Audit, Business Processes and Digitalization [BL 5]

Business Level II | CA Sri Lanka

Study Text

By: M B G Wimalarathna [FCA, FCMA, FMAAT, MCIM, CPFA, CIPFA, MCPM] [MBA (PIM/USJ)]

Contents of the Curriculum

PART C: DIGITALIZATION AND BUSINESS PROCESSES

C.1: Effectiveness of Controls and Digitalization

We understand the role play by internal controls [system] within the organization and level importance of effective internal controls to continue the business operations smoothly and successfully. In modern business era, most of the internal controls and related activities are automated and use advanced technology with digitalization process.

Notes:

Chapter contents

C.1.1. The importance of effective internal controls

Internal controls should be effective and should achieve their control objective

Internal controls are implemented to reduce risks that have been identified. It is important that the controls, taken together, should reduce the residual risk (the risk still remaining after controls are applied) to a tolerable/acceptable level. In other words, internal controls should fulfil the purpose for which they are intended

Internal controls should always be efficient and effective all types & levels

However, there are two main reasons why internal controls may not be effective:

- ❑ They may be badly designed. If they are badly designed, they will not achieve the control purpose (control objective) for which they are intended.
- ❑ They may be well designed, but they may not be implemented properly.

In other words, internal controls may lack design effectiveness or they may lack operating effectiveness

C.1.2. Design effectiveness of internal controls

In general terms, the control objective may be to give a reasonable level of assurance that operations are performed effectively or efficiently and are conducted in accordance with the organization's policies; assets are safeguarded; fraud is prevented or detected; accounting records are complete and reliable; and there is compliance with important laws and regulations

Internal controls should be designed to achieve a specific purpose or control objective. In general terms, the objective of an internal control may be to give a reasonable level of assurance that:

- ❑ Operations are performed effectively or efficiently: controls may be applied to prevent or detect human error in operations, for example, or to reduce the risk of an IT system failure
- ❑ Operations are conducted in accordance with the organization's policies
- ❑ Assets are safeguarded, including information
- ❑ Fraud is prevented, or detected if it occurs
- ❑ Accounting records are complete and reliable
- ❑ There are no misstatements in the financial statements
- ❑ There is appropriate compliance with important laws and regulations

Internal controls are designed by management, although advice may be provided by external or internal auditors

Why might internal controls have ineffective design?

Possible reasons are as follows

Reason for design ineffectiveness	Comment
Risks are not properly assessed.	As a consequence, the need for controls is not recognised.
Risks are recognised for routine operations but not for non-routine situations.	As a consequence, there are no controls to deal with unusual, non-routine circumstances.
Controls are not automated but require response from an individual.	Automated responses are more effective than controls requiring a human response. Humans may fail to identify a risk warning or may be too slow to react.
The control measure is not sufficient to achieve its purpose/objective.	As a consequence, the risk associates are not addressed.

C.1.3. Operating effectiveness of internal controls

Internal controls may be ineffective because they are not implemented, or because there are mistakes with the implementation of controls.

There are inherent limitations in internal controls because of:

- The potential for human error: individuals may forget to carry out a control check, or may perform a control incorrectly
- Collusion between employees
- The possibility that controls may be by-passed or overridden by management
- Software failures in an IT system, or successful hacking of an IT system

A deficiency in internal control exists when:

(a) A control is designed, implemented or operated in such a way that it is unable to prevent, or detect and correct, misstatements in the financial statements on a timely basis; or

(b) A control necessary to prevent, or detect and correct, misstatements in the financial statements on a timely basis is missing (SLAuS 265: para. 6(a)).

A significant deficiency in internal control is a deficiency or combination of deficiencies in internal control that, in the auditor's professional judgment, is of sufficient importance to merit the attention of those charged with governance (SLAuS 265: para. 6(b)).

Internal auditors may investigate business process, with a view to identifying both design failures and operating failures in the application of controls. Internal auditors may investigate for control failures in operations and compliance, as well as in the accounting system

C.1.4. Internal control questionnaires (ICQs)

Internal control questionnaires and internal control evaluation questionnaires are documents that may be used when investigating the effectiveness of internal controls

To help them identify weaknesses in the design of internal controls, external and internal auditors may use internal control questionnaires (ICQs).

The major question that questionnaires are designed to answer is: how good is the system of controls?

An ICQ consists of a list of questions that are designed to determine whether suitable controls are present. There should be a questionnaire for each different business process or transaction cycle

The ICQ questions below dealing with goods inwards provide additional illustrations of the ICQ approach

Goods received

(a) Are supplies examined on delivery to check for quantity and quality?

