Compliance driven vulnerabilities

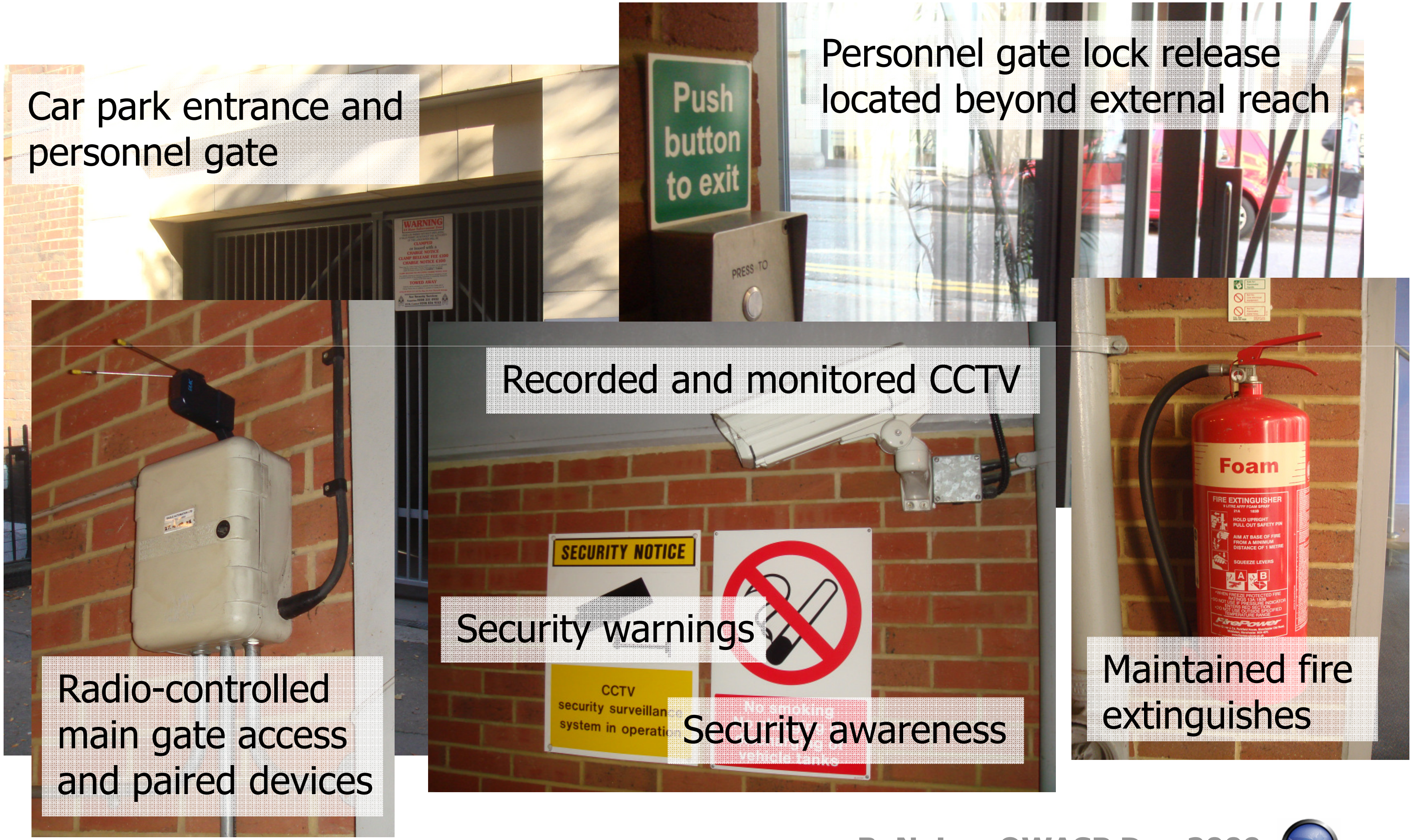
The effect of a quality aspect on software security

Colin Watson
Watson Hall Ltd
colin.watson(at)owasp.org

BeNeLux OWASP Day 2009

The OWASP Foundation
http://www.owasp.org

Conflicts: Building security/Human safety (1/2)



Car park entrance and personnel gate

Personnel gate lock release located beyond external reach

Recorded and monitored CCTV

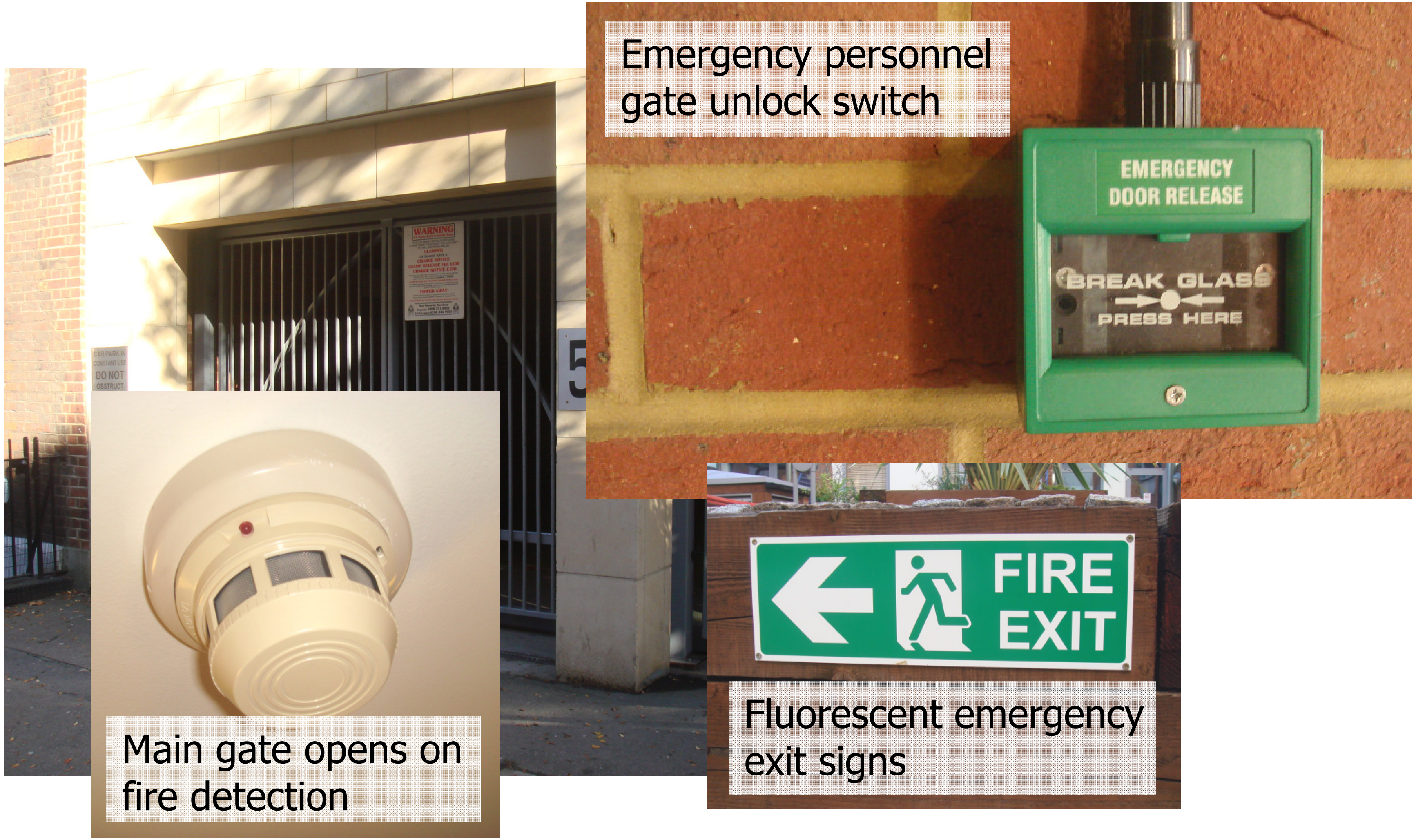
Security warnings

Radio-controlled main gate access and paired devices

Security awareness

Maintained fire extinguishes

Conflicts: Building security/Human safety (2/2)



Emergency personnel gate unlock switch

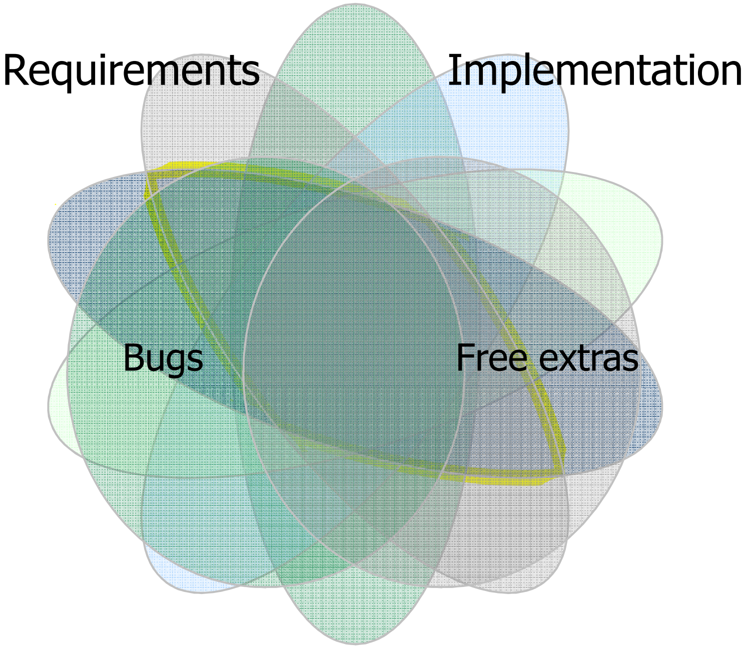
Main gate opens on fire detection

Fluorescent emergency exit signs

Software quality characteristics

- Functionality
  Suitability, Accuracy, Interoperability, Security, Compliance
- Reliability
  Maturity, Fault Tolerance, Recoverability
- Usability
  Understandability, Learnability, Operability
- Efficiency
  Time behaviour, resource utilisation
- Maintainability
  Analysability, Changeability, Stability, Testability
- Portability
  Adaptability, Installability, Co-existence, Replaceability, Conformance

Requirements and implementation



□ Implemented accessible features

▨ What the application actually does (implemented)

▨ Quality aspect B

▨ Quality aspect A

▨ What the development team thought they built

▨ What the client wants (requirements)

JA Whittaker and HH Thompson 2003[8]

Mandates

Military Firing Range.
Keep out when
red flags or lights
are displayed
or barriers closed.
Danger
Do not touch
any military debris.
It may explode
and kill you.

Compliance

- Compliance with all types of mandates:
  - Corporate

    Objectives, policies, contracts, agreements, initiatives
  - External standards

    Sectoral, national, international
  - Regulation

    Legislation, guidance, codes of practice
- In this presentation, **not** compliance with security mandates
- Compliance with mandates that can have security side-effects

Why does this matter?

- Design
  - Writing security specification
  - Identifying security implications early in the development lifecycle
  - Resolving conflicting demands
- Development
- Verification and testing
  - Black box
    - Assessment planning
    - Fault identification
  - White box
    - Understanding of critical areas

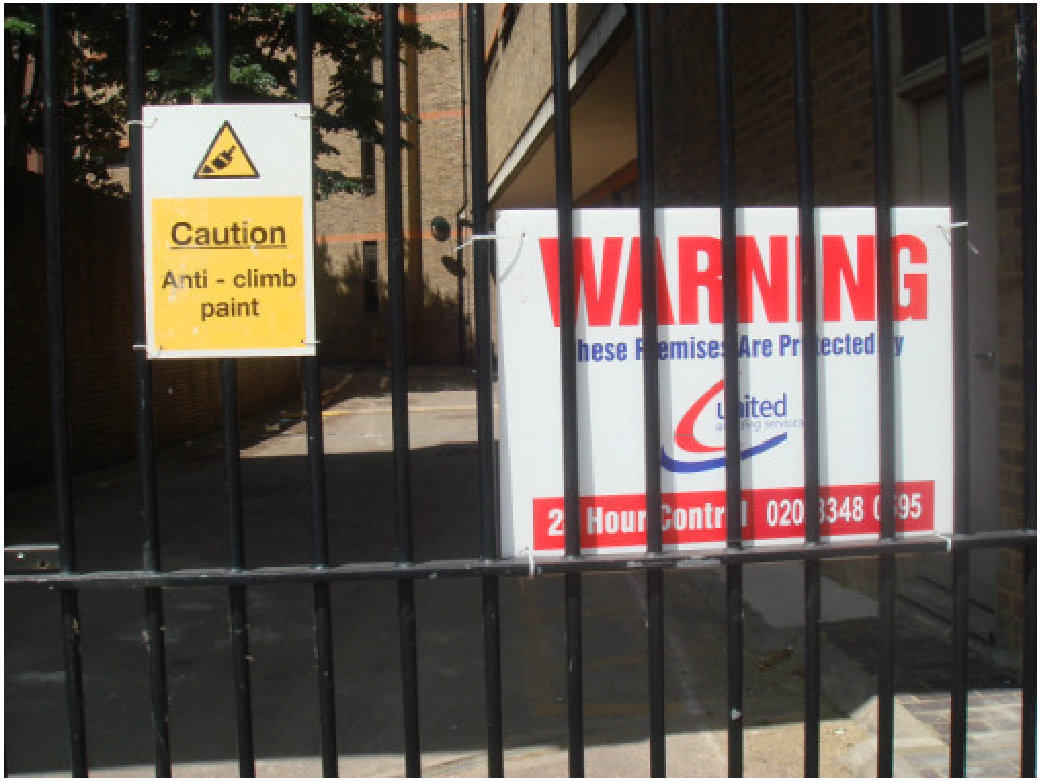
✗ Think like an attacker?

