Week 2 Practical Exercises

Notes:

- Exercises 4 and 5 will be assessed as part of the Practical Set 1 submission.
- Include HTML comments for your student ID, Name, and Practical Class Time at the top of each source file created.
- All files must be uploaded to your TWA web site before submission of Practical Set 1.

Objectives:

1. Obtain and record your TWA website credentials and URL
2. Become confident using the Site Manager on the TWA website to create, edit, delete & upload files
    a. **Note**: Site Manager documentation is available in vUWS in the `Practical Resources` link.
3. Create a simple HTML5 document using the HTML template (see **Practical Resources** link) as a starting point & upload it to your TWA website
4. Validate HTML5 documents using the w3c validator – *https://validator.w3.org*
    a. **Suggestion**: use the second or third tab on this page rather than the first.
5. Complete all exercises for Week 2 Practical Exercises

Suggested Resources:

- HTML tutorial *https://www.w3schools.com/html/default.asp*
- HTML5 tutorial *https://www.w3schools.com/html/html5_intro.asp*
- HTML tag list *https://www.w3schools.com/tags/default.asp*
- HTML validator *https://validator.w3.org*

Exercise 1:

If you already have your TWA site credentials go to exercise 2.

Go to vUWS and click on `'Web Site Allocation → Start Web Site Allocation'`, then register for your TWA web site.
Please record your TWA site URL, username and password (this is a one-time process).

Exercise 2:

For this exercise, you will create a basic HTML document and upload it to your TWA site. The base HTML template is found on vUWS in the `Practical Resources` link.

- Open the template in a text editor (eg, Code, notepad++, Atom) and mark up the following text with HTML so that when rendered in the browser it looks like:

    # Hello TWA

    This is my first HTML document. It is pretty plain, but there will be more to come!

- Save the file **locally** as `helloTWA.html`
- navigate to the `practicals/week2` folder in your TWA web site
- Upload `helloTWA.html` to the `practicals/week2` folder on your TWA web site.

Exercise 3:

An HTML file has been provided in the zip file named `exercise3-Broken.html`. This file includes **deliberate** errors in the HTML markup.

- Use the W3C HTML validator to check the document for errors and then fix the errors.
- Save the corrected HTML file as `exercise3-Fixed.html`
- Upload `exercise3-Fixed.html` to the `practicals/week2` folder on your TWA web site.

Tips:

1. The Validator will list errors in the order in which they are found in the HTML. The best way to correct the errors is to work from the top of the error list down (ie, don't jump around in the error list)
2. Sometimes fixing an error may expose further errors (don't panic).
3. Sometimes fixing an error may remove multiple errors (rejoice).

Instructions for exercises 4 and 5

General Aim - In exercise 4 and 5 you will create HTML documents using the content of the provided text files which correspond to the numbered exercise. To do this you will markup the content found in the text file with HTML tags so that the ***document structure*** is identical to that shown in the figures starting on page 3. The resulting html document should be saved using the same name as the text file but must have an **html** extension instead. For example, in exercise 4, the file `index.txt` should be marked up using appropriate html tags then saved as `index.html`.

File locations – the HTML files created in these exercises will all reside in the `practicals/week2` folder on your TWA site. The image files used for these exercises will all reside in the `practicals/images` folder on your TWA site.

Hypertext links - if a hypertext link is to be created in the html file it will be indicated as follows in the text file:

In general:	`LINK[link text | link URL | target]`
Example:	`LINK[Accessibility Requirements | requirements.html | new tab]`
Resultant browser rendering:	Accessibility Requirements

Images - if an image is to be displayed in the html document it will be indicated as follows in the text file:

In general:	`IMAGE[image filename | alternate text | caption | width | height]`
Example:	`IMAGE[contrast.png | Contrast Checker icon | 560 | 256]`

All such image files have been supplied in the practical zip file. See note above regarding file locations.

Videos - if a video is to be displayed in the html document it will be indicated as follows in the text file:

In general:	`VIDEO[video URL | width | height | title]`
Example:	`VIDEO [https://www.youtube.com/embed/8Ik_LHmZx8Y | 560 | 315 | youtube vid]`

Document Validation – all of the completed HTML documents must be valid HTML5. That is, validate your HTML and fix all errors.

Exercise 4:

For this exercise, you are to **create** an HTML document named `index.html` by marking up the text found in the `index.txt` file with HTML so that the ***document structure*** is identical to that shown in Figure 1. Think about the tags you will need to achieve your coding. There should be appropriate semantic HTML tags present.

- The *title* of the page is: `Information Security Manual (ISM) | Cyber.gov.au`
- Upload `index.html` to the `practicals/week2` folder on your TWA site

Exercise 5:

For this exercise, you are to create an HTML document named `using.html` by marking up the text found in the `using.txt` file with HTML so that the ***document structure*** is identical to that shown in Figure 2, 3. Think about the tags you will need to achieve your coding. There should be appropriate semantic HTML tags present.

