors must adhere to in the collection, handling, storage and distribution of data about people. The main issues involve the important need to ensure that a person's data is kept private so that his rights and overall welfare is not compromised in any way. Failure to adhere to NPP may result in people being harassed, discriminated against etc.

Electronic work monitoring issues concern the employer's right to know at all times what an employee is doing and the rights of workers to feel that they are not being harassed and having to work in a stressful environment.

Parts (c) and (d) were answered quite poorly with some candidates resorting to creative answers when unsure.

In part (c), better candidates discussed the need for a personalised HCI so that all can use a computer efficiently. This would require people with disabilities to have an HCI such as a GUI or interactive touch screen whilst a less restrictive one for power users.

Question 11

Approximately 60% of the candidates answered part (a), 30% part (c) and 10% part (b).

In part (a) most candidates were able to comment on the B & B's responsibility to request permission from the customer to pass on information to other B & Bs. Better candidates attempted to list data that might be shared with other B & Bs with respect to the National Privacy Principles. Some also commented on the ethics of sharing information within the same organisation. Poorer candidates referred to situations where the customer "trashed a room" as the only situation in which it was ethical to pass on information to other B & Bs (without reference to passing it on to the police).

In part (b) most candidates commented on requesting the customer's permission to pass on information. Most did not comment on the ethics of collecting data without identifiers. Very few candidates showed why the groups mentioned (the health department, employer groups and health insurance companies) might want to collect and analyse this data. Instead, they tended to comment that sharing this information would cause an individual's premium to rise or that an individual might lose his/her job due to health issues.

In part (c) some answers took a somewhat naïve attitude to what monitoring would mean and what the Internet is really used for. Better candidates demonstrated an understanding of the need for governments to monitor email/chat etc., and the individual's right to ensure their emails or communications remain private. Poorer candidates focussed only on the individual's rights and did not represent both sides of the issue.

Section D – Sample Solutions**Question 10**

- (a) Refers to what can be done with personal data. Includes accuracy, age, distribution and purpose for collection. Responsibility of collector.
- (b) Electronic work monitoring uses the technology that an employee is using to record the amount of work the employee is doing. Can record throughput (transactions over time), error rate, length of breaks and so on. Impacts on stress, unfair dismissal.
- (c) Human Computer Interface details how the user interacts with software – GUI is a prime example, but specialist hardware also exists – inclusion.
- (d) Data-mining – searching through existing data to extract information of value. Using data for a purpose different to that for which it was collected.

Question 11

- (a) The tourists would need to be told that their data would be shared and why. The tourist may not want some of the information disclosed to operators that they do not intend using. There is the potential for misuse of the information. Covered by Privacy laws.

Sharing would be ethical if they were the one organisation and the information was needed in a life threatening situation, or when the law had been broken.

It would not be ethical to use the information to force unwanted services on the tourist.

- (b) The people would need to give permission for their information to be used in this way, otherwise the data is being used for a purpose different to that for which it was collected. If the information did not allow identification of the person, then its ok? Who owns this data/information?

Discussion of current Privacy Laws with reference to disclosure of collection and forwarding of data/information. Discussion of whether the release of this type information is detrimental to disabled/elderly.

- (c) It's ok if access is being used in the commission of a crime, or if citizens are informed that this will happen. The methods used to identify potential terrorist would need careful development so that innocent people weren't caught by the surveillance.

The Government has the responsibility to keep its citizens safe; citizens have the right to keep their (law abiding) activities private. Citizens would need to be told that their access was being monitored.

Transborder data flow would be subject to different laws in different countries.

Option to draw similarities with other types of monitoring and their appropriateness and acceptance.

SECTION E

Question 12

- (a) Although a popular question, few referred to IT-related copyright, e.g. of programs. A common error was to incorrectly refer to the covering "ideas".
- (b) In general, clearly answered by about 20% of candidates, but sometimes lacked sufficient details for good assessment (3 - 4 good points expected).
- (c) Most candidates demonstrated a good understanding of this topic, and referred to the importance of keeping anti-virus software up-to-date. The most popular question.
- (d) Though answered by only 15% of candidates, most did so accurately. Some candidates confused security protocols, e.g. SSL, with digital certificates as an authentication tool.

Question 13

- (a) Many candidates did not address most/all parts of the question. In general, only a superficial explanation of the increasing value of IP in today's world was given.
- (b) Many candidates presented an extensive argument why customers shouldn't give approval – but that was not the question! Many also suggested that chemists might give "prescriptions history" – unlikely.

Candidates rarely gave details of privacy expectations on the part of health and fitness clubs, and the ability of customers to inspect their data, edit, cancel, etc.

- (c) Candidates often confused spyware with viruses. Spyware would not (normally) corrupt data. The full range of questions was rarely answered.

Section E – Sample Solutions

Question 12

- (a) Copyright – the right under law for an author, artist, musician, etc. to control the distribution of their work and the expression of their idea. Includes software (1984 Amendment to Copyright Act).
One of the IP protections, together with patents, trademarks, trade secrets.
- (b) Australian act makes it illegal to send unsolicited, commercial, electronic messages (email, SMS, ...) to users, with some exceptions, e.g. politicians, religious organisations. Generally done for economic reasons.

Act also provides rules for how legitimate commercial electronic messages can be sent (receiver's consent, sender's address, 'unsubscribe' option).
- (c) Malicious software designed to disrupt/destroy data and systems. Where viruses are designed to act **on** a computer, worms spread **through** networks, blocking network paths.
- (d) Digital certificate – electronic verification from a trusted source that the item in question comes from who they say they are (e.g. person or website). Trusted third party. Uses key system.

Question 13

- (a) Permission must be obtained to use the logos (no permission required for links). The intellectual property is the development that went into developing the logos, they represent the particular company. Permission must be gained because the logo may be associated with something that is derogatory towards the company.

Many companies are identified by their logo, also the logo may attract customers because it is clever, etc.

The BBA's website has text, pictures, perhaps audio/video content, and website colour schemes, etc. as IP.

A definition of Intellectual Property should be included. Notion of Intellectual Property is beginning to be ignored as copy/paste becomes common place.

A company's value is based upon their intellectual property and the information held by the company. Many people/companies do not 'make' anything physical in this 'information age', but earn significant income from their IP, eg. Google, software companies, eBay. Copying/plagiarising music, videos, programs deprives their creators of income.

- (b) Socially, the client gets access to new range of services, the clubs get access to potential new clients. Legally, client releases his rights; chemists have freedom to do many things. Fitness club has obtained data legally. We may end up with a fitter society? Economically

the club gets the data cheaply, the chemist makes a profit selling the data, the client may get cheaper services.

- (c) Spyware is software that sits on your computer and reports information back to its owner. It is often installed as a result of trying some free software, or visiting a particular website. The software can report on what websites you visit, or what applications you have on your computer etc. It allows the supplier to gain information without your knowledge, and use it for whatever purposes they choose. Sometimes associated with popup ads and browser hijacking. (Some spyware is approved by the user.)

There is a significant cost involved in protecting systems against spyware, both in time and disk space, slower systems, data communications costs for transferring unwanted data etc. Owners of databases have a legal obligation to protect data they manage (Privacy Act).

State and Federal laws emphasise the criminality of illegally accessing data, but prevention of attack is better than tracking down the hacker later.

All correspondence should be addressed to:

Tasmanian Qualifications Authority
PO Box 147, Sandy Bay 7006
Ph: (03) 6233 6364 Fax: (03) 6224 0175
Email: reception@tqa.tas.gov.au
Internet: <http://www.tqa.tas.gov.au>