✓ **Think like a developer**

Webapp security / Accessibility compliance

- To illustrate how this might…. we will look at accessibility requirements, which are a common aspect in webapp requirements
- In particular WCAG
- Frameworks do not support it so coders have to make it up
- Even a fairly simple website, that decides to adopt the standard, starts getting into heavy programming

How accessible?



Usability and accessibility

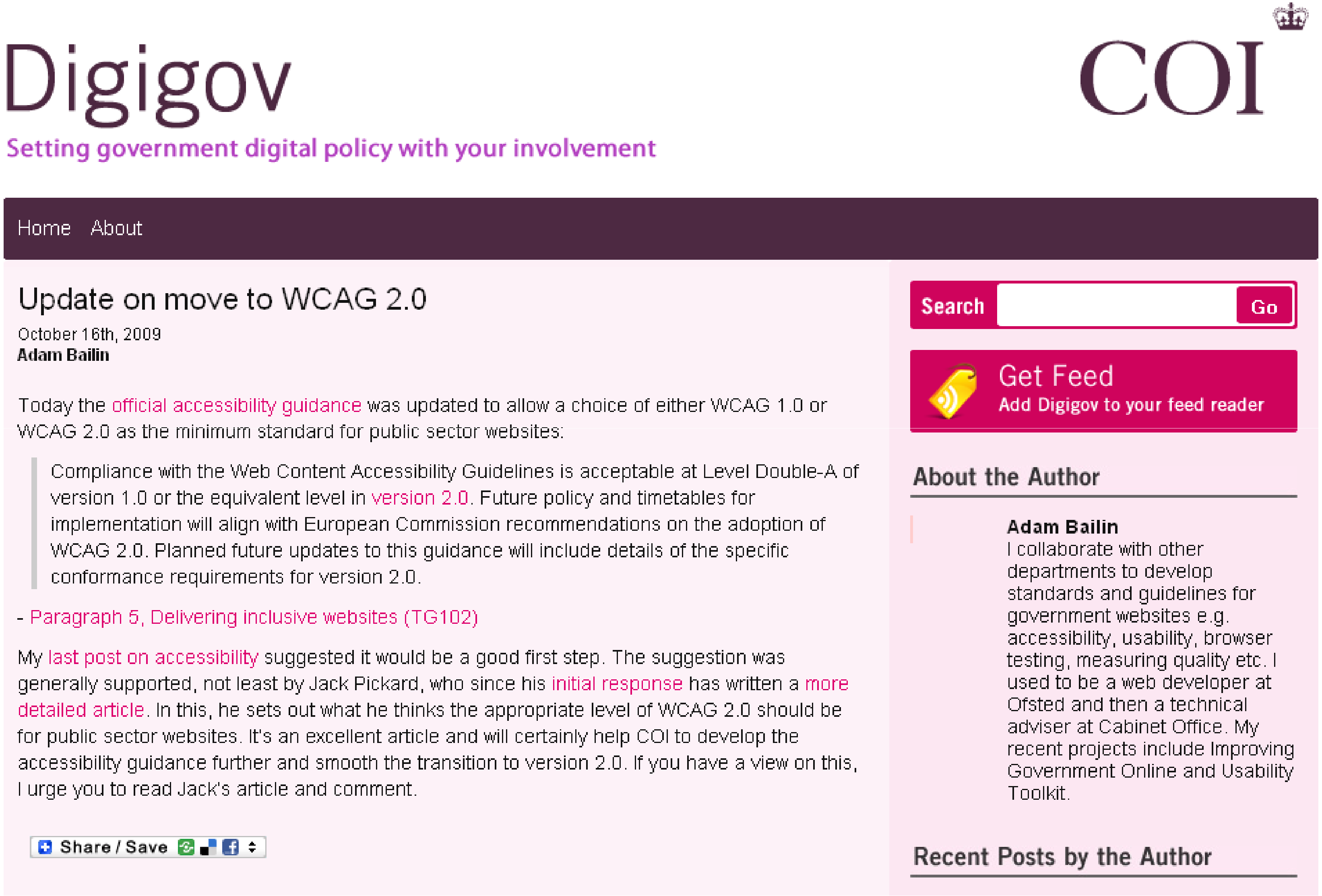
- Usability and accessibility have different though not incompatible design philosophies and goals[2,3,4,5]
- Accessibility is not just about disability
- W3C Web Content Accessibility Guidelines (WCAG)[6]
- Like security…"build accessibility in"[7]

Q: Why do they care?

A: (usability and accessibility)

- Business case
  - Increased audience reach
  - Higher conversion rate and repeat business
  - Lower support costs
  - Higher productivity
- Legal requirements[1]
- Side effects
  - Improved search engine optimisation
  - Greater ability to repurpose information

WCAG Sniffing: On the way (1/2)



Digigov

Setting government digital policy with your involvement

COI

Update on move to WCAG 2.0

October 16th, 2009
Adam Bailin

Today the official accessibility guidance was updated to allow a choice of either WCAG 1.0 or WCAG 2.0 as the minimum standard for public sector websites:

> Compliance with the Web Content Accessibility Guidelines is acceptable at Level Double-A of version 1.0 or the equivalent level in version 2.0. Future policy and timetables for implementation will align with European Commission recommendations on the adoption of WCAG 2.0. Planned future updates to this guidance will include details of the specific conformance requirements for version 2.0.

- Paragraph 5, Delivering inclusive websites (TG102)

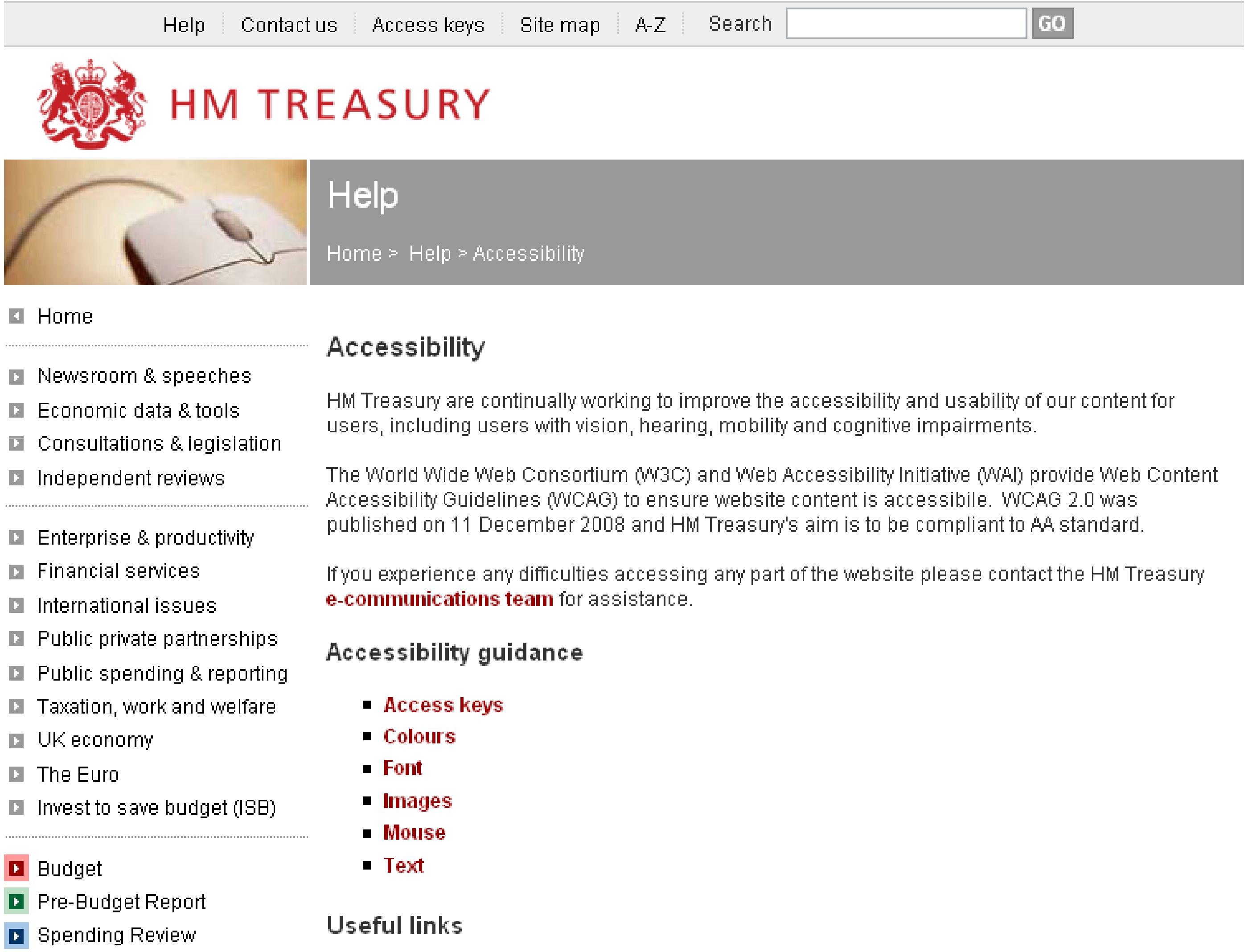
My last post on accessibility suggested it would be a good first step. The suggestion was generally supported, not least by Jack Pickard, who since his initial response has written a more detailed article. In this, he sets out what he thinks the appropriate level of WCAG 2.0 should be for public sector websites. It's an excellent article and will certainly help COI to develop the accessibility guidance further and smooth the transition to version 2.0. If you have a view on this, I urge you to read Jack's article and comment.

About the Author

Adam Bailin
I collaborate with other departments to develop standards and guidelines for government websites e.g. accessibility, usability, browser testing, measuring quality etc. I used to be a web developer at Ofsted and then a technical adviser at Cabinet Office. My recent projects include Improving Government Online and Usability Toolkit.

Recent Posts by the Author

WCAG Sniffing: On the way (2/2)


Help | Contact us | Access keys | Site map | A-Z | Search
GO
HM TREASURY
Help
Home > Help > Accessibility
Home
Newsroom & speeches
Economic data & tools
Consultations & legislation
Independent reviews
Enterprise & productivity
Financial services
International issues
Public private partnerships
Public spending & reporting
Taxation, work and welfare
UK economy
The Euro
Invest to save budget (ISB)
Budget
Pre-Budget Report
Spending Review

Accessibility

HM Treasury are continually working to improve the accessibility and usability of our content for users, including users with vision, hearing, mobility and cognitive impairments.

The World Wide Web Consortium (W3C) and Web Accessibility Initiative (WAI) provide Web Content Accessibility Guidelines (WCAG) to ensure website content is accessibile. WCAG 2.0 was published on 11 December 2008 and HM Treasury's aim is to be compliant to AA standard.

