## Learning Objectives

2.1 **Introduction** ......................................................... 3

2.2 **Bring Your Own Device (BYOD)** ........................................ 3

2.2.1 **Advantages of BYOD** .......................................... 4

2.2.2 **Security Concerns of BYOD** ...................................... 4

2.2.3 **Controls Relating To BYOD** .................................... 5

2.2.4 **Opportunities for CAs** .......................................... 5

2.3 **XML-XBRL** ........................................................... 5

2.3.1 **XML** ..................................................................... 5

   - What is XML? ............................................................ 5

   - Why to use XML? ....................................................... 6

   - How is XML used? ..................................................... 6

   - Where is XML used? ................................................. 6

   - Who is using XML? .................................................. 7

   - Risks of using XML .................................................. 7

   - Controls in XML .................................................... 7

2.3.2 **XBRL** ............................................................... 7

   - Use of XBRL in financial sector ................................ 8

   - Advantages of XBRL ................................................. 8

   - How is XBRL used? .................................................. 9

   - Risks in XBRL ........................................................ 9

   - Controls in XBRL .................................................... 10

2.4 **Use of Social Media** .................................................. 10

2.4.1 **Risks and Security Concerns in Use of Social Media** ........ 11

2.4.2 **Mitigating Security Concerns** .................................. 11

2.4.3 **Opportunities for CAs** .......................................... 12
2.5 Geolocation

2.5.1 Benefits of Geolocation

2.5.2 Risks and security of Geolocation

2.5 Summary

2.6 References

2.7 Questions

2.8 Answers
CHAPTER 3: OVERVIEW OF CLOUD COMPUTING AND MOBILE CLOUDING: CHALLENGES AND OPPORTUNITIES FOR CAS

PART 2: EMERGING TECHNOLOGIES: BYOD, XML-XBRL AND SOCIAL MEDIA

Learning Objectives

- To gain an overview of BYOD
- To gain an overview of XML and XBRL
- To gain an overview of use of Social Media

2.1 Introduction

IT environment is continually evolving and growing. The growing trend in this direction is BYOD (Bring your own Device) and now even BYOT (Bring your own Technology) where employees are encouraged to use their hand-held devices for organisation’s business. A common term sometimes used is BYODT. Use of XML and XBRL has changed the way of corporate reporting and enhances the distribution and usability of existing financial statement information. Another technology trend that has brought a whole revolution is the use of Social Media. Social media has become a big booster to any business. Whereas all these provide advances in technology at the same time, the potential risks associated with these cannot be ignored. Chartered Accountants have to know about these technologies works, their risks, security and controls and impact on assurance. This understanding can help CAs in using these technologies as relevant not only in their own offices and professional practice but also to provide consulting and assurance services to organisations in these emerging area.

2.2 Bring Your Own Device (BYOD)

BYOD refers to that policy of an organisation that allows its employees to use a preferred computing device like a laptop or a smart phone. It allows employees to use personal devices to connect to the corporate network for information. The workspaces are made flexible that allows employees to work beyond the required hours. It has reduced IT costs for organisations because a onetime investment is made by the organisation that enables employees to buy and maintain their devices. However, it
Module 1: Facilitated e-Learning

also means surrendering all control over the end-user device. Service delivery, data protection and providing support and services when user device is not working are some of the challenges. If not properly controlled the device may become conduit for a serious data security breach.

2.2.1 Advantages of BYOD

BYOD implementation has many advantages. These are:

- **Happy Employees**: Employees love to use their own devices when at work. This also reduces the number of devices an employee has to carry; otherwise he would be carrying his personal as well as Organisation provided devices.
- **Lower IT Budgets**: Could involve financial savings to the Organisation since employees would be using the devices they already possess thus reducing the outlay of the Organisation in providing devices to employees.
- **IT reduced support requirement**: IT Department does not have to provide end user support and maintenance for all these devices resulting in cost savings.
- **Early adoption of new technologies**: Employees are generally proactive in adoption of new technologies. Their early adoption of technologies also results in enhanced productivity of employees leading to overall growth of business.
- **Increased Employee efficiency**: Employees using their own devices are adept at these and are familiar with these devices. The efficiency of employees is more whereas in Organisation provided devices employees have to learn and there is a learning curve involved.

