DUMPSARENA

CIW Web Foundations Associate

CIW 1D0-610

Version Demo

Total Demo Questions: 18

Total Premium Questions: 187

Buy Premium PDF

https://dumpsarena.co

sales@dumpsarena.co

sales@dumpsarena.co
dumpsarena.co

Topic Break Down

Topic	No. of Questions
Topic 1, Internet Business Associate	66
Topic 2, Site Development Associate	57
Topic 3, Network Technology Associate	64
Total	187

QUESTION NO: 1

Carlos is the Information Technology (iT) administrator for a small company. Over the past year, employees have been using their personal mobile devices and smart phones for business use. This has reduced costs of purchasing new devices for employees. Carlos is now considering whether he should stop supplying employees with company phones and instead require all employees to use their personal smart phones for work. How can Carlos address the most significant security vu inerrability?

A. Develop a robust app to push security updates out to the various mobile OS devices

B. Create an employee policy that requires employees to keep phones updated to the latest technology

C. Create a policy that specifies acceptable use, ensuring security measures are in place for mobile devices

D. Mandate that employees switch to the company's mobile service provider to ensure security policies are enforced

ANSWER: C

Explanation:

Create a policy that specifies acceptable use, ensuring security measures are in place for mobile devices is correct because the central risk in a bring-your-own-device environment is that the organization does not inherently control personally owned phones in the same way it controls company-issued assets. A formal mobile-device and acceptable-use policy establishes the conditions under which personal devices may access company data, email, applications, and networks. It can require practical safeguards such as supported operating-system versions, timely security updates, strong screen locks, device encryption, multifactor authentication, approved applications, secure network use, and reporting of a lost or stolen device.

The policy also defines employee responsibilities and gives the company authority to enforce those requirements through mobile-device-management or mobile-application-management tools where appropriate. This creates a consistent, documented security baseline across different device models, operating systems, and carriers while recognizing that the devices remain personally owned. NIST's mobile-device guidance emphasizes establishing organization-wide mobile-device security requirements and managing devices throughout their use. Its guidance is available in NIST SP 800-124 Rev. 2, Guidelines for Managing the Security of Mobile Devices in the Enterprise. Additional policy and management considerations for personally owned devices are covered by CISA's mobile-device security resources.

QUESTION NO: 2

SuperBank is considering a cloud service from Local Data Center, Inc., to support the bank's expanding needs. SuperBank's managers are concerned about security. What can SuperBank request to protect its data from security threats?

A. For Local Data Center to run multiple hypervisors

B. For Local Data Center to install a DDoS mitigation system

C. For SuperBank staff to manage the servers at Local Data Center, Inc.

D. For SuperBank to perform background checks on the staff at Local Data Center, Inc.

ANSWER: D

Explanation:

Requesting background checks on the staff at Local Data Center, Inc. is an appropriate security requirement because cloud-provider personnel can potentially access customer systems, facilities, infrastructure, or sensitive information while performing operational and administrative duties. Personnel screening helps the bank and provider reduce the risk that individuals with unsuitable histories are placed in trusted roles. This is particularly important for a financial institution, where protecting confidential customer and business data requires attention to insider threats as well as technical threats.

SuperBank can make personnel-security expectations part of its cloud-service agreement and due-diligence process. The requirement should define which roles require screening, when checks occur, how personnel changes are handled, and how the provider demonstrates compliance while respecting applicable employment and privacy laws. Background checks are one component of a broader cloud security program, but they directly address the trustworthiness of people who may be able to affect the confidentiality, integrity, or availability of SuperBank data. NIST's cloud-computing security guidance

identifies the importance of assessing cloud-provider security controls, and NIST's personnel-screening control specifically addresses screening individuals before authorizing access to systems and information. See NIST SP 800-144 and NIST SP 800-53, Personnel Screening.

QUESTION NO: 3

Irena is reviewing several promotional product videos from her company's marketing department before they are published on the company's Web site. The videos are in RealMedia format, but they do not open in Irena's Windows Media Player. What should Irena do in order to view the videos?

A. Contact her company's Technical Support department and schedule service for her computer.

B. Convert the video files to the WMV format, because RealMedia files will not play in Windows Media Player.

C. Upload the videos to the Web server to be viewed through Windows Media Player because they will not play from a local computer.