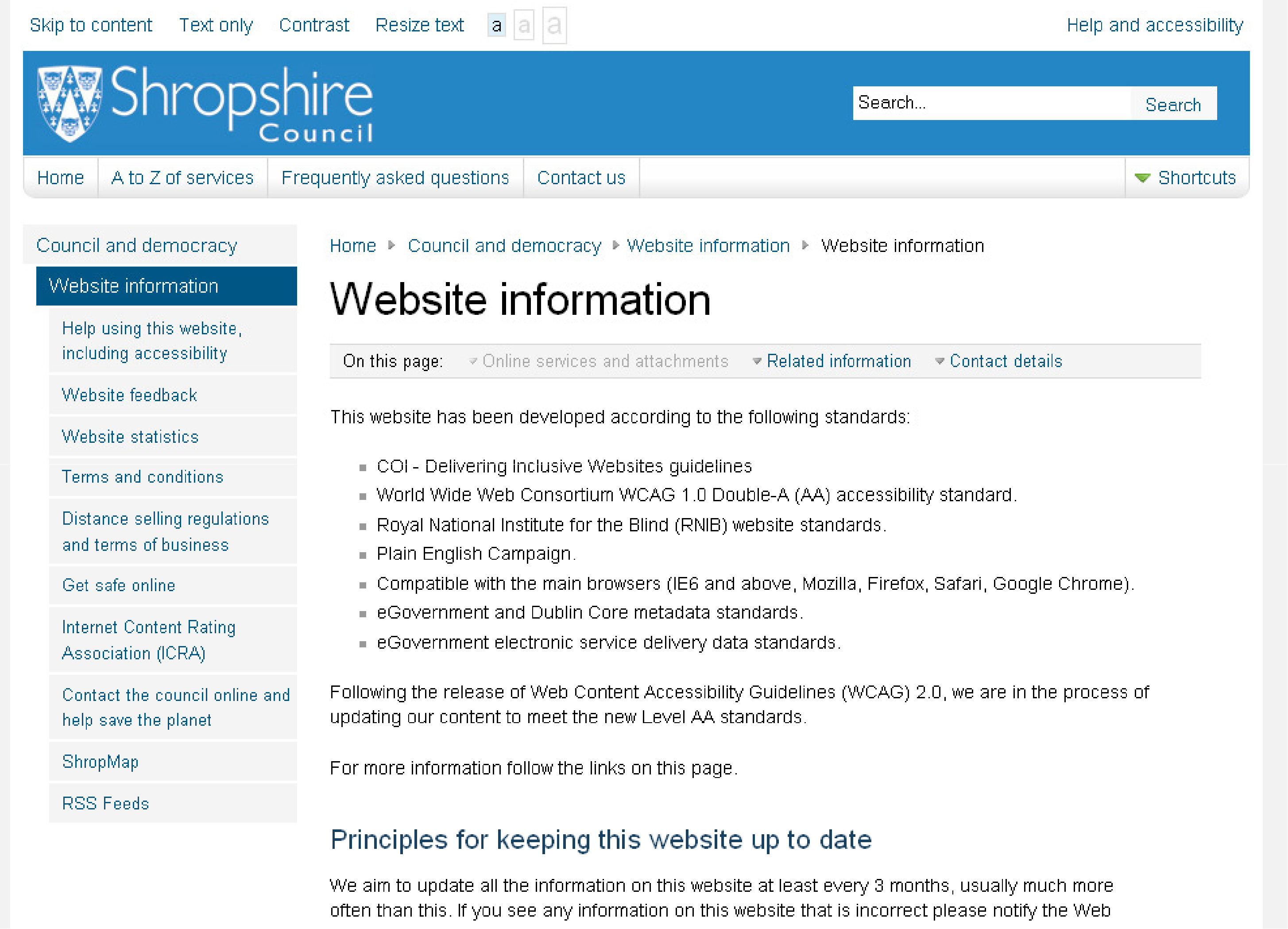
If you experience any difficulties accessing any part of the website please contact the HM Treasury e-communications team for assistance.

Accessibility guidance

- Access keys
- Colours
- Font
- Images
- Mouse
- Text

Useful links

WCAG Sniffing: Coming soon



Skip to content
Text only
Contrast
Resize text
a a a
Help and accessibility
Shropshire Council
Search...
Search
Home
A to Z of services
Frequently asked questions
Contact us
Shortcuts
Council and democracy
Website information
Help using this website, including accessibility
Website feedback
Website statistics
Terms and conditions
Distance selling regulations and terms of business
Get safe online
Internet Content Rating Association (ICRA)
Contact the council online and help save the planet
ShropMap
RSS Feeds
Home ▸ Council and democracy ▸ Website information ▸ Website information
On this page: Online services and attachments
Related information
Contact details

Website information

This website has been developed according to the following standards:

- COI - Delivering Inclusive Websites guidelines
- World Wide Web Consortium WCAG 1.0 Double-A (AA) accessibility standard.
- Royal National Institute for the Blind (RNIB) website standards.
- Plain English Campaign.
- Compatible with the main browsers (IE6 and above, Mozilla, Firefox, Safari, Google Chrome).
- eGovernment and Dublin Core metadata standards.
- eGovernment electronic service delivery data standards.

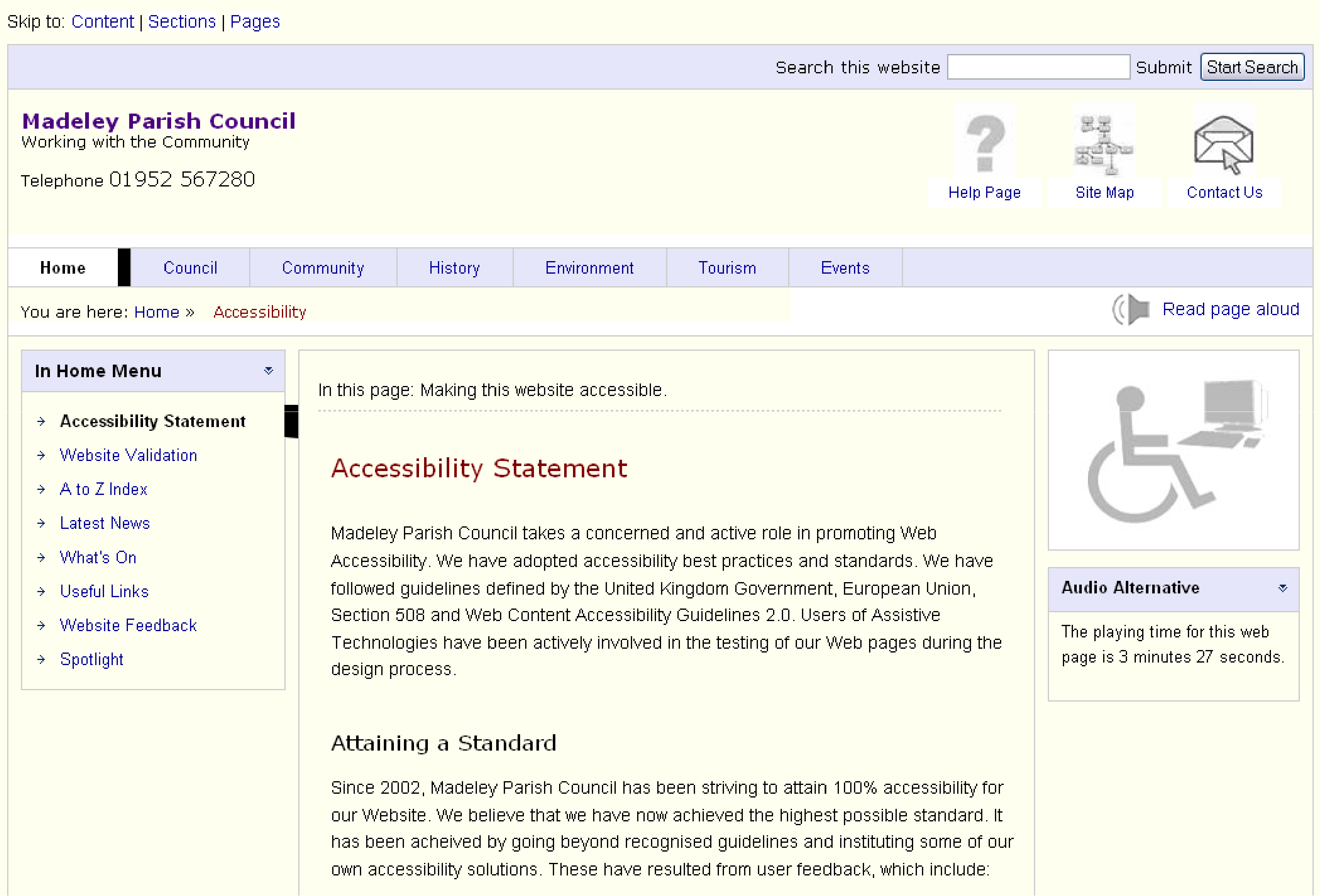
Following the release of Web Content Accessibility Guidelines (WCAG) 2.0, we are in the process of updating our content to meet the new Level AA standards.

For more information follow the links on this page.

Principles for keeping this website up to date

We aim to update all the information on this website at least every 3 months, usually much more often than this. If you see any information on this website that is incorrect please notify the Web

WCAG Sniffing: Been there, done it (1/2)



Skip to: Content | Sections | Pages

Search this website Submit Start Search

Madeley Parish Council
Working with the Community

Telephone 01952 567280

You are here: Home » Accessibility

In this page: Making this website accessible.

Accessibility Statement

Madeley Parish Council takes a concerned and active role in promoting Web Accessibility. We have adopted accessibility best practices and standards. We have followed guidelines defined by the United Kingdom Government, European Union, Section 508 and Web Content Accessibility Guidelines 2.0. Users of Assistive Technologies have been actively involved in the testing of our Web pages during the design process.

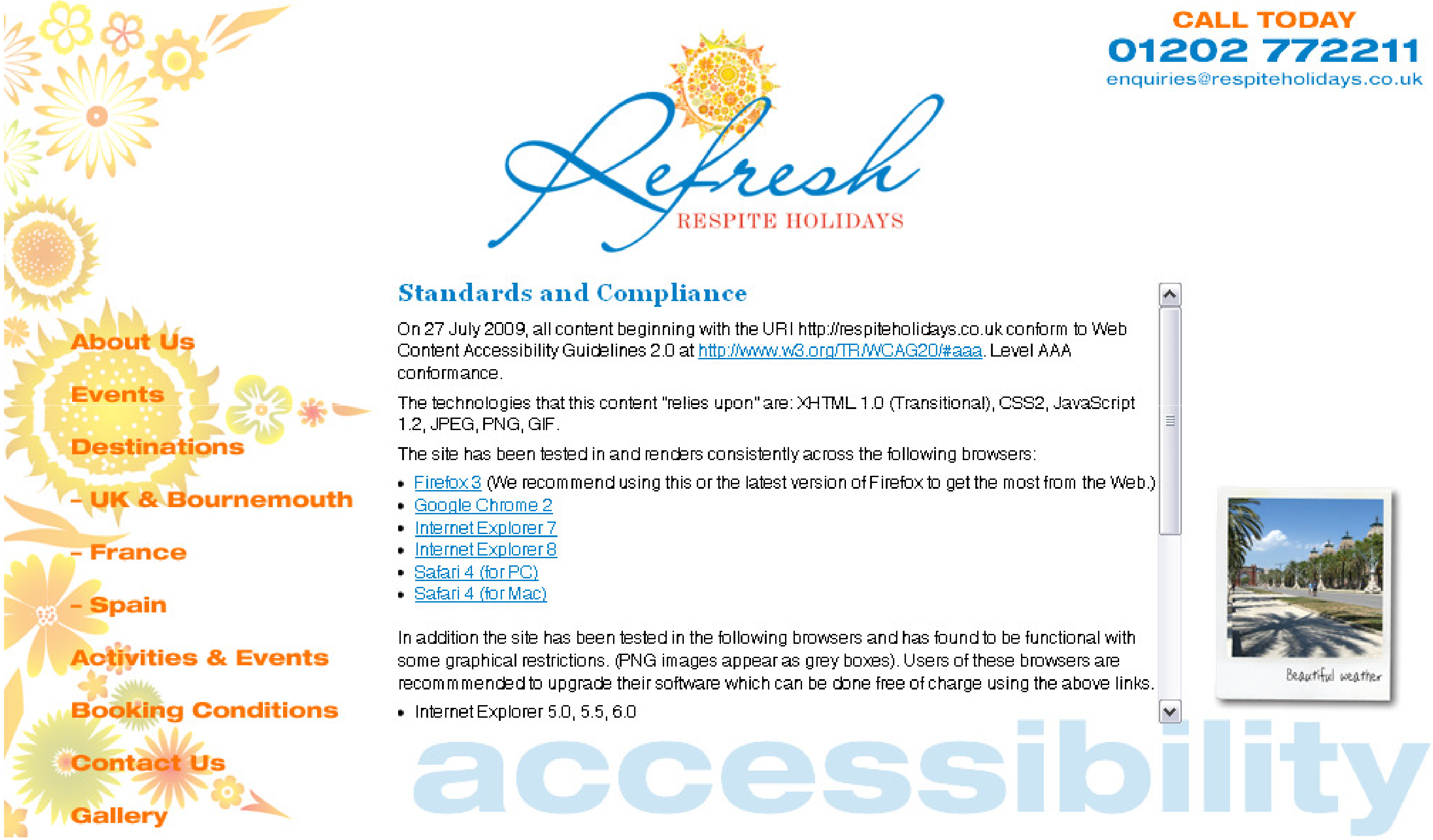
Attaining a Standard

Since 2002, Madeley Parish Council has been striving to attain 100% accessibility for our Website. We believe that we have now achieved the highest possible standard. It has been acheived by going beyond recognised guidelines and instituting some of our own accessibility solutions. These have resulted from user feedback, which include:

Audio Alternative

The playing time for this web page is 3 minutes 27 seconds.

WCAG Sniffing: Been there, done it (2/2)



Standards and Compliance

On 27 July 2009, all content beginning with the URI http://respiteholidays.co.uk conform to Web Content Accessibility Guidelines 2.0 at http://www.w3.org/TR/WCAG20/#aaa. Level AAA conformance.

The technologies that this content "relies upon" are: XHTML 1.0 (Transitional), CSS2, JavaScript 1.2, JPEG, PNG, GIF.

