THE BCS PROFESSIONAL EXAMINATIONS
BCS Level 6 Professional Graduate Diploma in IT

April 2008

EXAMINERS' REPORT

The World Wide Web – Beyond the Basics

General Comments

This was the final time this paper was on offer, having been superseded by the paper Web Engineering. The quality of answers was generally poor in comparison to previous years.

Recurring issues from previous years, which still remain issues today:

- Many candidates write far too much often taking two or more pages to make a simple point worth very few marks.
- Handwriting continues to be an issue. There is ample time to write clearly and carefully whilst answering all questions in full.
- There is a tendency for students to consider the answer pointers in these reports as full and complete answers and quote them verbatim, without considering the context of the actual question asked. This is not appropriate for a paper at this level, and does not score highly.
- The answers continue to be very heavy in textbook theory and not sufficiently contextualised. Answers must refer to real life issues, events and topics when asked.

.

Question 1

You are acting as a consultant for a financial institution, advising on the development of an online banking service.

(a) One possible security risk to a banking site is **brute forcing** the password; this is often solved by locking out an account after a certain number of unsuccessful attempts.

(i) What is meant by a brute force attack?

(2 marks)

(ii) Aside from a brute force attack, outline **FOUR** other security risks and, for each risk, describe a method to prevent it.

(8 marks)

(b) The in-house developers have outlined three possible schemes for authenticating their users. You have been asked to comment on these systems from a *security* perspective (how safe the scheme will be) as well as from a *user's* perspective (how easy the scheme will be to use).

Proposed scheme A

- Type in your *email address*
- Type in your *password* (6 characters, alphabetic)
- Select the first and the third digits of your *PIN* (6 digits) from a drop-down list

Proposed scheme B

- System-generated *user number* (created on registration, 11 digits long)
- Type in your *password* (6-12 alphanumeric characters)
- Type in your *mother's maiden name*

Proposed scheme C

- Type in your *first name*
- Type in your *last name*
- Type in your *postcode/Zip code*
- Type in your *date of birth*
- Type in your *favourite colour*

(i) For each of the three schemes, outline **TWO** strengths and **TWO** weaknesses.

(9 marks)

(ii) Devise a new scheme for authenticating users on this site which is superior to all three schemes outlined above. Explain how it overcomes the weaknesses identified in part (b)(i).

(6 marks)

Answer Pointers

a)

(i) A brute force attack is a method of breaking a cryptographic scheme by trying a large number of input possibilities (e.g. trying all 10,000 possible combinations of a 4-digit PIN).

(ii) Sample risks include:

- Phishing (Microsoft's anti-phishing filter).
- Packet sniffing (use encryption).
- Keylogger on client machine (check physical hardware and/or run a rootkit checker/antivirus).
- SQL injection attack (ensure all user inputs are validated on the server side).
- Denial of service attack (maintain mirror of server application & data).
- Spyware on client machine (use antivirus/spyware checkers).

- Not destroying letters with sensitive information e.g. passwords (shred confidential documents when disposing).

b)

(i) Possible answers:

	Strengths	Weaknesses
A	• Reasonably easy to remember login details. • Defends against keylogging by using drop down lists • Partial defence against phishing by only needing two digits from the PIN.	• Short alphabetic password gives only ~300 million combinations => brute forcible. • Requiring only the first and third digit of the PIN gives only 100 combinations.
B	• Reasonably strong password. • Relatively fast to log in (only three text fields to be entered).	• Difficult to remember login details (randomly generate user ID), so more likely to write details down. • Mother's maiden name is known by other people (e.g. family members). • All data is typed, so susceptible to keylogging.
C	• Very easy to remember login details. • Requires a collection of details that would be very difficult to brute force (but not find out through other means).	• Susceptible to identity fraud, as login details are almost entirely based on common personal details. • Lots of details to be typed in. • Favourite colour might be guessable (e.g. most people would choose a primary colour or black) • Susceptible to keylogging.