D. Decompress the files before attempting to play them in Windows Media Player, because RealMedia files are compressed for uploading/downloading.

ANSWER: B

Explanation:

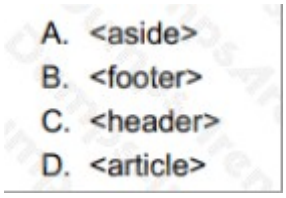
Convert the video files to the WMV format, because RealMedia files will not play in Windows Media Player. is the appropriate action when Irena needs to use Windows Media Player to review the files. RealMedia is a multimedia format historically associated with RealNetworks software and commonly uses RealMedia file extensions and codecs. Windows Media Player is designed primarily for Microsoft-supported media formats, including Windows Media Video, whose usual file extension is .wmv. Converting the videos creates files encoded in a format Windows Media Player is intended to recognize and decode, allowing Irena to open and review the promotional content before publication.

This is a format-compatibility issue, rather than a problem requiring computer service, server upload, or decompression. Media files are generally already encoded and packaged for playback; simply placing them on a web server does not change the player's ability to decode their format. Microsoft's documentation describes Windows Media Player's supported file types and the role of codecs in playback: File types supported by Windows Media Player. For background on the Windows Media format family, see Windows Media Format SDK.

QUESTION NO: 4

Sampson has used HTML5 to create a Web page that contains image-based navigation buttons.

He would like to add text-based navigation to help ensure accessibility. Which of the following HTML5 elements should he use?



A. Option A

B.

C. Option C

D. Option D

ANSWER: B

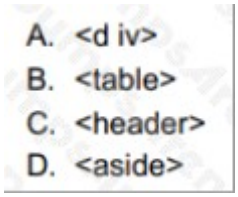
Explanation:

The <nav> element is the appropriate semantic HTML5 container for a major set of navigation links. Sampson can place accessible, text-based <a> links inside this element, giving visitors a clear alternative to image-only controls. Text links are more broadly usable because they can be read by screen readers, reached with a keyboard, resized by users, and understood when images are unavailable. The semantic meaning of <nav> also helps assistive technologies identify the region as navigation, allowing users to move efficiently among page landmarks and locate groups of links.

The HTML specification defines <nav> as a section that contains links to other pages or to parts within the current page, particularly a major navigation block. A navigation landmark should contain meaningful link text that communicates each destination or action without relying on the appearance of an image. This combines HTML5 semantic structure with an accessible text-based navigation method. See the HTML Living Standard definition of the nav element and MDN's guidance for the <nav> element.

QUESTION NO: 5

Web pages structured with which tag will fail W3C validation tests, no matter what standard is used?



A. Option A

B. Option B

C. Option C

D. Option D

ANSWER: B

Explanation:

The markup shown in the correct response uses a tag structure that is not permitted by a W3C-defined HTML document model. Validation is not simply a check that angle brackets and closing tags appear to be present; it checks whether each element is allowed at that location and whether the document conforms to the declared HTML standard or document type. When a page is built around markup that no supported W3C HTML specification permits in that role, changing the declared standard cannot make the document valid. The validator will therefore report a structural or element-content-model error consistently, because the page's organization conflicts with the formal rules used to define valid HTML. This matters in practice because valid, well-structured markup improves predictable rendering, maintainability, accessibility-tool interpretation, and compatibility across browsers and devices. The W3C Markup Validation Service describes validation as checking Web documents against formal markup rules, while the HTML Standard defines the required element structure and content models that validators evaluate. See the W3C Markup Validation Service and the HTML Living Standard.

QUESTION NO: 6

You have 20 remote employees flying in to attend a corporate meeting. The morning of travel day, the administrator tells you that the hotel reservations have changed. What is the best way to send each traveling employee a quick message with the new hotel information?