(b) Is there documentary evidence of this examination of goods?

(c) Is the receipt of supplies recorded by means of goods received notes?

(d) Are records of goods received prepared by a person independent of those responsible for:

(i) Ordering functions?

(ii) The processing and recording of invoices?

e) Are goods received records controlled to ensure that invoices are obtained for all goods received?

(f) (i) Are goods received records regularly reviewed for items for which no invoices have been received?

(ii) Are such items investigated?

C.1.5. Internal control evaluation questionnaires (ICEQs)

Auditors may also use internal control evaluation questionnaires (ICEQs). These are used to assess whether specific errors (or fraud) are possible, rather than establishing whether appropriately designed controls exist

Internal control evaluation questionnaire: control questions

The procurement cycle

Is there reasonable assurance that:

(a) Goods could not be received without a liability being recorded?

(b) Receipt of goods is required in order to establish a liability?

(c) A liability will be recorded:

(i) Only for authorized items?

(ii) At the proper amount?

(d) All payments are properly authorized?

(e) All credits due from suppliers are received?

(f) All transactions are properly accounted for?

(g) Unauthorized cash payments could not be made to a supplier?

C.1.6. Controls in IT systems: general controls and application controls

There are many controls in IT systems. These consist of general controls and controls for specific IT applications. Many application controls are written into application software

Many business processes involve IT systems, and it is therefore essential that controls within IT systems should provide reasonable assurance against operational failures

General IT controls are policies and procedures that relate to many different IT applications within the organization. General controls support the effective functioning of application controls. They commonly include controls over:

- ✓ Operations in IT centers and network operations
- ✓ System software acquisition
- ✓ Changes to an IT system and system maintenance
- ✓ Access security
- ✓ General rules and procedures for the acquisition, development and maintenance of application
  IT systems

Application IT controls are procedures that operate mostly at a business process level. They are preventative or detective controls designed to ensure the integrity of the data and records in the system. Accordingly, they relate to procedures (both manual and computerized procedures) that are used to initiate, record, process and report transactions

C.1.7. General IT controls

GENERAL CONTROLS	EXAMPLES
Development of computer applications	**Standards** over systems design, programming and documentation Full **testing procedures** using test data, to be applied to all new application systems **Approval** of new applications by computer users and management **Segregation of duties** so that those responsible for design of a new application are not also responsible for testing **Installation procedures** so that data is not corrupted in transition **Training** of staff in new procedures, and availability of adequate **documentation**
Prevention or detection of unauthorised changes to programmes	**Segregation of duties** **Full records** of programme changes **Password protection** of programmes so that access is limited to computer operations staff **Restricted access** to central computer by locked doors and keypads Maintenance of **programmes logs** **Virus checks** on software: use of anti-virus software and policy prohibiting use of non-authorised programmes or files **Back-up copies** of programmes being taken and stored in other locations **Control copies** of programmes being preserved and regularly compared with actual programmes **Stricter controls** over certain programmes (utility programmes) by use of **read-only memory**

GENERAL CONTROLS	EXAMPLES
Testing and documentation of programme changes	Complete **testing procedures for changes** to any software **Documentation** of changes **Approval** of changes by computer users and management **Training** of staff using programmes
Controls to prevent wrong programmes or files being used	**Operation controls** over programmes **Libraries** of programmes **Proper job scheduling**
Controls to prevent unauthorised amendments to data files	**Password protection** **Restricted access** to authorised users only
Controls to ensure continuity of operation	Storing **extra copies** of programmes and data files off-site **Protection of equipment** against fire and other hazards **Back-up power sources** **Disaster recovery procedures,** eg availability of back-up computer facilities **Maintenance agreements** and **insurance**

C.1.8. Application IT controls

Application controls in IT systems are controls that operate at a business process level. They can be preventive or detective in nature and are designed to ensure the integrity of the IT records

The purpose of application controls is to establish specific control procedures over IT processing. In an IT system for processing transactions, application controls are designed to provide reasonable assurance that all transactions are authorized and recorded, and are processed completely, accurately and on a timely basis