2.2.2 Security Concerns of BYOD

- **Security Administration Issues**: The device may have been built on relatively nascent, consumer focussed platform that does not provide the underlying management controls of the organisation. Allowing employees to bring their own devices has to be aligned with the Security Governance and security policies.
- **Ownership of Data and Regulatory compliance issues**: Private and corporate data is on the same device could raise ownership issues. Much regulatory compliance would become difficult for corporates to follow.
- **Confidentiality and Privacy issues**: This would be a huge challenge for the Organisation, protecting the data on devices not owned by it. Many organisations having sensitive data, this could be the toughest challenge. If the device is connected to the network of the organisation without appropriate controls having been put in place, this could lead to unauthorized access to the whole network.
- **Compatibility issues**: Since employees will be having diverse devices, there will not be a uniformity and whole lot of compatibility issues could arise. Applications on devices also could be different leading to incompatibilities
- **Reluctance of employees**: Not all employees could be comfortable with using their own devices for office work.
2.2.3 Controls Relating To BYOD

Effective implementation of controls to mitigate these risks could be:

- **Establishing a BYOD Governance framework:** A strategy for BYOD usage could be framed taking into account Network access Controls, Device Management controls, Application Security management controls.

- **Security Policy:** A well-defined security policy specifying the rules for use and organisations expectations regarding security should be there clearly specifying the security requirements like security tool to be mandatorily installed or prohibiting download of black listed applications or encryption of data. Policy may specify that only approved and duly authorized devices that are known to have appropriate security controls are used.

- **Appropriate Use Policy:** The employees may be required to sign an AUP that specifies organisation’s expectations of employee responsibilities.

- **Network Security:** Secure access to corporate networks could be ensured using VPNs.

- **Segregation of Personal and Corporate Data:** Data classification should be followed to determine the kind of data which can be stored on personal devices. Important data of Organisation could be in a separate container with encryption, apart from providing protection this also makes it easy to wipe corporate data when an employee leaves the organisation or the device is stolen, where data could be wiped remotely.

- **Secure Remote Support:** Organisations may deploy remote Support Solutions that facilitates remote configuration and control of the device from Help Desk. They also provide access and activity logs for monitoring.

- **Regular Audits:** All the BYOD Devices should be subject to audits to determine adherence to Security policies and determining the kind on data residing on those devices.

2.2.4 Opportunities for CAs

Due to significant risks involved in BYOD adoption, Chartered Accountants being control experts can provide assurance or consulting services in formulating right type of policies, implementing governance framework and implementing right level of security using best practices as appropriate.

2.3 XML-XBRL

2.3.1 XML

What is XML?
World Wide Web Consortium (W3C) has defined XML as follows: “XML is a set of rules, guidelines, conventions, whatever you want to call them, for designing text formats for such data, in a way that produces files that are easy to generate and read (by a computer), that are unambiguous, and that
avoid common pitfalls, such as lack of extensibility, lack of support for internationalization or localization, and platform-dependency."

XML was initially developed by the World Wide Web Consortium (W3C). XML is universally accepted method of exchanging information. XML stands for eXtensible Markup Language. It is a markup language just like HTML. XML is a platform-independent, self-describing, expandable, standard data exchange format. XML was designed to describe data and to carry data, it does not do anything, it is created to structure, store, and to send information. XML uses self-Descriptive XML Schema or Data Type Definition (DTD) to describe Data.

It is much more powerful than HTML (Hypertext Markup Language). HTML is a page description language and is used for specifying how text, graphics, videos and sound are placed on a web page document. Whereas HTML describes how data should be presented in the form of web pages, XML performs presentation, communication and storage of data. In XML, tags represent a price, a date or a PIN code for example. XML makes it possible for computers to manipulate and interpret data automatically and perform operations on the data without human intervention.

In HTML Tags are predefined, whereas in XML Tags are not predefined; we must define our own tags. The XML tag teaches the receiving program how to read the data. For example <DATE>March 31, 2014</DATE> i.e. it describes information not presentation and tags <Date> has been defined by us. With XML, data can be stored outside an HTML in another file or can also be stored inside HTML.

Why to use XML?

Computer systems and databases may contain data in incompatible formats. The challenge is how to make these systems interoperable so that they can exchange data. This exchange of data is facilitated by XML, since XML helps create data so that it can be read by different applications. XML enables new levels of interoperability as it is portable, vendor neutral and is also in an easily readable format which is supported by all major software products. XML provides a standard format for data exchange, enabling web services to pass data from one process to another.

How is XML used?