A. Update the meeting agenda with the hotel information.

B. Post an announcement to the company's Web site with the new hotel information.

C. Call each stakeholder and leave a message with the address of the hotel.

D. Send a text message with the hotel information to the mobile phone of each traveler.

ANSWER: D

Explanation:

Sending a text message with the hotel information to the mobile phone of each traveler is the best choice because it provides immediate, direct communication to people who are likely in transit and may not have convenient access to email, a meeting agenda, or the company website. SMS messages are designed for short, time-sensitive updates and are typically delivered quickly over a cellular network. A concise message can include the replacement hotel's name, street address, phone number, and any essential reservation or transportation instructions, allowing each employee to act on the change without needing to search for information elsewhere.

Because the change occurs on the morning of travel, speed and visibility are especially important. Mobile messaging is well suited to urgent operational notices because recipients commonly carry their phones while traveling and can review the details immediately. The FCC's consumer guidance on text messaging describes text messaging as a wireless communication service, and the CISA guidance on recognizing phishing supports the practical security habit of ensuring messages contain clear, recognizable organizational details when sharing important information. Use the organization's established messaging process and confirm that traveler mobile numbers are current.

QUESTION NO: 7

You are a small-business owner and would like to encourage employees to bring their own devices (BYOD) to work. Which of the following can help reduce the security risks associated with a BYOD implementation?

A. Expense accounts

B. Acceptable use policy

C. End user license agreement

D. In-house device maintenance

ANSWER: B

Explanation:

An acceptable use policy can reduce BYOD security risk by establishing the rules employees must follow when using personally owned devices for business purposes. A well-defined policy identifies permitted business use, prohibited activities, required security safeguards, and each employee's responsibilities for protecting company information. For example, it can require a screen lock, strong authentication, current operating-system updates, approved applications, encrypted storage, and prompt reporting when a device is lost, stolen, or suspected of being compromised. It can also state the organization's authority to manage business data on the device, including removing organizational data when employment ends or when a device no longer meets security requirements.

BYOD introduces a mix of personal and organizational information on endpoints that may not be purchased, configured, or physically controlled by the business. An acceptable use policy creates clear, communicated expectations that support consistent security practices and enforcement. It should be acknowledged by users and reviewed periodically as technology, threats, and business needs change. NIST notes that organizations should define and communicate mobile-device security requirements, including policy requirements, as part of mobile-device management. See NIST SP 800-124 Rev. 2 and the CISA cybersecurity best-practices guidance.

QUESTION NO: 8

Carol is experiencing read/write errors when trying to save files on her Windows-based laptop. To correct the issue, she could consider performing which of the following maintenance tasks?

A. Disk cleanup

B. fsck command

C. chkdsk command

D. Disk defragmentation

ANSWER: C

Explanation:

The **chkdsk command** is the appropriate Windows maintenance task because it checks a disk volume's file-system integrity and can identify problems that lead to read/write errors. When Windows encounters errors while saving files, the cause may be logical file-system corruption, invalid file records, directory errors, or bad sectors on the storage device. Running CHKDSK with repair parameters allows Windows to correct detected file-system errors; using the scan for bad sectors also attempts to recover readable data and marks unusable sectors so they are avoided in the future. For example, an elevated Command Prompt can run `chkdsk C: /f` to fix errors, and `chkdsk C: /r` to locate bad sectors and recover readable information. Because the system volume is normally in use, Windows may schedule the check for the next restart. This makes the chkdsk command a practical first maintenance step for persistent disk-related save failures on a Windows laptop. Microsoft documents CHKDSK syntax, parameters, and its role in checking volume metadata and file-system errors in its CHKDSK command reference. For additional guidance on checking a drive for errors through Windows tools, see Microsoft Support.

QUESTION NO: 9

Which line of code uses the correct syntax to apply an external CSS style sheet to HTML documents?

A. <link rel=stylesheet type=css href=syb/syb.css/>
B. <style ref =stylesheet type=text/css href=syb/syb.css/>
C. <style ref="stylesheet" type="css" href="syb/syb.css"/>
D. <link rel="stylesheet" type="text/css" href="syb/syb .css"/>

A. Option A

B. Option B

C. Option C

D. Option D

E.