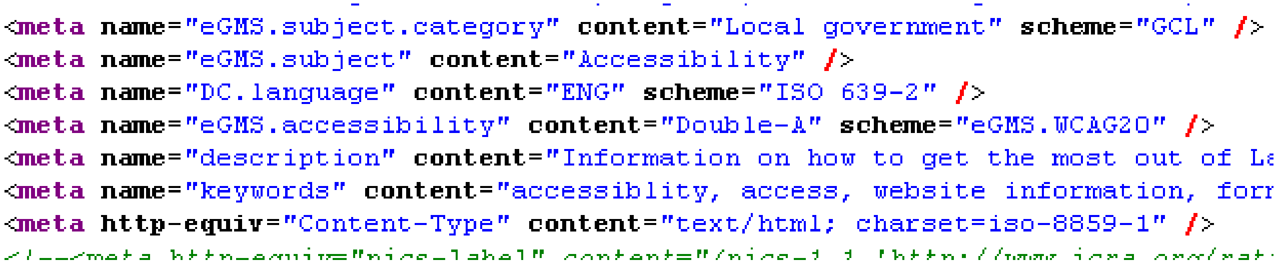
The site has been tested in and renders consistently across the following browsers:

- Firefox 3 (We recommend using this or the latest version of Firefox to get the most from the Web.)
- Google Chrome 2
- Internet Explorer 7
- Internet Explorer 8
- Safari 4 (for PC)
- Safari 4 (for Mac)

In addition the site has been tested in the following browsers and has found to be functional with some graphical restrictions. (PNG images appear as grey boxes). Users of these browsers are recommmended to upgrade their software which can be done free of charge using the above links.

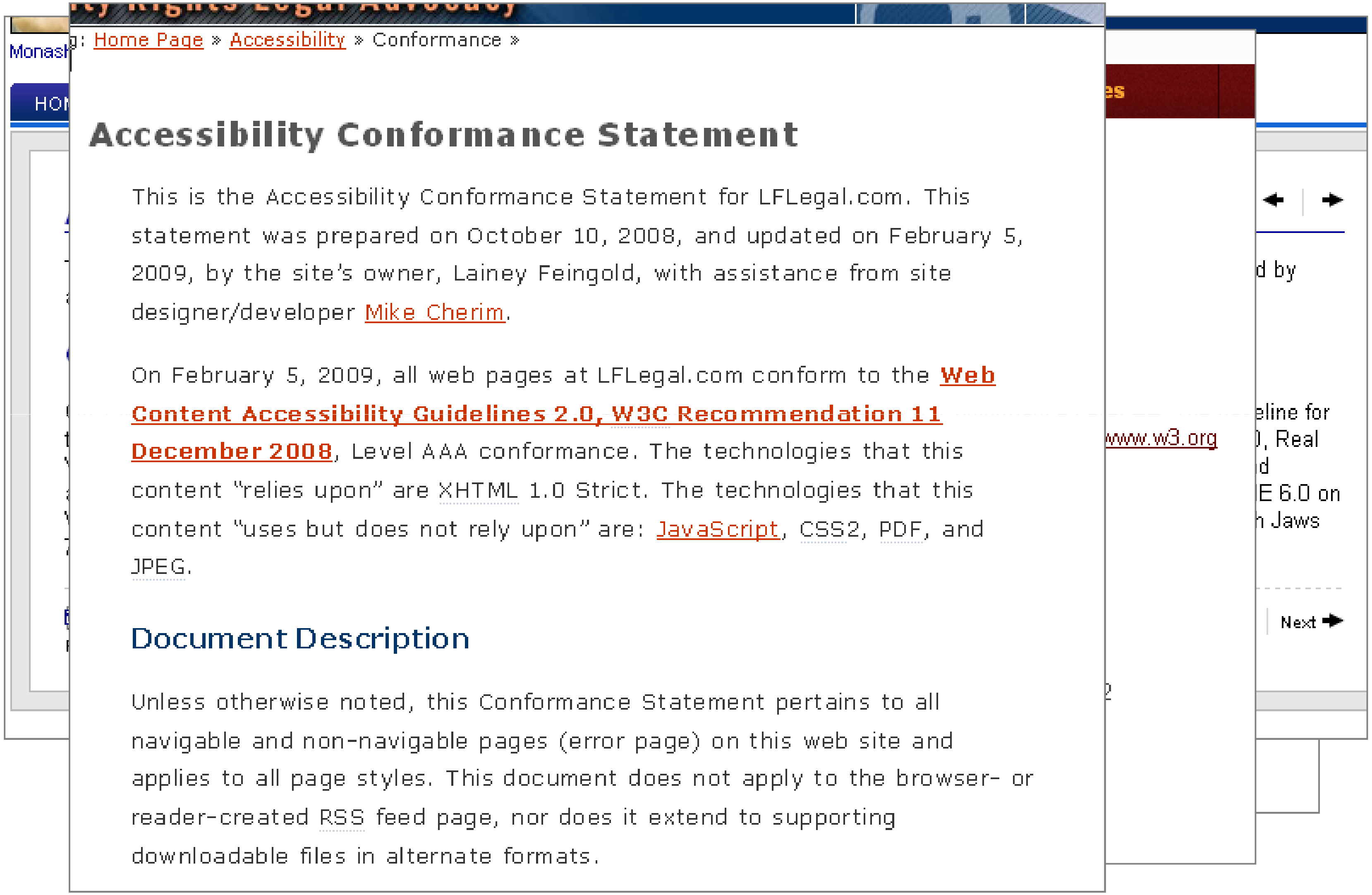
- Internet Explorer 5.0, 5.5, 6.0

WCAG Sniffing: In the meta data



```
<meta name="eGMS.subject.category" content="Local government" scheme="GCL" />
<meta name="eGMS.subject" content="Accessibility" />
<meta name="DC.language" content="ENG" scheme="ISO 639-2" />
<meta name="eGMS.accessibility" content="Double-A" scheme="eGMS.WCAG20" />
<meta name="description" content="Information on how to get the most out of La
<meta name="keywords" content="accessiblity, access, website information, forr
<meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1" />
<!--<meta http-equiv="pics-label" content="(pics-1.1 'http://www.icra.org/rat
```

WCAG Sniffing: Conformance claims



g: Home Page » Accessibility » Conformance »

Accessibility Conformance Statement

This is the Accessibility Conformance Statement for LFLegal.com. This statement was prepared on October 10, 2008, and updated on February 5, 2009, by the site's owner, Lainey Feingold, with assistance from site designer/developer Mike Cherim.

On February 5, 2009, all web pages at LFLegal.com conform to the **Web Content Accessibility Guidelines 2.0, W3C Recommendation 11 December 2008**, Level AAA conformance. The technologies that this content "relies upon" are XHTML 1.0 Strict. The technologies that this content "uses but does not rely upon" are: JavaScript, CSS2, PDF, and JPEG.

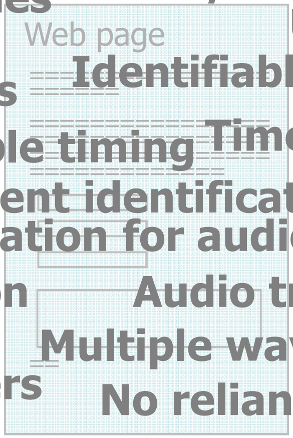
Document Description

Unless otherwise noted, this Conformance Statement pertains to all navigable and non-navigable pages (error page) on this web site and applies to all page styles. This document does not apply to the browser- or reader-created RSS feed page, nor does it extend to supporting downloadable files in alternate formats.

WCAG 2.0 principles, guidelines and success criteria

- 4 principles
  - Perceivable, operable, understandable and robust
- 12 guidelines
  - 4, 4, 3 and 1 guidelines for the principles respectively
- 61 success criteria
  - Mapped to 264 sufficient techniques
- 3 conformance claim levels
  - Level A, AA or AAA (strictest)

WCAG 2.0 impact on a typical web page



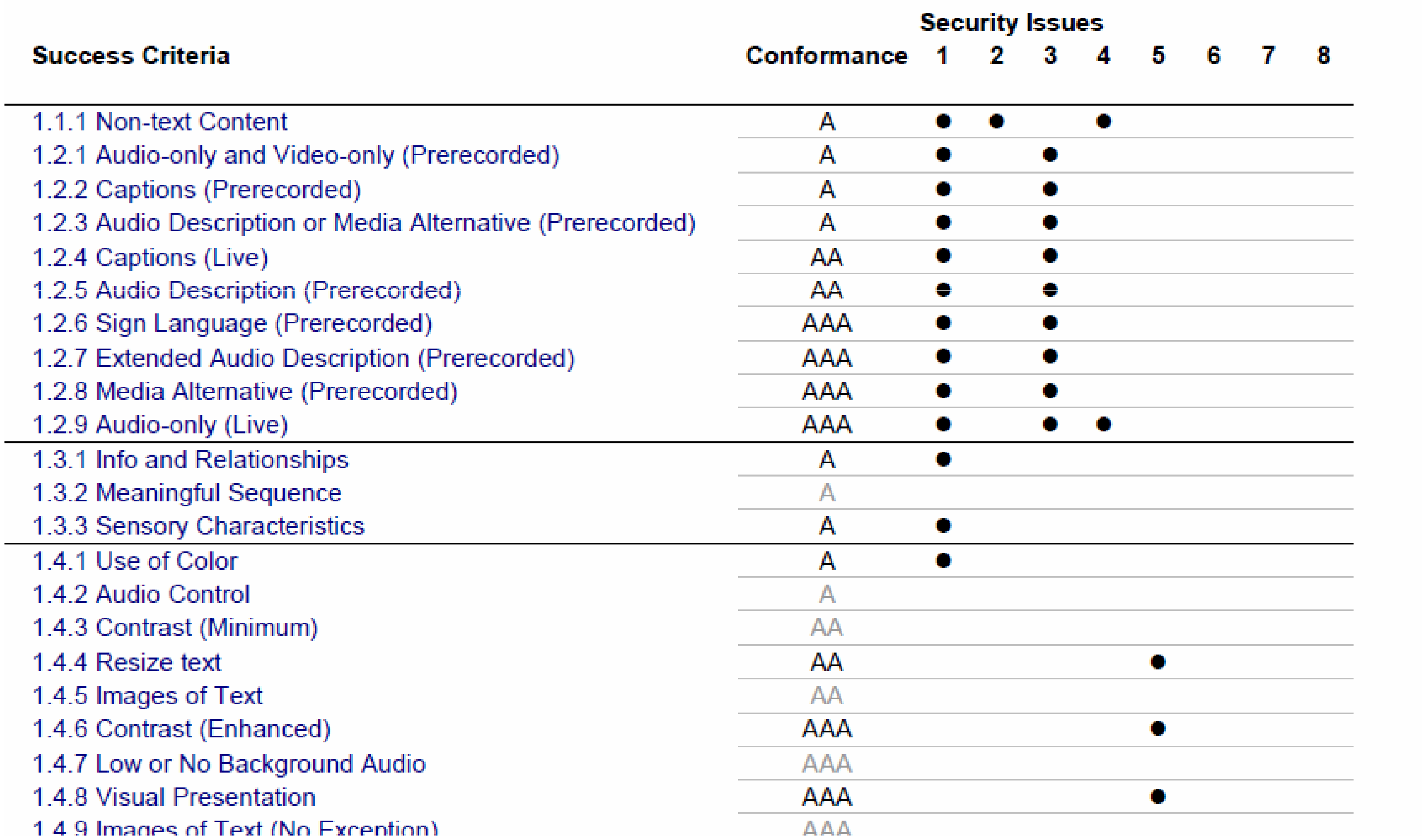
Input instructions
No keyboard trap
Postpone or suppress interruptions
Unusual word definitions
CAPTCHA text alternatives
Focus order
Minimum contrast
User error prevention
Page titles
Pause/stop/hide moving/blinking content
Purpose names
User error identification
HTML parsing
Focus visible
Identifiable structure and relationships
Labels
Text alternatives
Time-based media alternatives
Adjustable timing
Names, roles and values
Consistent identification
Link purpose
Resizable text
Sign language interpretation for audio
Headings
Visual presentation
Audio track for video-only content
Change context on request only
Multiple ways to locate
Abbreviations
Descriptive identifiers
No reliance on sensory characteristics
Flashing restrictions
Extended audio descriptions
Ability to pause or stop audio
Re-authenticate and continue
Pronunciation information
Reading level
Captions
Functionality via keyboard
Low or no background audio
Context sensitive help
Content bypass
No timing
Alternatives to live audio
User error prevention
Consistent navigation
Language identifiers
Identifiable reading sequence
Location in structure
Link purpose
On focus/input does not change context

Eight issues relating to application security

No	Issue	WCAG 2.0 Conformance Level	A	AA	AAA
1	Additional text instances		✓	✓	✓
2	Alternate forms of CAPTCHA		✓	✓	✓
3	Additional files		✓	✓	✓
4	Use of third-party services		✓	✓	✓
5	Additional client-side scripting		✓	✓	✓
6	Flexible session timeouts		✓	✓	✓
7	Re-authentication recovery				✓
8	Code validity		✓	✓	✓

Mappings (1/4)