An example of how XML is used is given below:

```xml
<Account>
  <AccountID>123456</Name>
  <Name>Travelling Expenses</Name>
  <Group>Expenses</Group>
  <Opening Balance>2344.00</Opening Balance>
  <Type>Dr</Type>
</Account>
```

It gives meaning to raw data by describing information through use of tags.

Where is XML used?

Today XML is being used to exchange financial information, business information, and Industry information. It is being used in many B2B (Business to Business) applications. Many Web Services
rely upon integrated software solutions. All these are using XML for data interchange amongst the applications.

Who is using XML?
XML is being used by:

- Software developers use XML as the core technology for new products to derive advantages of interoperability. Microsoft has made MS Excel 2007 onwards XML based so that data can be shared by different applications.
- Database developers build XML support into their products, since XML data is structured in such a way that allows machines to read it and make it accessible to the database.
- An organisation may have different applications for different processes within the organisation. To enable them to share data, XML is used thus tying inter and intra organisation processes together.

Risks of using XML
The ease of viewing and editing text produces risks related to confidentiality and integrity. The XML specification does not provide mechanisms to enforce standard data formats; thus XML lacks inherent security and does not provide any means of validation, confidentiality or integrity. XML could be cause of denial of service attack through means where XML causes machine to use lot of memory and processing, ultimately hanging the system.

Controls in XML
Controls in XML could be

- For validation, external validation utilities can be used.
- Encryption could be used to ensure confidentiality.
- Security through SSL has to be ensured whenever transmitting XML data over unsecured networks.
- The applications receiving XML may have validations to prevent XML DOS attacks.

2.3.2 XBRL
XBRL (eXtensible Business Reporting Language) is a freely available and global standard for exchanging business information. XBRL allows the expression of semantic meaning commonly required in business reporting. The language is XML-based and uses the XML syntax and related XML technologies such as XML Schema. One use of XBRL is to define and exchange financial information, such as a financial statement. The XBRL Specification is developed and published by XBRL International.

XBRL is a standards-based way to communicate and exchange business information between business systems. It offers major benefits at all stages of business reporting and analysis. XBRL is being used across a wide range of sectors, including securities regulation, banking, insurance, data
aggregators and taxation, as well as for non-financial reporting such as carbon disclosure, sustainability efforts and risk reporting.

Tags for XML are most of the times defined by industry consortiums. These industry’s standard tags are commonly referred to as taxonomy. Taxonomies are similar to dictionaries; they are long lists of agreed-upon definitions for all the terms used in specific types of business reports. Each definition has a “tag” that can be read and used by computers. One such standard taxonomy for business reporting is defined by XBRL. XBRL is “extensible,” meaning local users can extend XBRL taxonomies to satisfy their own needs.

Use of XBRL in financial sector
XBRL is flexible and is intended to support all current aspects of reporting in different countries and industries. Its extensible nature means that it can be adjusted to meet particular business requirements, even at the individual organisation level. With different financial statements speaking different languages, there will always be an inefficient analysis of financial information leading to ineffective communication to investors and stakeholders. With enabling of XBRL, documents can be prepared efficiently, exchanged reliably, published easily, analysed quickly and retrieved by investors simply to enable smarter investments.

Advantages of XBRL
The advantages of XBRL data over conventional forms of data are:

- **Standard** - XBRL is a standard that has been accepted and adopted the world over thus reducing inconsistencies in terminologies and data formatting.
- **Accuracy** - XBRL provides highly accurate data as the data can be both calculated and verified.
- **Speed** - XBRL allows much faster and real-time preparation of reports and at the same time allows efficient, accurate and relevant ways to search data.
- **Reusable** - XBRL data once entered can be reused to represent the same data in multiple ways and multiple formats.
- **Platform Independent** - XBRL is an open standard and hence platform independent, this allows the data to be exchanged and transferred with ease.
- **Region Independent** - XBRL allows the presentation and exchange of data in many different languages.

It also helps in reducing cost of analysing and reporting financial information and helps in corporate decision making. Today by submission of financial information in XBRL to bank, bank will take a lesser time to analyse information and quickly sanction loans to the corporates. A Large Multi-national Corporation using XBRL can quickly publish the financial statements of numerous subsidiaries in different countries, with different languages, using different GAAPs on different computer systems.
How is XBRL used?

