Week 3 Practical Exercises

Notes:

- Exercise 1 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:

- Become proficient in writing and applying simple CSS to HTML documents
- Complete exercise 1 below and upload the solution to your TWA web site in the folder indicated below. Test and **validate** the pages.

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`
- CSS tutorial `https://www.w3schools.com/css/default.asp`
- CSS reference `https://www.w3schools.com/cssref/default.asp`
- HTML validator `https://validator.w3.org`
- CSS validator `https://jigsaw.w3.org/css-validator/`

Exercise 1:

- Upload the completed **html** files from Week 2 Exercise 4, and 5 to your TWA web site in the `practicals/week3` folder.
- Upload the new copy of `Cyber_Security.jpg` (found in the week 3 zip file) to your TWA web site in the `practicals/images` folder. This new version of the file has been modified to have the same height as `AUS_GOV_ASD.png` to assist with achieving the desired layout of the pages. In the html of both pages the width and height attributes for `AUS_GOV_ASD.png` remain unchanged. However, for `Cyber_Security.jpg` change height to 180 (width remains unchanged at 200) in both html files.
- For this exercise, you will create a **CSS file** that will be linked to `index.html`, `using.html` that you have uploaded to the `week3` folder.
- Some of the css that you implement may require you to make some changes to your html code. Make these changes to the html files in the `week3` folder but not the `week2` folder.
- Screenshots of the finalised web pages have been provided starting on page 3 of this document.

i. Create a CSS file named `master.css` using your chosen text editor. `Master.css` is to be saved in the `practicals/css` folder of your TWA website.

ii. **Link** `master.css` to `index.html`, `using.html` in the `week3` folder by adding the appropriate html tag(s) to **each** of the html documents.

iii. The styles that you implement in `master.css` should modify the rendering of your html such that it looks like the screen shots on pages 4, 5, and 6 of this document. To achieve the desired layout you should investigate responsive css techniques such as Grid or Grid-view. To assist with the description of the styles to implement in `master.css` the following conventions are adopted:

   a. `Document` refers to the entire html page,
   b. `Header` refers to the section of the html page above the first horizontal line that spans the html page,
   c. `Footer` refers to the section of the html page below the second horizontal line that spans the html page,
   d. `Main Body` refers to the section of the html page between the `Header` and `Footer`,
   e. `Info Box` refers to the green boxes in the `Main Body`.

The following descriptions provide the css rules that apply to the `Document`, `Header`, `Main Body`, `Footer`, and `Info Boxes`. Add appropriate CSS rules to `master.css` to achieve the following:

iv. `Document`

   a. background colour is to be white.
   b. typeface is to be set to a fallback list of fonts in the following order: Arial, and sans-serif.
   c. font size is to be set to 100% of the browser default.
   d. font colour is to be set to black.
   e. One and half line spacing for paragraphs.

f. h1 headings font size of 300% of the browser default font size.
g. h2 headings font size of 220% of the browser default font size.
h. h3 headings font size of 180% of the browser default font size, bottom margin of 0 pixels.
i. h1 and h4 headings text colour of `#003980`.
j. ordered lists display numbering as lower-case roman numerals, top and bottom padding of 10 pixels, one and half line spacing, a left margin of 30 pixels, and the text is indented 30 pixels from the roman numerals.
k. When the mouse moves over a hypertext link the underlining should change to dotted underlining and text colour to `#003980`.

NOTE: Unless stated otherwise, the background and text colours for elements in the following rule descriptions, should inherit from the parent element.

v. Header

a. The two images and two headings should be displayed next to each other as shown in the screen shots. Each image should occupy 25% of the available page width. The two headings occupy 50% of the available page width.
b. Headings h1 and h2 should have a top margin of 0 pixels, be centred, and should use a fallback list of fonts in the following order: Oswald, Arial, and sans-serif. **Hint**: Oswald is not a standard web font. You will need to use the Google Font repository.

vi. Footer

a. The footer should have a top margin of 50 pixels with a 1-pixel solid black border at the top.
b. Headings, paragraphs, and links in the footer should have a bottom margin of 0 pixels. Headings and links should have a font size that is 80% of the browser font size.
c. Paragraphs in the footer should be a font size of 70% of the browser font size.
d. The heading `Popular Pages` should be centred across the page.
e. The two images should be displayed next to each other as shown in the screen shots. The associated links should be displayed beneath the images as shown. Each image and the associated link should occupy 25% of the available screen width in the middle of the page with 25% either side being empty. Each image and link should be centred across the 25% width.

vii. Main Body

a. A 1-pixel wide solid black border at the top.
b. h3 headings are displayed in italics, and in text colour `#003980`.
c. Paragraphs that immediately follow h3 headings have a top margin of 0 pixels.

viii. Info Boxes

a. The info boxes on each page should be displayed in two columns of three. Each column occupies 50% of the available page width.
b. Each info box has 15 pixels around the outside that separates it from the other info boxes.
c. Each info box should have a background colour of `#cae7d0`, left and right padding of 15 pixels, bottom margin of 15 pixels, a 1-pixel wide solid black border which has rounded corners of radius 15 pixels. Each info box should be 130 pixels high. If the content doesn't fit in the info box, scrolling should be possible to view the content.
d. Headings in each info box should have a font size that is 150% of the browser default and have a top margin of 10 pixels.

Screenshots start on the next page…..

Australian Government
Australian Signals Directorate

Australian Signals Directorate

ASD AUSTRALIAN SIGNALS DIRECTORATE
ACSC Australian Cyber Security Centre

Information Security Manual (ISM)

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

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

Archived ISM releases
List of archived ISM releases.

Index.html page

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

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

Australian Government
Australian Signals Directorate

Australian Signals Directorate

ASD AUSTRALIAN SIGNALS DIRECTORATE
ACSC Australian Cyber Security Centre

Using the Information Security Manual

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.

Start of Using.html

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:

i. define the system,
ii. select controls,
iii. implement controls,
iv. assess controls,
v. authorise the system,
vi. 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.

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

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

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

Implement controls
Implement controls for the system and its operating environment.

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

End of Using.html

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

Executive summary

Mouse over link in main body of page

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.

Popular Pages

Essential Eight


Alerts and Advisories

Mouse over link in footer

https://www.cyber.gov.au/resources-business-and-government/essential-cyber-security/essential-eight

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

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

Mouse over link in info box