(ii) An open question, but solutions must address all weaknesses of the previous schemes (both security and usability), whilst remaining reasonably simple for the end user. Possibilities might include:

- Selecting random digits from a 6 digit PIN instead of merely two predetermined ones.
- Asking for one personal detail from a random selection (e.g. mother's maiden name, favourite colour, and name of first pet).
- Offering to remember the system username (not advised for multi-user PCs or accessing the site from a public computer).
- Allowing passwords to be alphanumeric and of variable length, with a sensible minimum length (e.g. 6 characters).
-

Examiners' Guidance Notes

Very few candidates appeared to know what is meant by "brute forcing", with many equating it to "hacking into a server". The answers given for part a) ii) were overly generic – textbook definitions of basic threats did not carry many marks unless applied to the problem this question is concerned with – e.g. that of securing online banking. Solutions given to the problems identified were often very basic. Part b) i) was reasonably answered from a security point of view, but less so from the user's perspective. Generic statements that "the password is not secure" is not sufficiently critical to be awarded marks without a reason. Part b) ii) was poorly answered in almost every case – the idea was to demonstrate that the new scheme addresses all the weaknesses from previous schemes. Simply mentioning the use of biometrics without explaining how it addresses the problems (and without mentioning the practicalities of such schemes from a usability perspective) was not worth many marks.

Question 2

A company selling digital cameras wishes to enhance its website to incorporate e-commerce. To this end, four modules are to be added to the existing website:

- User Registration & Login;
- Shopping Cart (links into existing company financial and stock control databases);
- Check Out (converting a *Shopping Cart* into an order, taking payment); and
- Order Management (status of existing orders, cancelling pending orders, etc.).

(a) (i) State **THREE** possible solutions to the problem of handling payments.
(3 marks)

(ii) Adopt **ONE** solution from part (i) and give a reason why it is preferable to each of the other solutions outlined.
(2 marks)

(b) In terms of the customer shopping experience on the website, outline the required functionality of the *Shopping Cart* module.
(6 marks)

(c) (i) Considering any **THREE** of the modules, identify the key aspects that would form a core part of an *acceptance test plan* for each. Amongst other things, the test plan should specifically address issues of performance and security.
[Note: individual detailed test cases are not required here.]
(10 marks)

(ii) Construct an *integration test plan* involving all four modules.
(4 marks)

Answer Pointers

a)

i)

- Third party: Paypal/Google checkout
- Credit/debit cards in real time
- Credit/debit cards over the phone
- Cash on Delivery
- Vouchers
- Cheques

ii) Any logically argued and consistent method is acceptable, so long as it considers speed, security, and cost. The argument should consider the relative size of the company, number of transactions per time period, etc.
The recommendation of slow methods (e.g. cheques, COD) would have to have a very strong justification.
Depending on the cost of custom built check out with the added cost of security and fraud prevention (Authentication, Authorisation and settlement), it might be cheaper to adopt one of the following on offer say from Google

- Buy Now buttons
- Email invoicing
- Off-the-shelf shopping trolleys
- Custom-built shopping trolleys

b)

Functionality could include:
Browse items, search for an item, place an order for a single item, place an order for a number of items, Check for availability of an item, amend an order to increase/decrease the quantity as well as deleting an item. Have an itemised cost and running total and postage/delivery costs, times including taxes, save shopping cart for later.

c)

i) Construct a coherent unit test strategy looking only at the individual modules, not at the interaction. Possible aspects to consider could include:

User Registration and login	**Shopping Cart**	**Check out**	**Order Management**
Load testing: • No of concurrent users Verification of functionality: • Address lookup on post code Data Validation: • House number/name • Email address – valid characters and verification • Title (Mr, Mrs, etc.) • First name & Last name – valid characters (accented letters?) • Password – a mix of characters and digits and a min length • Unique username	Load testing: • No of concurrent users Verification of functionality: • Browse item to display correct amount in stock • Order a single item • Order multiple items • Amend orders to increase/decrease quantity by one, qty 1 to 0 should be removed from the cart • Qty cannot exceed stock level • Qty must be positive digits with error trapping and offer to re-enter qty • Each item selected should be displayed with a qty chosen and cost and running total • Check the figures • On-the-fly currency conversion estimation?	Load testing: • No of concurrent users Verification of functionality: • Currency conversion/choice of currencies? • Payment options • Correct delivery charges • Correct taxes • Delivery address • Delivery options – free express, next day • Order saved for a latter session • Confirmation of order • Confirmation of payment approval Verification of security: • Valid server digital certificate • SSL, appropriate	Load testing: • No of concurrent users Verification of functionality: • Correct Retrieval of an order • Time stamped for cancellation to be valid until • Payment not approved – order cancelled or user informed • Time until which order can be amended – amendments to be done – confirmation of amended order

ii) The integration test should consider the interaction between the different modules – e.g. adding products to the shopping cart and then checking out, trying to check out when not logged in, cancelling an order that doesn't exist, adding items to a shopping cart when not logged in, trying to check out with an empty shopping cart, etc.

Examiners' Guidance Notes

Part a) was well answered. Part b) was considering the site from the user's perspective, but many candidates simply quoted the answer pointers from last year's paper – which did not apply this year. For example, candidates would talk about the "producer" and "owner" of the site, instead of focussing solely on the "user." Part c) was poorly answered. Candidates failed to appreciate that the acceptance test would have been conducted by the owner, not the users. Part c) ii) was answered well in some cases, but many were quite theoretical in nature rather than considering the actual modules outlined in the question.

Question 3

(a) (i) List the characteristics of ***static*** and ***dynamic*** web pages.

(3 marks)

(ii) Outline the technologies and tools used in the creation of a static web page containing images.

(3 marks)

(iii) Aside from those elements mentioned in (ii) above, outline the additional technologies and tools used in the creation of a dynamic web page.

(4 marks)

(b) Figure 3.3 (overleaf) details the source code of a web site for an electronics retailer.

(i) Draw a diagram to complete the missing sections A, B and C indicated in Figure 3.1 (overleaf) to illustrate the output of this file when it is first loaded in a browser window. (State the browser you are assuming use of.)

(3 marks)

(ii) The page has JavaScript actions attached to it. Describe what will happen on screen in relation to user interaction with the page.

(4 marks)

(iii) The retailer wishes to add extra details to the web page, with the same format and functionality as the current content. Write code to enable the menu group displayed in Figure 3.2 (overleaf) to be generated and displayed in the same way as the other groups. **(4 marks)**

(iv) Using CSS, list modifications to the code to change the appearance of the listed groups to the following:

Cameras: Bold text, surrounded by a solid 3-pixel border

(2 marks)

PCs: Italic text, surrounded by a dotted 2-pixel border

(Note: Your answer should list only the changes and additional lines required.)

(2 marks)