ANSWER: E

Explanation:

The line `<link rel="stylesheet" href="styles.css">` correctly associates an external CSS resource with an HTML document. The `link` element supplies metadata and relationships between the current document and an external resource, and it belongs in the document's `head` section. Its `rel="stylesheet"` attribute identifies the relationship as a style sheet, allowing the browser to treat the referenced file as CSS. The `href` attribute provides the URL or relative path to that CSS file; in this example, `styles.css` refers to a file in the same directory as the HTML page. When the browser loads the document, it retrieves that file and applies its CSS rules to matching elements in the page. This approach separates presentation rules from HTML content, enables the same styles to be reused across multiple pages, and makes site-wide maintenance more efficient. The HTML Standard defines `link` as the mechanism for linking external resources, while MDN documents the stylesheet relationship and the relevant attributes. See the HTML Standard link element specification and MDN's link element reference.

QUESTION NO: 10

Which term describes the practice of actively collecting wireless networking data from companies and individuals?

A. War driving

B. Spear phishing

C. Dictionary attack

D. Social engineering

ANSWER: A

Explanation:

War driving is the practice of searching for, detecting, and collecting information about wireless networks while moving through an area, traditionally by using a vehicle equipped with a wireless-capable device and scanning software. The collected information can include network names (SSIDs), signal strength, wireless security configuration, access-point identifiers, and sometimes location data. This activity can identify wireless networks operated by businesses or private individuals and may be used for legitimate wireless surveying and security assessment when authorized. However, it is also associated with reconnaissance by attackers seeking poorly protected networks. The key idea is the active discovery and recording of nearby Wi-Fi network data, rather than attempting to persuade a user, guess a password, or target a message at a particular recipient. NIST's cybersecurity glossary defines wardriving as using a vehicle and wireless equipment to locate wireless networks, which directly matches the activity described in the question. See the NIST CSRC definition of wardriving and NIST's Guide to Securing Legacy IEEE 802.11 Wireless Networks for related wireless-security context.

QUESTION NO: 11

Jenny recently switched from broadband cable Internet to ADSL service with her local phone company. To economize, she chose the self-installation option. It appears that her ADSL modem is not allowing her to connect to the Internet. Which setting should she check first?

A. Loopback address

B. Software version

C. Default gateway

D. Device name

ANSWER: C

Explanation:

The correct setting to check first is **Default gateway**. On a home ADSL installation, the DSL modem or modem/router commonly serves as the local network's default gateway. A computer uses its default gateway whenever it needs to send traffic beyond the local LAN, including requests for Internet sites. If the computer still has network settings left over from the previous cable connection, or if it did not receive the proper gateway automatically from the ADSL modem's DHCP service, it can communicate only with devices on its own local subnet and will not be able to reach the Internet.

Checking the default-gateway value helps confirm that the computer is directing Internet-bound traffic to the ADSL modem's LAN address. In a typical self-installation, the computer should be configured to obtain TCP/IP settings automatically unless the provider supplied specific static values. The gateway shown by the operating system should match the modem/router's local management address, as documented by the service provider or device manufacturer. Microsoft's networking documentation describes the default gateway as the route used for traffic destined outside the local network: Microsoft Learn: Network subnetting. For practical Windows troubleshooting and IP configuration review, see Microsoft Support: Using the ipconfig command.

QUESTION NO: 12

Which security issue is most closely associated with wireless networks?

A. Spoofing

B. War driving

C. Eavesdropping

D. Man-in-the-middle

ANSWER: B

Explanation:

War driving is the security issue most closely associated with wireless networks because it specifically involves traveling through an area, often in a vehicle, while using a wireless-enabled device to discover and map nearby Wi-Fi networks. The activity can identify network names (SSIDs), signal strength, channel use, and whether an access point appears to use wireless security protections. This reconnaissance can reveal exposed or poorly configured WLANs and helps illustrate why wireless networks need deliberate configuration, strong authentication and encryption, and monitoring for unauthorized access points.

The defining feature of war driving is its focus on locating wireless access points from outside a building or organization's physical perimeter. Radio signals can extend beyond the intended coverage area, so a person does not necessarily need to enter the premises to detect a network. NIST's guidance on securing wireless local area networks addresses the need to protect WLAN communications and manage wireless risks: NIST SP 800-153, Guidelines for Securing Wireless Local Area Networks. The term and practice are also discussed in security-awareness material from CISA's Wi-Fi security guidance.