XBRL makes the data readable, with the help of two documents – Taxonomy and instance document. Taxonomy defines the elements and their relationships based on the regulatory requirements. Using the taxonomy prescribed by the regulators, companies have to map their reports, and generate a valid XBRL instance document. The process of mapping means matching the concepts as reported by the company to the corresponding element in the taxonomy. In addition to assigning XBRL tag from taxonomy, information like unit of measurement, period of data, scale of reporting etc., has to be included in the instance document. An XBRL instance document is a business report in an electronic format created according to the rules of XBRL.

Let’s say we have the data in table as given here:

<table>
<thead>
<tr>
<th>Company</th>
<th>Financial Statement</th>
<th>Line Item</th>
<th>Label</th>
<th>Year</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

In XBRL the same would be mapped as follows:

```xml
<group>
  <group type="CurrentAssets.CashandCashEquivalents">
    <item period="2012">Rs. 98765432</item>
    <item period="2013">Rs. 99887766</item>
  </group>
</group>
```

Risks in XBRL

Apart from risks related to XML discussed above, some specific risks of XBRL are:

- Creation and implementation of taxonomies incorrectly.
- Errors in Mapping - Inaccurate mapping of business information to tags and the use of inappropriate taxonomies (i.e., XBRL dictionaries that define the specific tags for individual items of data). This can mean that the data retrieved represents invalid and inaccurate transactions.
Module 1: Facilitated e-Learning

- As the XBRL documents may include internal and external links to the organisation; hackers may try to change those links or the linked files.

Controls in XBRL

- Evaluation of algorithms used to Tag XBRL data and an effective internal control structure to ensure accurate tagging.
- Enforcing Change Management Process for XBRL process.
- Hacking and related risks could be mitigated by implementation of appropriate firewall encryptions.

Impact and avenues for CAs

Chartered Accountants spend a lot of time importing data from corporate financial applications to their spreadsheets and allied Data Analysis Software, making the whole thing inefficient. XBRL can help reduce time spent manually preparing information for analysis; further data quality can also be improved through fully automated information exchanges among disparate software applications. Once CAs can electronically receive, validate and send standardized information, they can quickly analyse and confidently redistribute it to managers, stakeholders and others for use in better informed decision making.

Being well versed with the benefits and control issues is of special importance to auditors, as more and more countries are mandating the use of XBLR. The opportunities for CAs are in the area of Assurance Services to organisations, by:

- Developing controls framework tailored to the organisation's specific implementation.
- Assessing the quality of XBRL submission and evaluating the supporting XBRL business processes.
- Evaluating the effectiveness of firewall security controls for prevention of hacking attempts.

2.4 Use of Social Media

Social media is a blur of tweets, shares and content. It has pervaded every aspect of life of individuals and now impacting bottom-line of organisations also. Tech target defines “Social media is the collective of online communications channels dedicated to community-based input, interaction, content-sharing and collaboration. Websites and applications dedicated to forums, microblogging, social networking, social bookmarking, social curation, and wikis are among the different types of social media.” Some of the examples are Facebook, Twitter (microblogging), LinkedIn (social networking), Pinterest (social curation i.e. filtering of information and links in a socially enhanced way around a specific theme).

In Social Media, content is supplied and managed by user through the use of tools and platforms supplied by social media sites. Use of social media by people and organisations is increasing rapidly and the potential benefits of a successful social media strategy are significant. Organisations as well as individuals can create online presence easily and economically, since social media technologies
have significantly reduced the cost of content creation and dissemination to a small or a very large audience in virtually real time. Most of the businesses are changing their strategy of marketing through social media, this change has stemmed from the speed at which information travels in the social media arena. Social media provides an opportunity for businesses, giving them a personalized platform to connect with their customers. By using social media as a way to advertise, the organisation can speak directly to the consumer in an arena they are comfortable with. Social media allows businesses to connect with customers while shaping their perceptions of products and services.

2.4.1 Risks and Security Concerns in Use of Social Media

Many enterprises have adopted social media tools which require no further IT investments and are quick to implement, often these adoptions carry risks such as breach of privacy, fear of legal action, developing a negative reputation and lack of control. These carry a huge risk in terms of enterprise security. Risks could arise from use of social media for client communication or from use of social media by employees on organisation networks or organisation devices. Risks and security concerns also exist in the content put up on social media. The content put on social media could have security concerns relating to privacy and confidentiality and may also have implications in breach of regulations. For highly regulated sectors like finance, insurance and banking social media can be a legal minefield. As an example, on March 7, 2010, Gene Morphis, Chief Financial Officer (CFO) for fashion retailer Francesca’s Holding Corp., tweeted from his personal Twitter account (@theoldcfo): “Board meeting. Good numbers=Happy board.” — two days before the actual numbers were released. Morphis’ 238 Twitter followers were privy to insider information which is an SEC breach. He was fired shortly thereafter for the offense of “improperly communicating organisation information through social media.”