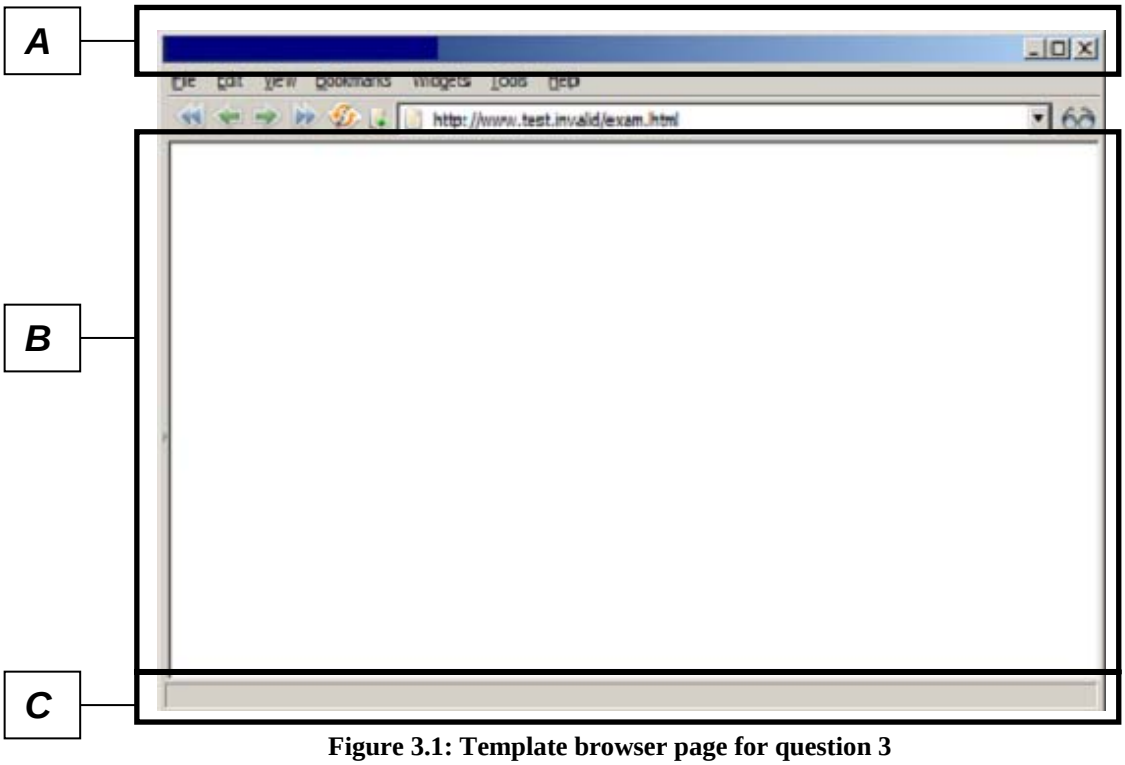


Figure 3.1: Template browser page for question 3

Microwaves

Sharp

Figure 3.2: Menu group to add for question 3

```
 1: <!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN"
 2:         "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">
 3: <html>
 4:     <head>
 5:         <meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1" />
 6:         <title>Electronics Limited</title>
 7:         <script type="text/javascript" language="javascript">
 8:         <!--
 9:         var activegroup = 0;
10:         var mingroupnum = 1;
11:         var maxgroupnum = 3;
12:
13:         function togglegroup(){
14:             activegroup++;
15:             if(activegroup > maxgroupnum) {
16:                 activegroup = mingroupnum;
17:             }
18:
19:         for(i = mingroupnum; i <= maxgroupnum; i++) {
20:                     thisgroup = eval("document.all.group"+i+".style");
21:
22:                     if(i == activegroup){
23:                         thisgroup.display = "block";
24:                     }
25:                     else {
26:                         thisgroup.display = "none";
27:                     }
28:                 }
29:              }
30:         -->
31:         </script>
32:         <style type="text/css">
33:             .group { display:none; margin-left:20px;}
34:         </style>
35:     </head>
36:     <body bgcolor="white">
37:         <h1 onmousedown="togglegroup()">Click here:</h1>
38:         <h3><a href="page1.html">
39:             Cameras</a></h3>
40:         <p id="group1" class="group">
41:             Sony<br />
42:             Canon
43:         </p>
44:         <h3><a href="page2.html">
45:             Televisions</a></h3>
46:         <p id="group2" class="group">
47:             Panasonic<br />
48:             Samsung
49:         </p>
50:         <h3><a href="page3.html">
51:             PCs</a></h3>
52:         <p id="group3" class="group">
53:             Dell<br />
54:             IBM
55:         </p>
56:         <p>
57:             <a href="http://validator.w3.org/check?uri=referer"><img
58:                     src="http://www.w3.org/Icons/valid-xhtml10"
59:                     alt="Valid XHTML 1.0 Transitional" height="31" width="88" /></a>
60:         </p>
61:     </body>
62: </html>
```

Figure 3.3: Source code for question 3

Answer Pointers

a)

i) A static web page has the following characteristics:

- Interaction only through traversing hyperlinks or through plugins.
- Information controlled by the website creator.
- No ability to configure the presentational aspects of the site, except at a local browser level.