- The *title* of the page is: `Using the Information Security Manual | Cyber.gov.au`
- Upload `using.html` to the `practicals/week2` folder on your TWA site

Australian Government
Australian Signals Directorate

Australian Signals Directorate

Information Security Manual (ISM)

ASD AUSTRALIAN SIGNALS DIRECTORATE
ACSC Australian Cyber Security Centre

The Australian Signals Directorate produces the Information Security Manual (ISM). The purpose of the ISM is to outline a cyber security framework that an organisation can apply, using their risk management framework, to protect their systems and data from cyber threats. The ISM is intended for Chief Information Security Officers, Chief Information Officers, cyber security professionals and information technology managers.

Using the Information Security Manual

This chapter of the Information Security Manual (ISM) provides guidance on using the ISM.

Cyber Security Principles

Follow the Information Security Manual (ISM)'s cyber security principles to protect systems and data.

Cyber Security Guidelines

Practical guidance on how an organisation can protect their systems and data from cyber threats.

Cyber Security Terminology

This chapter of the Information Security Manual (ISM) provides guidance on cyber security terminology.

Cyber Security Guidelines

Practical guidance on how an organisation can protect their systems and data from cyber threats.

Cyber Security Terminology

This chapter of the Information Security Manual (ISM) provides guidance on cyber security terminology.

Archived ISM releases

List of archived ISM releases.

ISM OSCAL releases

List of current and previous ISM releases in the OSCAL format.

Acknowledgement of Country

We acknowledge the Traditional Owners and Custodians of Country throughout Australia and their continuing connections to land, sea and communities.
We pay our respects to them, their cultures and their Elders; past, present and emerging. We also recognise Australia's First Peoples' enduring contribution to Australia's national security.

Australian Cyber Security Hotline

1300 CYBER1 (1300 292 371)

Popular Pages

Essential Eight

Alerts and Advisories

Figure 1 - screen shot of index.html

These images represent the document structure for each of the completed HTML documents from exercises 4 and 5. As indicated in the instructions, it is the document structure that is important. **That is, the presentational aspects of the content are not important at this stage.**

For example, the typeface (font), text colour and size, margins, where lines wrap, etc that are shown in the following pages may be different to what your browser displays depending upon browser defaults and browser window size. The presentational aspects of these html documents will be addressed in the week 3 exercises via CSS.

Australian Government
Australian Signals Directorate

Australian Signals Directorate

Using the Information Security Manual

ASD AUSTRALIAN SIGNALS DIRECTORATE
ACSC Australian Cyber Security Centre

Executive summary

Purpose

The purpose of the Information Security Manual (ISM) is to outline a cyber security framework that an organisation can apply, using their risk management framework, to protect their systems and data from cyber threats.

Intended audience

The ISM is intended for Chief Information Security Officers (CISOs), Chief Information Officers, cyber security professionals and information technology managers.

Authority

The ISM represents the considered advice of the Australian Signals Directorate (ASD). This advice is provided in accordance with ASD's designated functions under the Intelligence Services Act 2001.

ASD also provides cyber security advice in the form of Australian Communications Security Instructions and other cyber security-related publications. In these cases, device and application-specific advice may take precedence over the advice in the ISM.

Cyber security principles

The purpose of the cyber security principles within the ISM is to provide strategic guidance on how an organisation can protect their systems and data from cyber threats. These cyber security principles are grouped into four key activities: govern, protect, detect and respond. An organisation should be able to demonstrate that the cyber security principles are being adhered to within their organisation.

Cyber security guidelines

The purpose of the cyber security guidelines within the ISM is to provide practical guidance on how an organisation can protect their systems and data from cyber threats. These cyber security guidelines cover governance, physical security, personnel security, and information and communications technology security topics. An organisation should consider the cyber security guidelines that are relevant to each of the systems they operate.

Applying a risk-based approach to cyber security

Using a risk management framework

The risk management framework used by the ISM draws from National Institute of Standards and Technology (NIST) Special Publication (SP) 800-37 Rev. 2, Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy. Broadly, the risk management framework used by the ISM has six steps:

1. define the system,
2. select controls,
3. implement controls,
4. assess controls,
5. authorise the system and monitor the system.

Define the system

Determine the type, value and security objectives for the system based on an assessment of the impact if it were to be compromised.

Select controls

Select controls for the system and tailor them to achieve desired security objectives.

Implement controls

Implement controls for the system and its operating environment.

Assess controls

Assess controls for the system and its operating environment to determine if they have been implemented correctly and are operating as intended.

Figure 2 - screen shot of using.html

Implement controls

Implement controls for the system and its operating environment.

Assess controls

Assess controls for the system and its operating environment to determine if they have been implemented correctly and are operating as intended.

Authorise the system

Authorise the system to operate based on the acceptance of the security risks associated with its operation.

Monitor the system

Monitor the system, and associated cyber threats, security risks and controls, on an ongoing basis.

Acknowledgement of Country

We acknowledge the Traditional Owners and Custodians of Country throughout Australia and their continuing connections to land, sea and communities.
We pay our respects to them, their cultures and their Elders; past, present and emerging. We also recognise Australia's First Peoples' enduring contribution to Australia's national security.

Australian Cyber Security Hotline

1300 CYBER1 (1300 292 371)

Popular Pages

Essential Eight

Alerts and Advisories

Figure 3 - screen shot of using.html - continued