QUESTION NO: 13

You need to center and indent a quote on your Web page. Which is the best way to accomplish this using HTML5?

A. Use the tag.

B. Use the

tag.

C. Use the style attribute 1%lith the tag.

D. Use the text-align attribute with the tag.

ANSWER: B

Explanation:

Use the `<blockquote>` tag. The HTML `<blockquote>` element is the semantic HTML5 element for a section quoted from another source. Because it is a block-level quotation, browsers normally render it as a separate block with margins on the inline start and end sides. This conventional rendering indents the quoted material from surrounding page content and gives it the visually distinct, centered-block appearance intended for a longer quotation. The element also communicates the quotation's meaning to assistive technologies, search tools, and other software that interprets document structure. A `cite` attribute can be included when a source URL is available, preserving a machine-readable reference to the quoted work. Presentation can be refined with CSS when a particular layout is required, but `<blockquote>` remains the correct HTML foundation because it identifies the content as a block quotation rather than merely applying visual formatting. The HTML specification defines `<blockquote>` as a section quoted from another source, and MDN documents its usual browser rendering and attributes. See the WHATWG HTML specification and MDN blockquote reference.

QUESTION NO: 14

Configuring a wireless network involves several steps. Which of the following is a task that should be performed to configure and connect to a wireless network?

A. Configure a certificate authority and configure the trust settings.

B. Configure the wireless AP's SSID, encryption level and shared key.

C. Connect your computer to the same network hub as the wireless AP.

D. Connect your computer to the same network switch as the wireless AP.

ANSWER: B

Explanation:

Configuring the wireless AP's SSID, encryption level and shared key is a core task in establishing a usable and secure wireless LAN. The service set identifier (SSID) is the network name that client devices select when they search for available Wi-Fi networks. The encryption/security setting determines how wireless traffic and access are protected, such as WPA2-Personal or WPA3-Personal. When a personal Wi-Fi security mode is used, the shared key (also called a passphrase or pre-shared key) must be configured on the access point and supplied by clients so that they can authenticate and join the network.

These settings must be coordinated between the wireless access point and the connecting device: the client chooses the correct SSID and uses security settings and credentials compatible with those configured on the AP. Using modern Wi-Fi security and a strong, unique passphrase helps prevent unauthorized devices from accessing the network and protects data transmitted over the wireless link. The Wi-Fi Alliance provides an overview of Wi-Fi CERTIFIED WPA3 security at Wi-Fi Alliance: Wi-Fi Security. For practical guidance on selecting secure wireless encryption, see CISA: Understanding Wi-Fi Security.

QUESTION NO: 15

Marion has been hired by a popular national salon business to refresh its existing Web site and update it to valid HTML5 code. Money is not an issue, but time is. Marion is asked to complete the project within eight weeks. The site currently includes 10 pages and connects to a back-end database so that customers can sign in for a personalized experience. Marion suspects that most of the existing code will need to be replaced. Marion must ensure that she has plenty of time for the testing phase, so she needs to complete the planning phase, in which she selects the multimedia for the site, within the next couple days. Which strategy should Marion use in the planning phase?

A. Take pictures of the salons herself.

B. Purchase stock photos from online resources.

C. Hire a photographer to take pictures of the salons.

D. Edit existing images of the salons to update them.

ANSWER: B

Explanation:

Purchase stock photos from online resources. is the appropriate planning strategy because the project has a very short timetable and Marion needs to select usable multimedia within only a few days. Reputable stock-image libraries provide immediately searchable, downloadable assets with clearly defined license terms, allowing her to quickly identify images that fit the salon's visual style, page layouts, and technical requirements. This approach avoids scheduling, shooting, transferring, selecting, and processing a new set of photographs, leaving more of the eight-week schedule available for rebuilding the site, integrating the database-driven features, validating the markup, and performing thorough testing.

Because money is explicitly not a limiting factor, Marion can obtain professionally produced, high-resolution images and the appropriate commercial license without delaying the project. During planning, she should document the source, license, permitted uses, attribution requirements if any, and the versions selected for each page. That record supports lawful reuse and makes later maintenance easier. The U.S. Copyright Office explains that photographs are protected by copyright and require appropriate permission or licensing for reuse: Copyright Office FAQ. For practical guidance on licensing stock imagery, see Adobe Stock licensing information.