A dynamic page tends to have at least some of the following characteristics:

- Can respond to input data provided by the web browser when retrieving the page.
- Can alter or customise the output based on certain factors or criteria.
- Can obtain information from external sources e.g. databases.
- Can be transaction based

ii)

Static development tools and technologies include:

- Web page editor (either a standard text editor e.g. Notepad, or a WYSIWYG editor, e.g. Dreamweaver) for writing HTML.
- Image acquisition and manipulation tools e.g. Scanner, Photoshop
- File transfer software (such as FTP - possibly built into the web page editor)
- Web server (e.g. Apache)

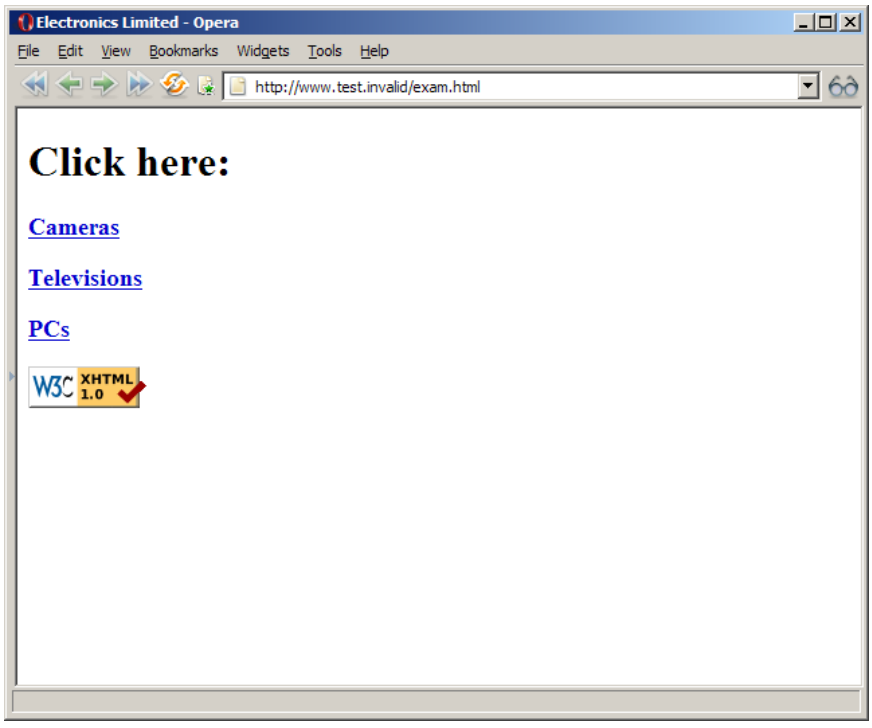
iii)

Dynamic development tools and technologies include:

- Scripting languages (e.g. PHP, ASP, JSP, Coldfusion, Perl)
- Possibly development tools/IDE for the dynamic language (e.g. Coldfusion, NetBeans).
- Web server supporting the chosen dynamic languages

b)

i)



When the mouse is clicked over the page header (the text marked “click here:”, the first menu will open. When it is clicked a subsequent time, it will close the current menu and open the next one (e.g. from Cameras to televisions, from televisions to PCs, from PCs to cameras).

ii)

Amend line 11:

```
var maxgroupnum = 4;
```

Add in line 50:

```
<h3><a href="page4.html">
    Microwaves</a></h3>
<p id="group4" class="group">
    Sharp<br />
    Sanyo
</p>
```

iii)

Add the following code after line 33:

```
.camera { font-weight: bold; border: 3px solid black; }
.pc    { font-style: italic; border: 2px dotted black; }
```

Amend line 40:

```
<p id="group1" class="group camera">
```

Amend line 52:

```
<p id="group2" class="group pc">
```

Examiners’ Guidance Notes

In general this question was well answered. However, part b) ii) was poorly answered – candidates assumed that it was the question from a previous year, but the JavaScript actions were entirely different – as they are on each paper.