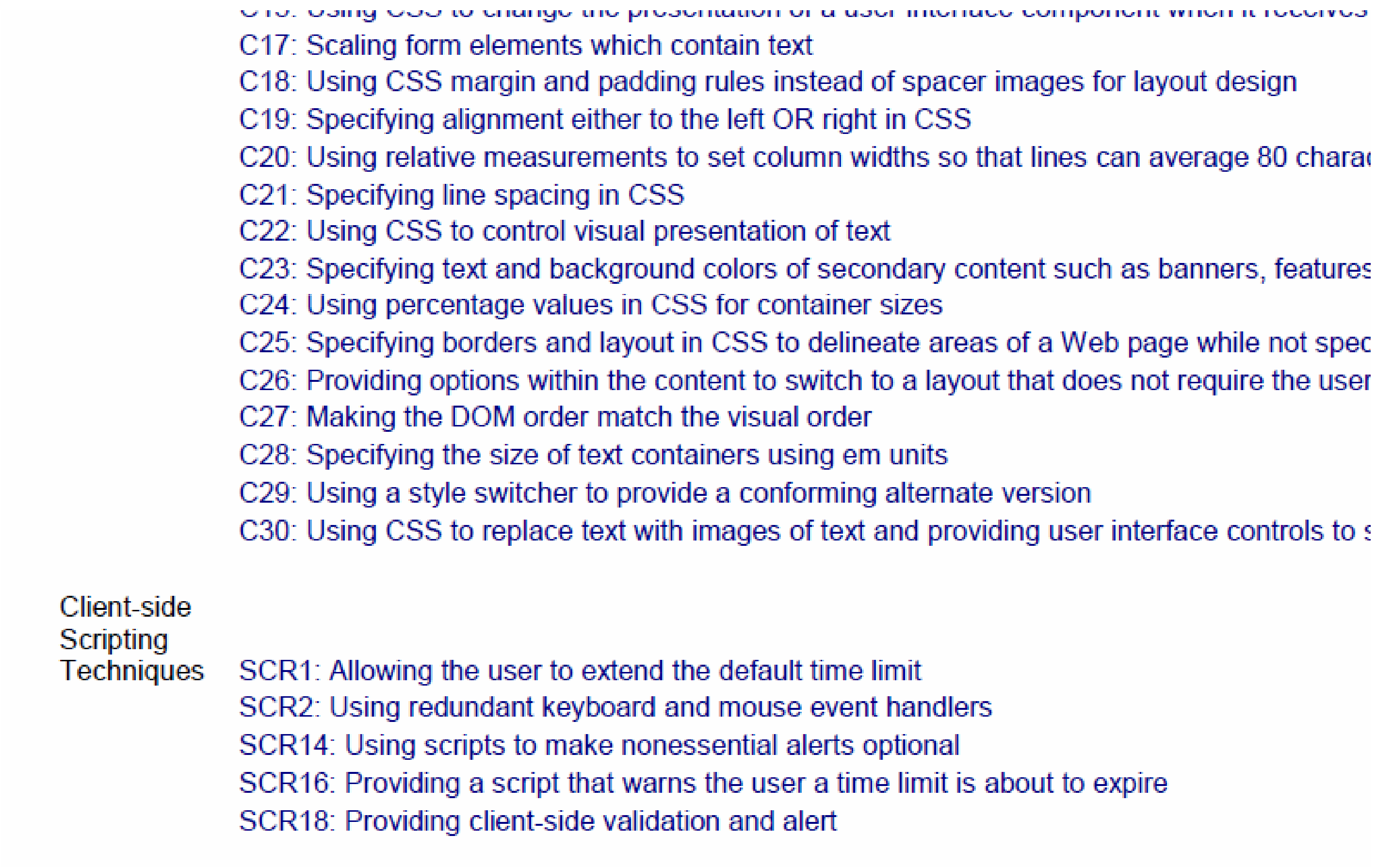
WCAG 2.0 Principles, Success Criteria and Conformance Levels to Security Issues



		Security Issues							
Success Criteria	Conformance	1	2	3	4	5	6	7	8
1.1.1 Non-text Content	A	●	●		●				
1.2.1 Audio-only and Video-only (Prerecorded)	A	●		●					
1.2.2 Captions (Prerecorded)	A	●		●					
1.2.3 Audio Description or Media Alternative (Prerecorded)	A	●		●					
1.2.4 Captions (Live)	AA	●		●					
1.2.5 Audio Description (Prerecorded)	AA	●		●					
1.2.6 Sign Language (Prerecorded)	AAA	●		●					
1.2.7 Extended Audio Description (Prerecorded)	AAA	●		●					
1.2.8 Media Alternative (Prerecorded)	AAA	●		●					
1.2.9 Audio-only (Live)	AAA	●		●	●				
1.3.1 Info and Relationships	A	●							
1.3.2 Meaningful Sequence	A								
1.3.3 Sensory Characteristics	A	●							
1.4.1 Use of Color	A	●							
1.4.2 Audio Control	A								
1.4.3 Contrast (Minimum)	AA								
1.4.4 Resize text	AA					●			
1.4.5 Images of Text	AA								
1.4.6 Contrast (Enhanced)	AAA					●			
1.4.7 Low or No Background Audio	AAA								
1.4.8 Visual Presentation	AAA					●			
1.4.9 Images of Text (No Exception)	AAA								

Mappings (1/4)

WCAG 2.0 Sufficient Techniques to Security Issues



	C15: Using CSS to change the presentation of a user interface component when it receives
	C17: Scaling form elements which contain text
	C18: Using CSS margin and padding rules instead of spacer images for layout design
	C19: Specifying alignment either to the left OR right in CSS
	C20: Using relative measurements to set column widths so that lines can average 80 charac
	C21: Specifying line spacing in CSS
	C22: Using CSS to control visual presentation of text
	C23: Specifying text and background colors of secondary content such as banners, features
	C24: Using percentage values in CSS for container sizes
	C25: Specifying borders and layout in CSS to delineate areas of a Web page while not spec
	C26: Providing options within the content to switch to a layout that does not require the user
	C27: Making the DOM order match the visual order
	C28: Specifying the size of text containers using em units
	C29: Using a style switcher to provide a conforming alternate version
	C30: Using CSS to replace text with images of text and providing user interface controls to s
Client-side Scripting Techniques	SCR1: Allowing the user to extend the default time limit
	SCR2: Using redundant keyboard and mouse event handlers
	SCR14: Using scripts to make nonessential alerts optional
	SCR16: Providing a script that warns the user a time limit is about to expire
	SCR18: Providing client-side validation and alert

OWASP Top Ten 2010 rc1[9] (3/4)

No	Issue	A	1	2	3	4	5	6	7	8	9	10
1	Additional text instances		●	●								
2	Alternate forms of CAPTCHA				●							
3	Additional files		●		●	●						
4	Use of third-party services			●			●		●			
5	Additional client-side scripting		●	●								
6	Flexible session timeouts				●				●	●		
7	Re-authentication recovery				●				●	●	●	
8	Code validity			●		●						

OWASP ASVS 2008[10] (4/4)

No	Issue	V	1	2	3	4	5	6	7	8	9	10	11	12	13	14
1	Additional text instances										●					
2	Alternate forms of CAPTCHA					●										
3	Additional files					●					●					
4	Use of third-party services					●	●	●			●		●		●	
5	Additional client-side scripting						●	●			●					
6	Flexible session timeouts					●										
7	Re-authentication recovery				●	●	●	●			●					
8	Code validity						●	●								

Issue 2: Alternate forms of CAPTCHA

Issue 2: Alternate forms of CAPTCHA

- 1.1.1 Non-text Content: All non-text content that is presented to the user has a text alternative that serves the equivalent purpose, except for the situations listed below. (Level A)
  - …
  - CAPTCHA: If the purpose of non-text content is to confirm that content is being accessed by a person rather than a computer, then text alternatives that identify and describe the purpose of the non-text content are provided, and alternative forms of CAPTCHA using output modes for different types of sensory perception are provided to accommodate different disabilities.
  - …
- Sufficient Techniques for 1.1.1 - Non-text Content
  - …
  - Situation E: If non-text content is a CAPTCHA:
    - G143: Providing a text alternative that describes the purpose of the CAPTCHA AND G144: Ensuring that the Web Page contains another CAPTCHA serving the same purpose using a different modality
  - …

Issue 6: Flexible session timeouts

Issue 6: Flexible session timeouts (1/3)

- SC 2.2.1 Timing Adjustable: For each time limit that is set by the content, at least one of the following is true: (Level A)
  - Turn off: The user is allowed to turn off the time limit before encountering it; or
  - Adjust: The user is allowed to adjust the time limit before encountering it over a wide range that is at least ten times the length of the default setting; or
  - Extend: The user is warned before time expires and given at least 20 seconds to extend the time limit with a simple action (for example, "press the space bar"), and the user is allowed to extend the time limit at least ten times; or
  - Real-time Exception: The time limit is a required part of a real-time event (for example, an auction), and no alternative to the time limit is possible; or
  - Essential Exception: The time limit is essential and extending it would invalidate the activity; or
  - 20 Hour Exception: The time limit is longer than 20 hours.

Issue 6: Flexible session timeouts (2/3)

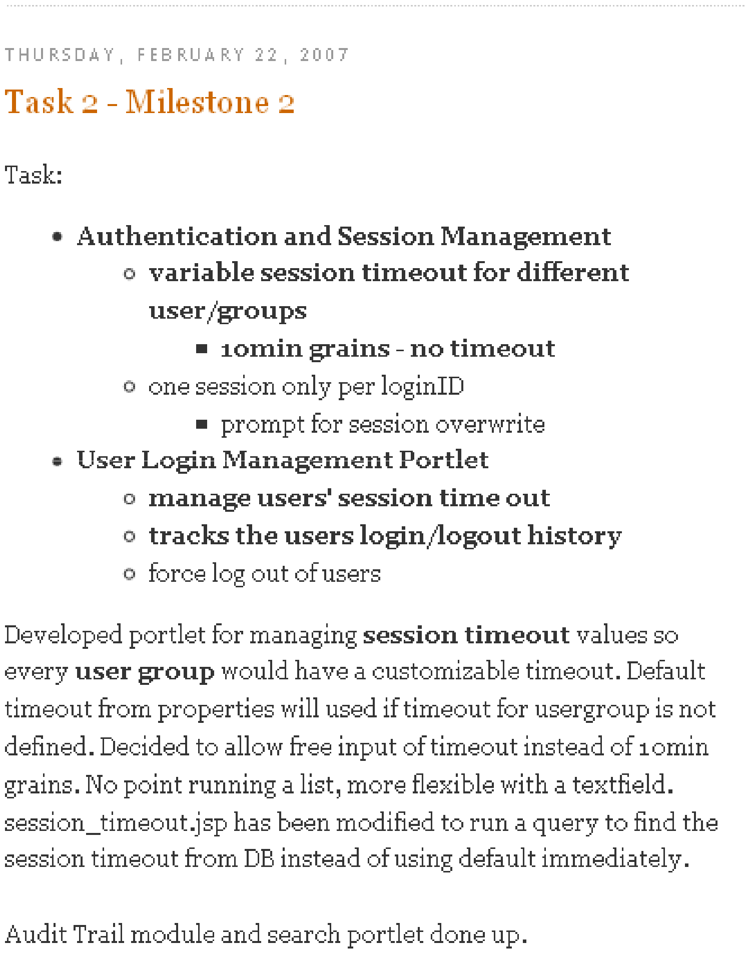
- Sufficient Techniques for 2.2.1 - Timing Adjustable
  - Situation A: If there are session time limits:
    - G133: Providing a checkbox on the first page of a multipart form that allows users to ask for longer session time limit or no session time limit
    - G198: Providing a way for the user to turn the time limit off
  - Situation B: If a time limit is controlled by a script on the page:
    - G198: Providing a way for the user to turn the time limit off
    - G180: Providing the user with a means to set the time limit to 10 times the default time limit
    - SCR16: Providing a script that warns the user a time limit is about to expire (Scripting) AND SCR1: Allowing the user to extend the default time limit (Scripting)
  - Situation C: If there are time limits on reading:
    - G4: Allowing the content to be paused and restarted from where it was paused
    - G198: Providing a way for the user to turn the time limit off
    - SCR33: Using script to scroll content, and providing a mechanism to pause it (Scripting)
    - SCR36: Providing a mechanism to allow users to display moving, scrolling, or auto-updating text in a static window or area (Scripting)

Issue 6: Flexible session timeouts (3/3)

- SC 2.2.3 No Timing: Timing is not an essential part of the event or activity presented by the content, except for non-interactive synchronized media and real-time events. (Level AAA)

- Sufficient Techniques for 2.2.3 - No Timing
  - G5: Allowing users to complete an activity without any time limit

WCAG Sniffing: Functionality defined (1/5)