2.4.2 Mitigating Security Concerns

The combination of the right policy and the right technology can mitigate the security concerns and make organisations compliant. These are explained below:

- **Social Media Policy:** The firm must have a social media policy specifying how there will be interaction between organisation and the world through social media. These policies should consider technology as well as regulatory compliance requirements.

- **Training of People:** Employees should be trained on a regular basis on the benefits, opportunities and risks relating to use of social media. Employees have to be educated about the dangers and common pitfalls in the use of social media and how to prevent them, as also acceptable use policy regarding the kind of material that could be posted on social media sites and their use.

- **Pre-approval and vetting of content before uploading:** There should be a system of pre-approval of content like profiles before posting on sites like Facebook and LinkedIn. Interactive content must be supervised both from an official account or an employee’s own personal account relating to business.

- **Provision for regulatory compliances:** Many companies having presence in US and other Countries could be subject to legal compliances relating to those countries. Regulations in
some countries provide for archival of business communication of social media for some periods which has to be adhered to. (Some technical tools are available which often integrate with existing email compliance solutions, can automatically capture social content from both desktops and mobile devices, storing it securely on cloud-based servers).

- **Technical Controls**: Some tools like enterprise social media management systems, allow firms to assign limited permissions to certain employees. Limited users are free to draft tweets and updates, which are then fed into approval queues for manager review. Organisations could also enable web content filtering, which can block all access or allow limited access. Use of Antivirus and Operating system security can provide protection against malware downloads and hacking.

### 2.4.3 Opportunities for CAs

Use of social media has changed the way an organisation functions today as new products are being launched on social media. This could have an important implication for Chartered Accountants in three areas:

- Using Social media for their own professional development.
- Using the power of social media for clients and providing services in development of social media governance and strategy.
- Providing assurance services in reviewing client’s strategy for risk mitigation in use of social media.

Some of the sample areas to consider which could be basis of providing consulting or assurance services from two different perspectives

(1) In respect of an organisation which is using social media for its business,

- Does the organisation strategy outline short, medium and long term goals relating to Social media and how these will be accomplished?
- Has the organisation assessed the different social media channels or Social Collaboration Platforms available and made an informed decision about which channel to focus on platform to adopt?
- Does the organisation’s policy fit into organisation’s culture and can employees understand it?
- Has the organisation ensured that employees understand the needs of the organisation in relation to social media?
- Has the organisation implemented the controls and are they effective?
- Have regulatory and legislative requirements been assessed and considered in internal policies and procedures?
- Has the organisation set out data classification criteria and are there controls established to ensure adherence?
- Have roles and responsibilities been defined and communicated?
- How does the organisation manage its data?
• Does the organisation have a detailed plan in place to deal with crisis related to social media?
• Does the plan identify responsible persons?
• Does it include timescales?

(2) In respect of all other organisations, assess the need to control access by its employees to social media.
• Does the organisation policy address employees’ use of social media?
• How the organisation has trained the employees to use social media responsibly?
• Does the organisation have a plan in place to deal with crisis created by employee use of social media?
• How does the organisation monitor to what is happening in social media outside of its own channels?

2.5 Geolocation

Geolocation refers to the technology that uses data acquired from an individual’s computer or mobile device (any type of radio or network-connection-enabled device) to identify or describe his/her actual physical location. This is one of the most popular usage of the current development of IT. This involves identification of the real-world geographic location of an object, such as a radar, mobile phone or an Internet-connected computer terminal. Geolocation is closely related to the use of positioning systems but can be distinguished from it by a greater emphasis on determining a meaningful location (e.g. a street address) rather than just a set of geographic coordinates.