Question 4

You have been asked to comment on the structure of a number of prototype websites of “NuPhone” – a mobile phone retailer.

(a) List, with brief explanation, **FOUR** characteristics of a well-defined, user friendly navigation scheme for a website.

(4 marks)

(b) One initial prototype site consists of five pages including the home page. The navigation scheme links every page to every other page.

(i) Display the above navigational scheme in a graphical format.

(2 marks)

(ii) State the advantages of such a scheme.

(2 marks)

(iii) Discuss the feasibility of using this scheme if the site increases in size (as a starting point, consider the site size doubling to 10 pages, and so on).

(5 marks)

(c) A second prototype consists of 100 web pages covering 4 distinct areas (i.e. each area will have about 25 pages). In addition, the site has other files to support the web pages (e.g. image files, script files, style sheets and multimedia content). The prototype design has not yet been laid out in terms of actual site structure and navigation.

(i) Discuss how the site should be structured from maintenance and enhancement viewpoints.

(4 marks)

(ii) Design a navigation scheme for this prototype and present it in a graphical format with a brief explanation and justification. You should make clear the use of global links within the site and the use of a breadcrumb trail.

(8 marks)

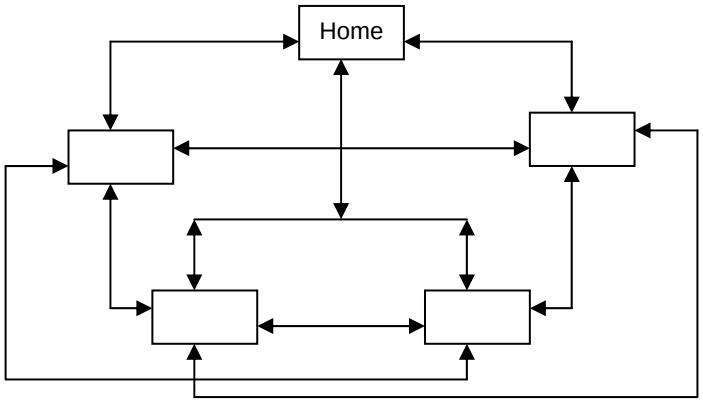
AnswerPpointers

a)

- All links are meaning full in text and appearance;
- Consistency in the use and positioning of the widgets
- User is always aware of where he/she is on the site
- Easy to revisit a visited page – breadcrumb trail and global links

b)

i)



ii) One click to reach any other page, simple, all options available all the time