THURSDAY, FEBRUARY 22, 2007

Task 2 - Milestone 2

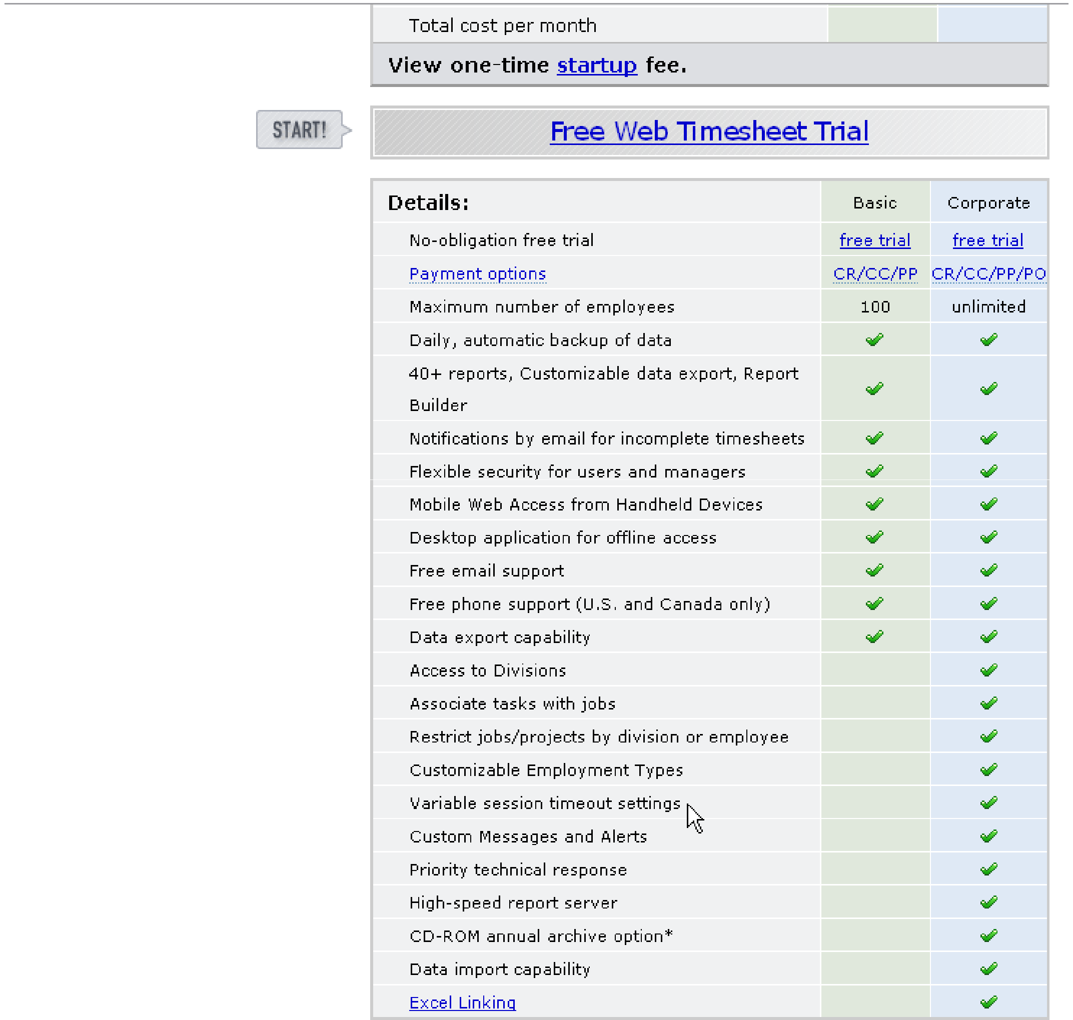
Task:

- **Authentication and Session Management**
  - **variable session timeout for different user/groups**
    - **10min grains - no timeout**
  - one session only per loginID
    - prompt for session overwrite
- **User Login Management Portlet**
  - **manage users' session time out**
  - **tracks the users login/logout history**
  - force log out of users

Developed portlet for managing **session timeout** values so every **user group** would have a customizable timeout. Default timeout from properties will used if timeout for usergroup is not defined. Decided to allow free input of timeout instead of 10min grains. No point running a list, more flexible with a textfield. session_timeout.jsp has been modified to run a query to find the session timeout from DB instead of using default immediately.

Audit Trail module and search portlet done up.

WCAG Sniffing: Functionality defined (2/5)



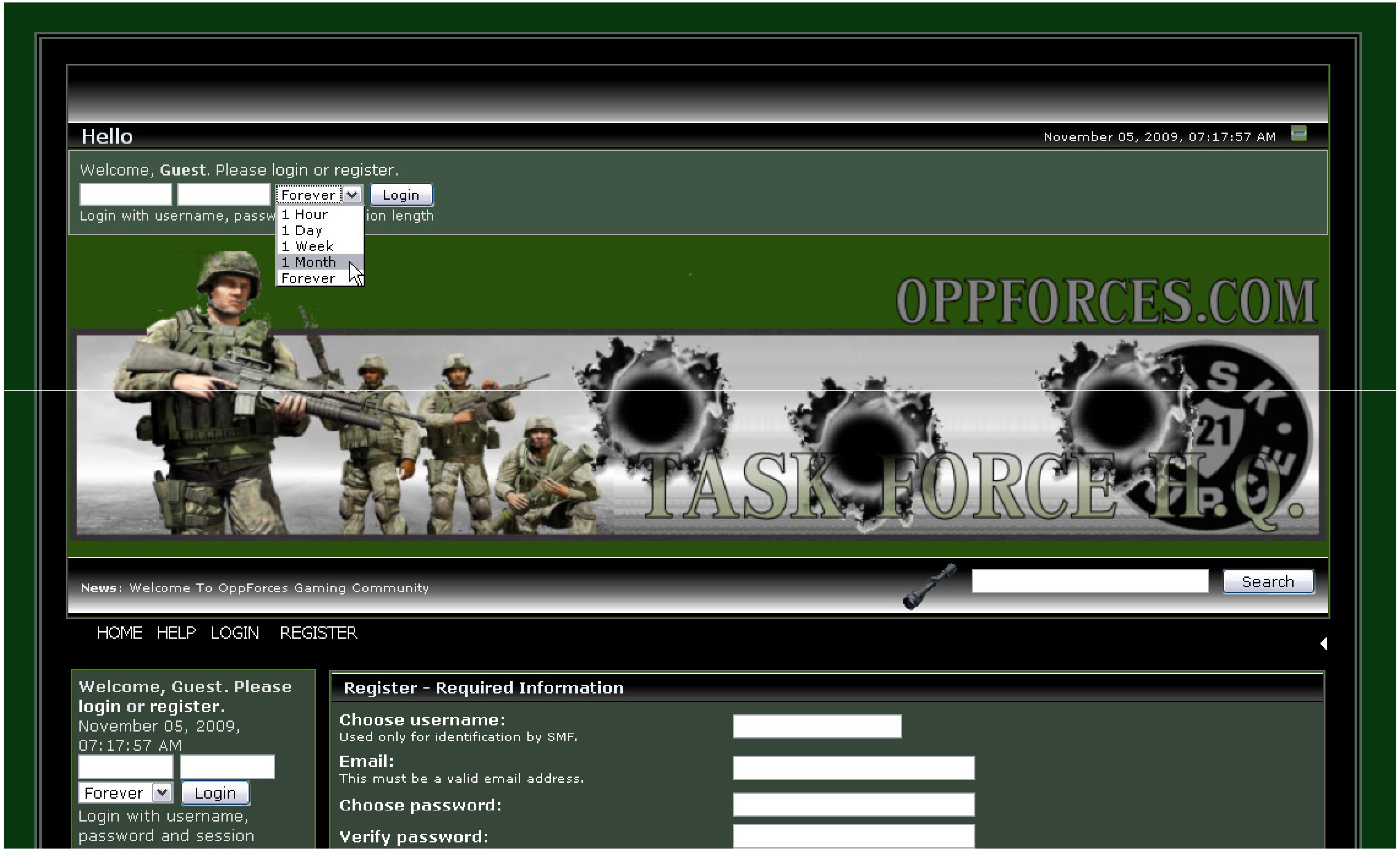
Total cost per month		

View one-time startup fee.

Free Web Timesheet Trial

Details:	Basic	Corporate
No-obligation free trial	free trial	free trial
Payment options	CR/CC/PP	CR/CC/PP/PO
Maximum number of employees	100	unlimited
Daily, automatic backup of data	✓	✓
40+ reports, Customizable data export, Report Builder	✓	✓
Notifications by email for incomplete timesheets	✓	✓
Flexible security for users and managers	✓	✓
Mobile Web Access from Handheld Devices	✓	✓
Desktop application for offline access	✓	✓
Free email support	✓	✓
Free phone support (U.S. and Canada only)	✓	✓
Data export capability	✓	✓
Access to Divisions		✓
Associate tasks with jobs		✓
Restrict jobs/projects by division or employee		✓
Customizable Employment Types		✓
Variable session timeout settings		✓
Custom Messages and Alerts		✓
Priority technical response		✓
High-speed report server		✓
CD-ROM annual archive option*		✓
Data import capability		✓
Excel Linking		✓

WCAG Sniffing: Functionality defined (3/5)



Hello

November 05, 2009, 07:17:57 AM

Welcome, **Guest**. Please login or register.

Login with username, passw ion length

News: Welcome To OppForces Gaming Community

Welcome, Guest. Please login or register.
November 05, 2009, 07:17:57 AM

Login with username, password and session

Register - Required Information

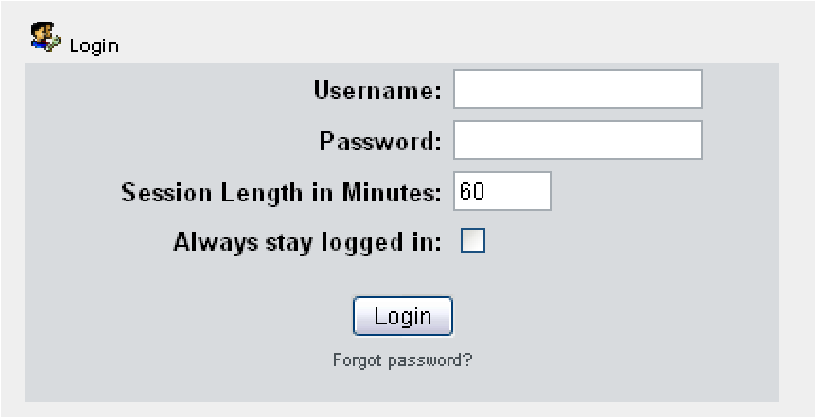
Choose username:
Used only for identification by SMF.

Email:
This must be a valid email address.

Choose password:

Verify password:

WCAG Sniffing: Functionality defined (4/5)

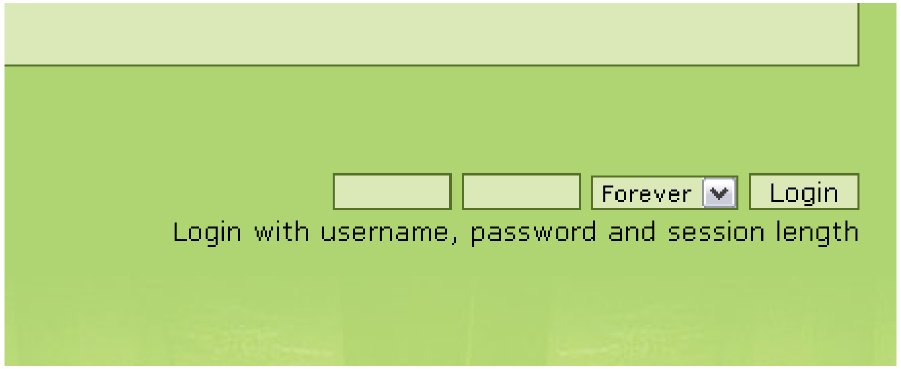


Username:

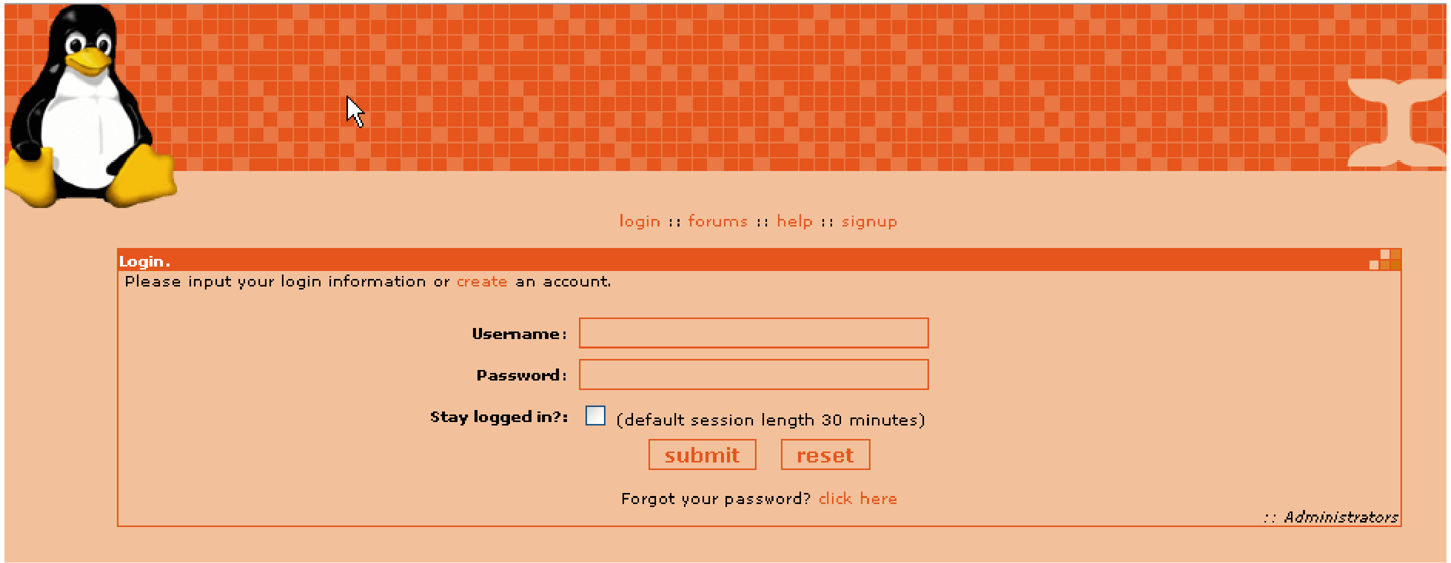
Password:

Session Length in Minutes: 60

Always stay logged in: □


Forever

Login with username, password and session length



Login.