QUESTION NO: 16

What does the following represent?

2E22: 4F00: 000E: 00D0:A267:97FF:FE6E:FE34

A. A MAC address

B. An IPv4 address

C. An IPv6 address

D. An IP diagnostic loopback address

ANSWER: C

Explanation:

An IPv6 address is correct because the value is written in IPv6's standard hexadecimal, colon-separated notation. An IPv6 address is 128 bits long and is conventionally represented as eight groups of four hexadecimal digits, with each group representing 16 bits. The supplied value contains exactly eight such groups: `2E22`, `4F00`, `000E`, `00D0`, `A267`, `97FF`, `FE6E`, and `FE34`. Together, these groups represent 128 bits, which is the defining address length for IPv6.

IPv6 permits leading zeroes in a group, as shown by `000E` and `00D0`. In normal use, those leading zeroes may be omitted, and one contiguous sequence of all-zero groups may be abbreviated with a double colon, but neither abbreviation is required. The full, uncompressed representation shown is therefore valid IPv6 formatting. The Internet Engineering Task Force defines IPv6 addressing architecture and its textual representation in RFC 4291. For an accessible overview of IPv6 addresses and notation, see ICANN's IPv6 Addressing guide.

QUESTION NO: 17

Since the advent of HTML5, which choice accurately describes a difference between a mobile app and a mobile Web site?

A. A mobile Web site is faster because it uses the mobile phone's default browser.

B. A mobile app is faster because it does not necessarily use the browser.

C. A mobile Web site cannot create an immersive experience for users.

D. A mobile app can be used on any operating system.

ANSWER: B

Explanation:

A mobile app is faster because it does not necessarily use the browser. A native mobile app is installed on the device and runs through the operating system's application framework rather than being rendered solely by a Web browser. This architecture can allow the app to use device resources, locally stored data, and operating-system services more directly. As a result, it can deliver responsive interaction and continue to provide key functionality when connectivity is limited, depending on how the app was designed.

HTML5 significantly improved what mobile Web sites can do by providing capabilities such as richer media, offline storage, and improved application-like interfaces. However, an HTML5 mobile Web site is still normally accessed and executed within a browser environment. The distinction in this question is therefore not that HTML5 prevents rich mobile Web experiences, but that a mobile app is not required to rely on the browser runtime. This is a general architectural difference; actual performance still depends on the quality of the app or site, the device, network conditions, and the work being performed. See MDN Web Docs: Native application and web.dev: Learn Progressive Web Apps.

QUESTION NO: 18

Consider the following HTML5 code:

```
<!DOCTYPE html>
<html lang="en">
<head>
    <title>My Favorite Movie Quotes</title>
    <link rel="stylesheet" href="css/styles.css"/>
</head>
<body>
<p> This Web site is devoted to my favorite movie quotes. These iconic movie quotes have
been used time and again but will never lose their appeal. </p>
<p> CAPTAIN (Strother Martin) in Cool Hand Luke (1967)
<blockquote> "What we've got here...is a failure to communicate." </blockquote>
</p>
</body>
</html>
```

The code does not validate as HTML5. Why?

A. The

B. The tag and its attributes are missing.

C. The tags.

D. The !DQCTYPE declaration is missing a reference to the Document Type Definition (DTD).

ANSWER: C

Explanation:

The <p> tags are the source of the validation problem because HTML paragraph elements have strict content rules. A <p> element represents a paragraph and cannot contain another paragraph element. When a browser encounters a new <p> start tag while a paragraph is already open, its HTML parser implicitly closes the first paragraph before processing the new one. This error-recovery behavior can make the rendered page appear reasonable, but it does not make the original markup conforming HTML5. The document must instead use properly separated paragraph elements, with each paragraph opened and closed independently, or use an appropriate container element when content needs to be grouped. The HTML specification defines the paragraph element and its permitted content model at the WHATWG HTML Standard. The markup can then be checked with the W3C Nu HTML Checker, which reports invalid paragraph nesting and related structural markup errors.