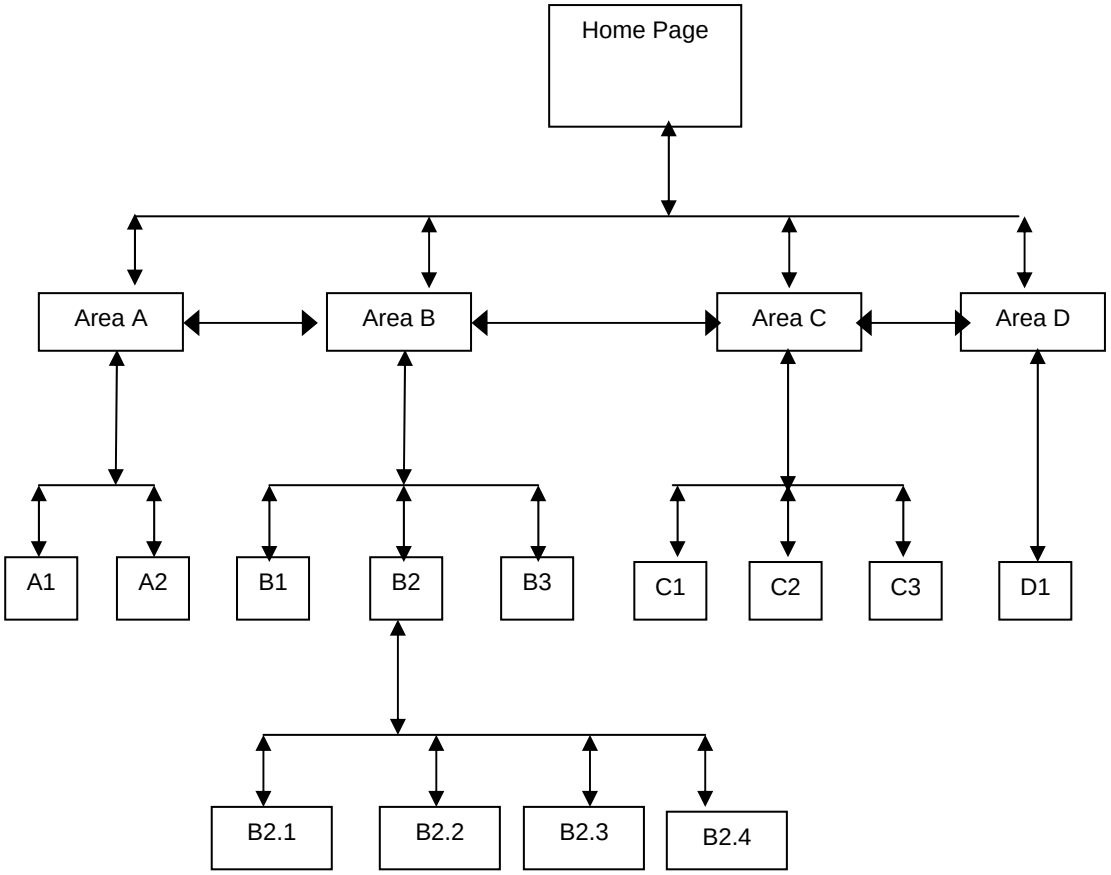
iii) Impractical to have links to every other page – the number of links could dominate the page and the page content could be obscured , adding a new page to the site could be extremely expensive from maintenance viewpoint as every page would have to be updated and similarly if a page were deleted.

c)

i)

- Site structure - A separate folder each type of file – img, avi,css, etc
- Web pages (HTML) organised by area

ii)



Page B2:
Global links – Home, Area A, Area B, Area C, Area D
Local Links: B1, B3, B2.1, B2.2, B2.3, B2.4

Navigation scheme is a hybrid of matrix and hierarchical with the appropriate use of global links. Breadcrumb trail would further enhance and simplify the user experience.

Examiners' Guidance Notes

In part a) candidates did not know what "characteristics" referred to, and instead simply namedropped navigation schemes (e.g. linear, hierarchical).

Part b) i) was answered well in some cases, but many simply drew a textbook navigation scheme, rather than drawing the actual scheme mentioned in the question. Also, links between pages were often not appropriately indicated (often not showing the direction of navigation with arrows, etc.).

Part b) ii) generally well answered, but some candidates simply restated the advantages of a linear scheme – this was not the question!

Part b) iii) was generally poorly answered and structured. Successful candidates would consider the site at 10 pages (which was generally accepted as being feasible), and then 15/20 and indicate the areas that do not scale up – this was the important aspect of the question, not simply when the site is doubled in size.