Please input your login information or create an account.

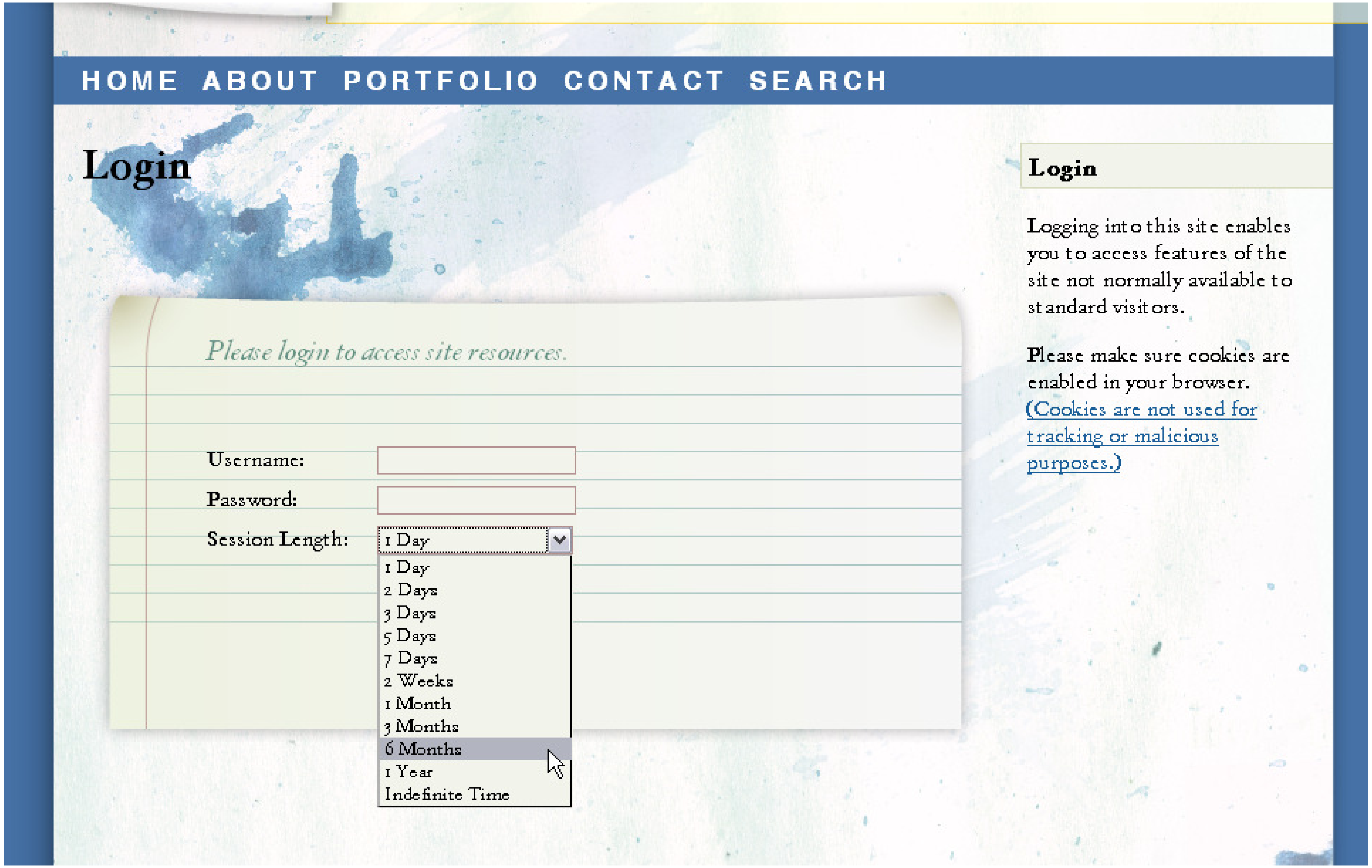
Username:

Password:

Stay logged in?: □ (default session length 30 minutes)

Forgot your password? click here

WCAG Sniffing: Functionality defined (5/5)



Login

Please login to access site resources.

Username:

Password:

Session Length: 1 Day

- 1 Day
- 2 Days
- 3 Days
- 5 Days
- 7 Days
- 2 Weeks
- 1 Month
- 3 Months
- 6 Months
- 1 Year
- Indefinite Time

Login

Logging into this site enables you to access features of the site not normally available to standard visitors.

Please make sure cookies are enabled in your browser. (Cookies are not used for tracking or malicious purposes.)

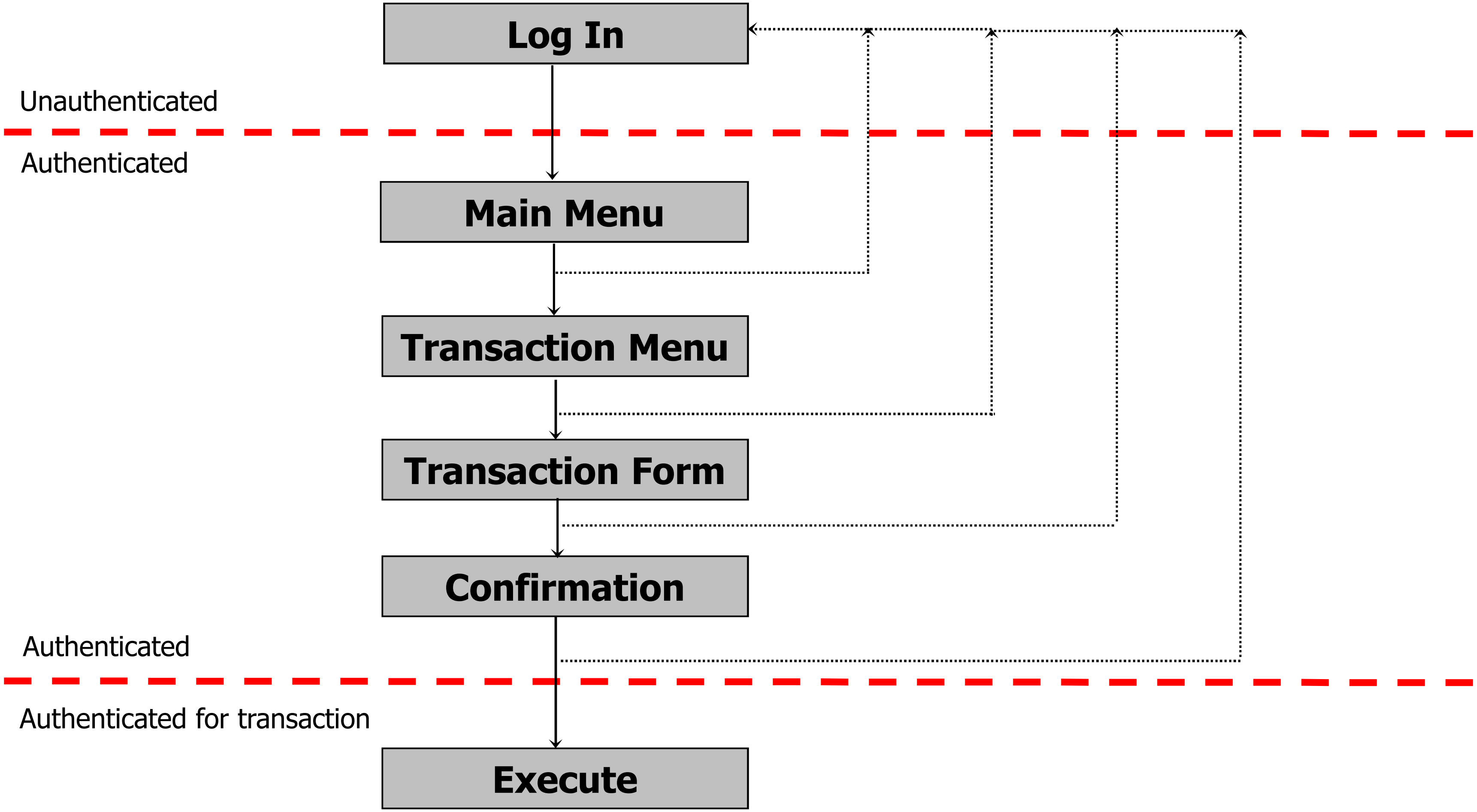
Issue 7: Re-authentication recovery

Issue 7: Re-authentication recovery

- SC 2.2.5 Re-authenticating: When an authenticated session expires, the user can continue the activity without loss of data after re-authenticating. (Level AAA)

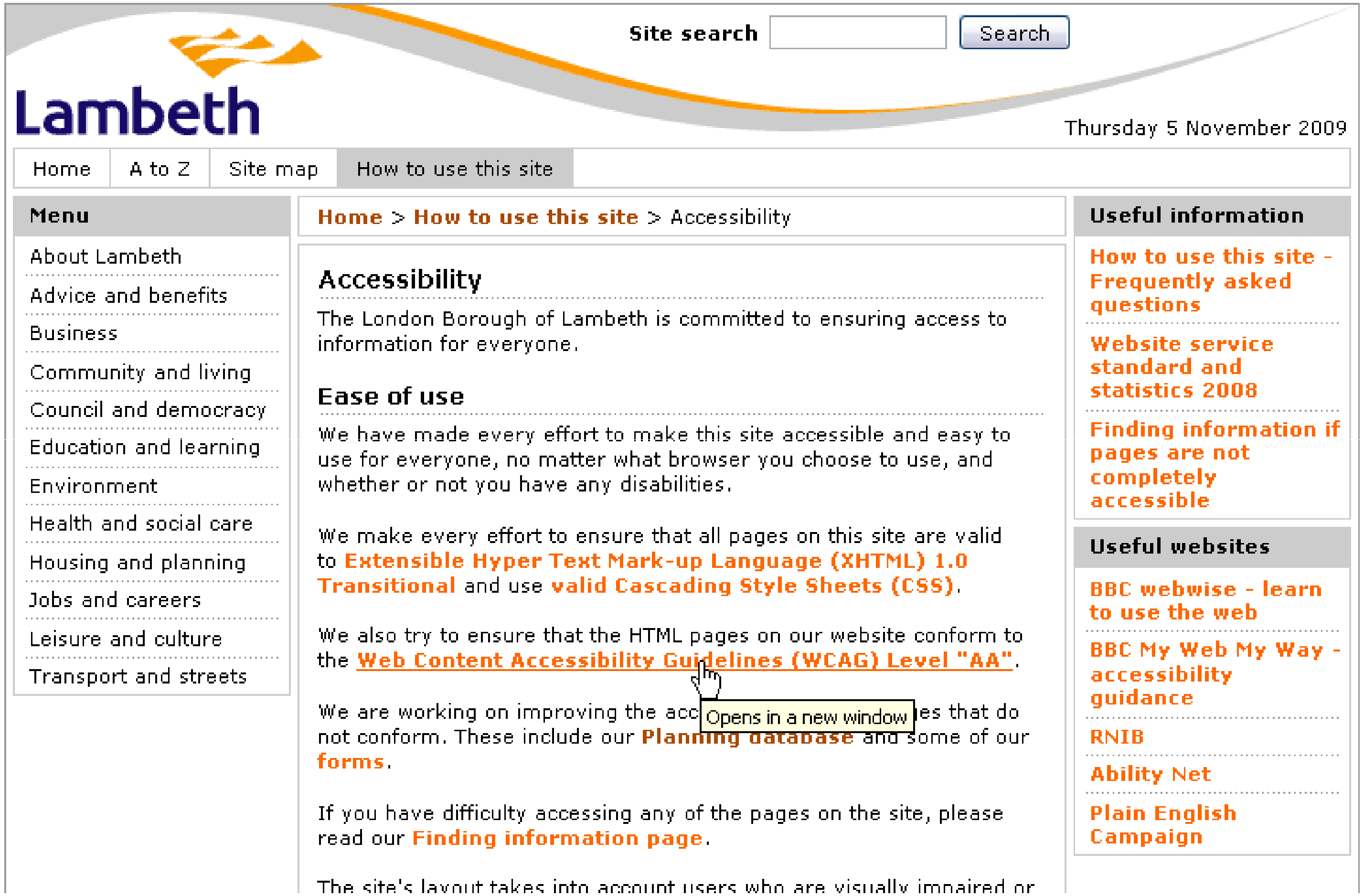
- Sufficient Techniques for 2.2.5 - Re-authenticating
  - Providing options to continue without loss of data using one of the following techniques:
    - G105: Saving data so that it can be used after a user re-authenticates
    - G181: Encoding user data as hidden or encrypted data in a re-authorization page

Re-authentication recovery transition graph*



*The Bank in the Browser - Defending Web Infrastructures from Banking Malware, Giorgio Fedon, AppSec EU 2009

WCAG Sniffing: Hopefully there... (1/3)



Home > How to use this site > Accessibility

Accessibility

The London Borough of Lambeth is committed to ensuring access to information for everyone.