2.5.1 Benefits of Geolocation

ISACA has published a white paper on “Geo Location: Risk, Issues and Strategies” which has outlined the business benefits and risks of Geolocation and how to implement the right level of governance and control. Mobile Geolocation services have become pervasive in the “always connected” world. They have introduced innovative, profitable and functional services and applications. With location technology, a user’s experience can be uniquely personalized, which appeals to marketers, retailers, government entities, law enforcement, lawyers but it also attracts many criminals. Geo location has far-reaching benefits and are being leveraged by all types of enterprises such as manufacturing, retail sales, financial services, insurance, transportation, utilities and governments. Some of the key business benefits are:
• In advertising, use of designated market areas (DMA) and demographic data
• Know your customer (KYC), e.g., better understanding of customer requirements and expectations for products and services and benefits accruing from targeted sales
• Delivery and asset management, e.g., truck location and manifest status
• Content customization and delivery, such as movies on demand
Module 1: Facilitated e-Learning

- Fine-grained management of Internet commerce activities and interests
- Optimal request routing
- Cloud balancing
- Fraud detection and prevention using IP location technology in conjunction with fraud profile data
- Real-time incident management through Geolocation enrichment of logs and other IT data

2.5.2 Risks and security of Geolocation

Although there are many benefits, the services of Geolocation also increase risk to the user, the service providers and those who utilize the data collected by the service providers. When a user utilizes an application and its services, there may be multiple data controllers: the service provider, wireless access points and/or developers. Multiple data controllers force users to accede control of the systems that determine and store their location and other personal information. Consequently, users usually cannot identify the source and ownership of data collection. This raises several questions of concern for the user, such as how their location data are being used, with whom the data will be shared, whether there will be onward transfer of the data, and the timeline for data retention and destruction.

As the rise in the use of location-aware apps and geo-marketing continue, concerns keep on growing around online privacy and specifically, business practices around the collection and use of the PII data. As the user group grows, continually utilizing new features and creative applications on their smartphones and other mobile devices, the prospect of criminal attacks becomes even more probable and a major cause of concern. The amount and the nature of individual and corporate information available to potential hackers would allow targeted attacks that are difficult to prevent, detect and manage. From social engineering arises the risk of a user being subjected to location-based spamming. IP Geolocation attacks can occur in two ways:

- It identifies the physical location of an organization’s hosted e-mail. The spammer uses this information to plan a targeted attack that will overload the enterprise’s servers, causing usage issues.
- Spamming attacks to an individual’s e-mail or mobile device are targeted and are, therefore, highly effective at soliciting a response acknowledgment from the victim.

Enterprise needs to understand the benefits and risks of Geolocation and harness the power of this technology but ensure that proper controls are implemented. The information Technology Act 2000 as amended in 2008 provides guidelines and stipulations on maintaining privacy of personal and sensitive information. Geo Location involves collection of personal information of the users. Hence, appropriate controls have to be implemented to ensure risks are identified and mitigated.

2.5 Summary

Emerging Technology trends such as BYOD are revolutionising the way organisations work and could have implications in terms of risks and security concerns which have to be mitigated. XML and XBRL
have made sharing of data among different applications easy and efficient. Use of social media provides unprecedented growth opportunities for any organisation but the use has to be controlled through appropriate security and controls so that benefits can be realised. Geo Location provides immense benefits to organisations but has its inherent risks which need to be mitigated by implementing the right level of controls. CAs with good understanding of these emerging technologies in terms of features, benefits, risks and controls can provide innovative IT enabled services of consulting, implementation and assurance services in all these emerging areas.

2.6 References

- http://www.xml.com/
- www.webdeveloper.com/xml/
- http://www.ucc.ie/xml/
- http://www.xbrl.org/
- www.isaca.org/socialmedia.

2.7 Questions

1. Which of the following is not a concern of BYOD?
   A. Reluctance of Employees
   B. Compatibility issues
   C. Reduced IT support requirement
   D. Security Administration issues

2. Which of the following facilitates data exchange and defining of tags?
   A. HTML
   B. Social Media
   C. BYOD
   D. XML

3. In which of the following, is content managed & supplied by user?
   A. XBRL
   B. XML
   C. BYOD
   D. Social Media

4. Social Media benefits both users and marketers because:
   A. it leads to an increase in Internet traffic.
Module 1: Facilitated e-Learning

B. through use of social media marketers will have a more robust online presence.
C. marketers will have monopoly over users.
D. users will have less influence over the marketplace.

5. Which of the following is not an advantage of XBRL?
   A. Accuracy
   B. Speed
   C. Reusability
   D. Taxonomies are always accurate

2.8 Answers

1  C
2  D
3  D
4  B
5  D