Part c) was extremely poorly answered, with candidates not understanding the distinction between the two subparts, and also not considering site structures and file management, but only navigation. Candidates did not think critically about their structures, instead sticking with plain hierarchical structures, and not considering the possibilities of more interesting navigation between the 4 website sections. Generic definitions were given for the terms "global links" and "breadcrumb navigation" rather than discussing their use. The stronger candidates gave a screen mockup indicating their use well – this was not explicitly asked, but was considered useful.

Question 5

(a) Expand each of the following terms and then define its **meaning**, in the context of the WWW:

(i) RSS **(1 mark)**

(ii) XML **(1 mark)**

(iii) AJAX **(1 mark)**

(iv) CSS **(1 mark)**

(v) TCP/IP **(1 mark)**

(b) (i) Define the term **blogging**. **(2 marks)**

(ii) State **three** possible uses for a blog. **(3 marks)**

(iii) Describe how a blog differs from a traditional website. **(5 marks)**

(c) Explain, with the aid of appropriate real-life examples, **four** risks in relying on information acquired from WWW sites and a way to mitigate each of these risks. **(10 marks)**

Answer Pointers

a)

(i) Really Simple Syndication (or equally, Rich Site Summary or RDF Site Summary) - a family of XML file formats for Web syndication.

(ii) Extensible Mark-up Language – a general mark-up language used to create special-purpose mark-up languages.

(iii) Asynchronous Java and XML – a technique used for creating interactive applications by performing tasks through the client side and transferring data to/from a server asynchronously.

(iv) Cascading Style Sheets - a stylesheet language used to describe the presentation of a mark-up document.

(v) Transmission Control Protocol/Internet Protocol – a set of two communications protocols which offer reliable delivery (c.f. UDP/IP) across diverse networks. IP defines the underlying network layer, whilst TCP is the transport layer, providing the reliable and sequenced delivery over IP.

b)

(i) A weblog or blog is a online journal – a web-based publication consisting primarily of periodic articles.

(ii) Photo album, Diary, Record keeping, Community forum, Live newsfeed (amongst others).

(iii) In contrast to a normal web site, blogs often:

- Are constructed using a content management system, which allows non-programmers to have a sophisticated, easily updated web site with no HTML skills.
- Follow common templates (so blog owners do not have to have design skills), into which content is fed.
- Allow the owner to add other authors, and easily manage permissions and access.
- Allow for adjusting the visibility of an article (public, private, friends only, etc.).
- Facilitate adding new pages through a webpage-based interface.
- Support other users commenting on articles, which can lead to discussion

- Allow easy filtering of content e.g. by date, category, author, etc.

c) Risks include:

Risk	Example
Doubts on accuracy of information	e.g. inaccurate sites on medical diagnostics
Doubts on currency of information	Sites not updated without a visible indication of its age.
Lack of authority and peer review	Certain Wikipedia pages
Lack of accountability	Certain Wikipedia pages
Ease of libel	E.g. Barrett vs Owen, 2001
Potential impersonation of other people/sites – website imitation	"Phishing" sites pretending to be e.g. eBay.
Potential bias or conflict of interests	Review of software by publisher from opposing camp

Ways to mitigate these risks include cross checking with other web sites, cross checking with peer reviewed or published works, authenticating sources and websites, looking for assurances of quality (e.g. sites owned and edited by well-respected experts).

Examiners' Guidance Notes

In part a) candidates defined the terms correctly (with the exception of AJAX which generated all kinds of interesting – and incorrect – definitions), but the description of the meaning of the terms was often less well answered.

Part b) was generally well answered, though there was a tendency to write verbatim answers from a previous examination, which did not score highly.

Part c) was poorly answered, with answer pointers from a previous examination quoted entirely verbatim and demonstrating little understanding of the risks – where the answer pointers indicate e.g. "certain Wikipedia pages", it is expected to detail why this is the case, or to give some actual examples of specific pages. There was also little connection between the risks identified and the ways to mitigate risks outlined. Finally, some candidates misinterpreted the question and began talking about security risks.