Ease of use

We have made every effort to make this site accessible and easy to use for everyone, no matter what browser you choose to use, and whether or not you have any disabilities.

We make every effort to ensure that all pages on this site are valid to Extensible Hyper Text Mark-up Language (XHTML) 1.0 Transitional and use valid Cascading Style Sheets (CSS).

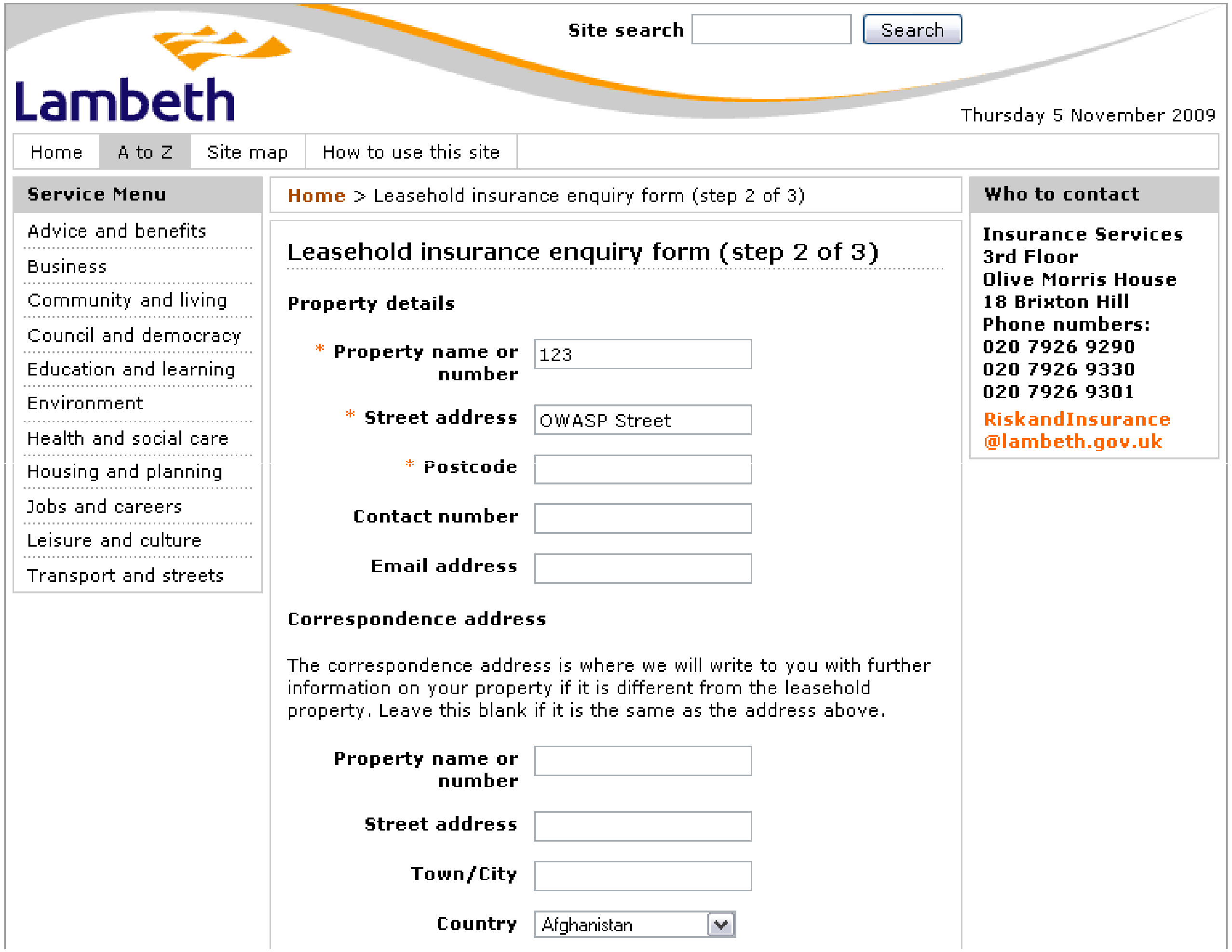
We also try to ensure that the HTML pages on our website conform to the Web Content Accessibility Guidelines (WCAG) Level "AA".

We are working on improving the acc[...]es that do not conform. These include our Planning database and some of our forms.

If you have difficulty accessing any of the pages on the site, please read our Finding information page.

The site's layout takes into account users who are visually impaired or

WCAG Sniffing: Hopefully there... (2/3)



Home > Leasehold insurance enquiry form (step 2 of 3)

Leasehold insurance enquiry form (step 2 of 3)

Property details

* **Property name or number**	123
* **Street address**	OWASP Street
* **Postcode**	
Contact number	
Email address	

Correspondence address

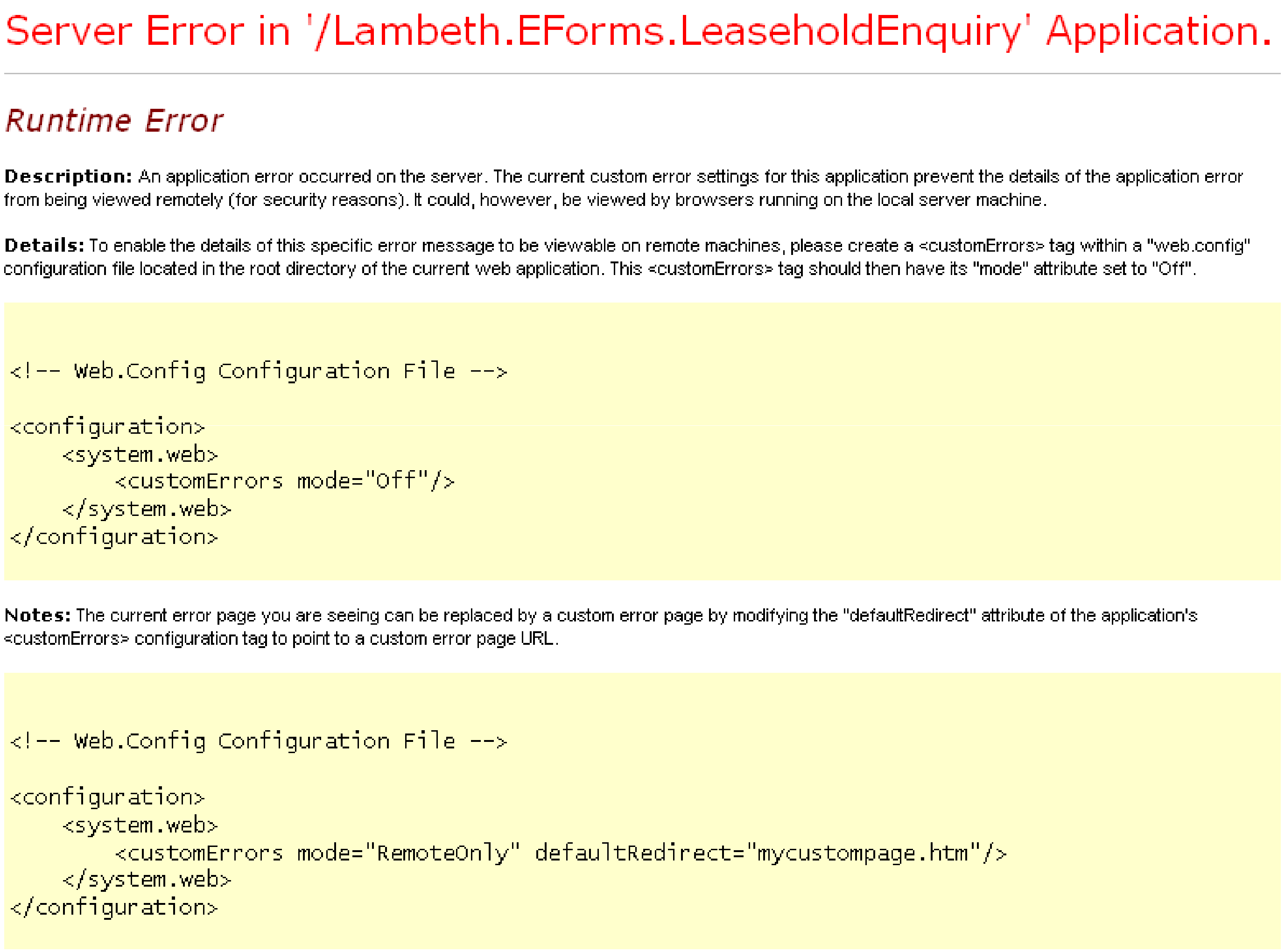
The correspondence address is where we will write to you with further information on your property if it is different from the leasehold property. Leave this blank if it is the same as the address above.

Property name or number	
Street address	
Town/City	
Country	Afghanistan

Who to contact

Insurance Services
3rd Floor
Olive Morris House
18 Brixton Hill
Phone numbers:
020 7926 9290
020 7926 9330
020 7926 9301
RiskandInsurance@lambeth.gov.uk

WCAG Sniffing: Hopefully there... (3/3)



Server Error in '/Lambeth.EForms.LeaseholdEnquiry' Application.

Runtime Error

Description: An application error occurred on the server. The current custom error settings for this application prevent the details of the application error from being viewed remotely (for security reasons). It could, however, be viewed by browsers running on the local server machine.

Details: To enable the details of this specific error message to be viewable on remote machines, please create a <customErrors> tag within a "web.config" configuration file located in the root directory of the current web application. This <customErrors> tag should then have its "mode" attribute set to "Off".

```
<!-- Web.Config Configuration File -->

<configuration>
    <system.web>
        <customErrors mode="Off"/>
    </system.web>
</configuration>
```

Notes: The current error page you are seeing can be replaced by a custom error page by modifying the "defaultRedirect" attribute of the application's <customErrors> configuration tag to point to a custom error page URL.

```
<!-- Web.Config Configuration File -->

<configuration>
    <system.web>
        <customErrors mode="RemoteOnly" defaultRedirect="mycustompage.htm"/>
    </system.web>
</configuration>
```

References

1. W3C, Policies Relating to Web Accessibility
http://www.w3.org/WAI/Policy/
2. Alexander D, Usability and Accessibility: Best Friends or Worst Enemies?, Monash University, 2006
http://www.valaconf.org.au/vala2006/papers2006/99_Alexander_Final.pdf
3. Henry SL, Accessibility Primer for Usability Specialists, UPA, 2002
http://www.uiaccess.com/upa2002a.html
4. Quesenbery W, What Does Usability Mean: Looking Beyond 'Ease of Use', 2001
http://www.wqusability.com/articles/more-than-ease-of-use.html
5. Thatcher J, Web Accessibility for Section 508
http://www.jimthatcher.com/webcourse1.htm
6. W3C, Web Content Accessibility Guidelines (WCAG) 2.0, Recommendation, 11 December 2008
http://www.w3.org/TR/WCAG20/
7. Henry SL, Integrating Accessibility Throughout Design, Just Ask
http://www.uiaccess.com/accessucd/
8. Whittaker JA and Thompson JA, How to Break Software Security, 2003, Addison Wesley, ISBN 0321194330
9. Open Web Application Security Project (OWASP), Top Ten 2010 rc1
http://www.owasp.org/index.php/File:OWASP_T10_-_2010_rc1.pdf
10. OWASP, Application Security Verification Standard Project (ASVS) 2008, Web Application Edition
http://www.owasp.org/index.php/ASVS#tab=Download

Further reading

1. OWASP, Mapping of WCAG 2.0 Principles, Success Criteria and Conformance Levels to Security Issues
   http://www.owasp.org/index.php/Image:Owasp-wcag2-success-criteria.pdf
2. OWASP, Mapping of WCAG 2.0 Sufficient Techniques to Security Issues
   http://www.owasp.org/index.php/Image:Owasp-wcag2-sufficient-techniques.pdf
3. W3C, Understanding WCAG 2.0 - A guide to understanding and implementing Web Content Accessibility Guidelines 2.0
   http://www.w3.org/TR/UNDERSTANDING-WCAG20/Overview.html#contents
4. W3C, How to Meet WCAG 2.0 - A customizable quick reference to Web Content Accessibility Guidelines 2.0 requirements (success criteria) and techniques
   http://www.w3.org/WAI/WCAG20/quickref/
5. Accessify, Web Accessibility Forums
   http://www.accessifyforum.com/
6. WebAIM, Accessibility Forums
   http://webaim.org/forums/
7. Watson Hall Ltd, Security and Usability
   http://www.watsonhall.com/methodology/security-usability.pl
8. Cranor L and Garfinkel S, Security and Usability: Designing Secure Systems that People Can Use, 2005, O'Reilly Media, ISBN 0596008279

End