APPLICATION CONTROLS	EXAMPLES
Controls over **input: completeness**	**One-for-one checking** of processed output to source documents **Programmed matching** of input to an expected input control file **Procedures** regarding submission of rejected items
Controls over **input: accuracy**	**Programmes to check data** fields (for example value, reference number and date) in input transactions for plausibility: • Digit verification (eg identity codes or reference numbers are as expected) • Reasonableness test (eg reasonable ratio of sales tax to total value) • Existence checks (eg checks on existence of customer name or existence of a code for an item of data) • Character checks (no unexpected characters used in an item) • Necessary information all entered in the transaction • Permitted range (no transaction processed over or under a certain value) • Agreement of **control totals** (manual/programmed)
Controls over **input authorisation:**	**Manual checks** to ensure information input was: • Authorised • Input by authorised personnel
Controls over **processing**	**Screen warnings** can prevent people logging out before processing is complete

C.1.9. Deficiencies in internal controls

Deficiencies in internal controls vary in significance. The significance of a control deficiency depends on the possible consequences of an operational risk event happening, that should have been prevented by internal control measures

The significance of a deficiency in internal control in a business process depends on the possible consequences of a control failure. What could happen as a consequence of a control failure in the event that a risk event occurs? A significant deficiency exists when the adverse consequences could be serious.

A failure in control is not itself the main problem. The main problem is that a failure in control could result in an operational risk event leading to losses (or other adverse consequences) for the organization

C.1.10. Mitigating controls

An internal control system may also include some mitigating controls.

A mitigating control is a control that is designed to discover (or prevent) failures in controls, and to correct them before the control failure has serious consequences

For example, an organization may have a master file of approved suppliers on an IT system. There should be controls over procedures for updating the details of suppliers on this file. However, there will be some risk that, due to error or fraud, unauthorized changes are made to the file.

A mitigating control might be to check an audit trail produced by the IT system which provides a record of all the changes that have been made to the supplier file in a given period of time. Checks on this list should reveal any unauthorized changes that have been made

C.1.11. Digitalization

Digitalization is rapidly changing the way in which the financial services sector and businesses are operating. New applications of digital financial technology, often collectively abbreviated to FinTech, are being used to transform the way consumers and service providers interact

FinTech

FinTech is now evolving to represent technologies that are disrupting traditional financial services, including mobile payments, money transfers and loans. Because all businesses of all sizes will deal with the financial services industry, all businesses are affected.

The best way to demonstrate the rapid increase in FinTech is to look at some examples

Mobile banking
Mobile banking is a well-known and large part of FinTech industry. Businesses and their staff have digital access to their bank accounts on computers, tablets and mobile phones. Almost all major banks offer mobile banking and a number of banks have emerged where everything is done online and there are no physical branches.
Payments
Payment companies have changed the way business is carried out. FinTech has made it much simpler to send and received money digitally anywhere in the world, no matter what the size of business. For example, tools like PayPal allow businesses to accept credit and debit cards and there is no minimum a particular volume of business required in order to qualify for an account.
Lending and borrowing
FinTech has changed provision of credit (loans) by speeding up risk assessment and the approval process. Businesses can apply for a loan on their mobile devices, and improved risk modelling is expanding global access to credit. Consumers can request credit reports numerous times without affecting their credit score, which increases transparency. Additionally, some lenders can use cloud accounting software's application programming interface (API) to directly access and interrogate a business's accounting data to make business lending decisions quickly and digitally.
Investments
FinTech has caused a huge increase in the number of investing and savings applications (or apps) available. Even very small amounts can be invested, increasing access to a wide range of consumers and making it easier to invest.

Digital currency
Digital currency is an intangible payment method which exists only in electronic form. **Cryptocurrency** is a type of digital currency which can be transferred between businesses with the help of FinTech and allows transactions to occur instantly. Cryptocurrencies such as BitCoin can be used to purchase goods and services and the benefits associated with digital currencies include lower transaction costs and business are able to proceed without needing to use intermediaries. There is, however, a security risk associated with holding purely electronic currency and the tax and regulatory system for this is yet to be fully established. Cryptocurrency is underpinned by **block chain technology**

Block chain technology

A block chain is an increasing collection of records (made up of 'blocks') that can be distributed but not copied or altered

The advantages of block chain are considered to include:

- Items of value or data can be transferred anonymously and globally from one party to another. It eliminates intermediaries.
- It offers transparency when dealing in currency because block chains are viewable by the public, unlike other currency types
- Block chain transactions simplify processes as they are part of a single public ledger rather than multiple ledgers which may be subject to different accounting rules

Block chain and auditing

Block chain may be used as an alternative source of verification compared to the more traditional methods. Auditors will be able to verify the transactions on publicly available block chain ledgers rather than request copies of bank statements. The automation of this verification process should bring cost efficiencies to the audit

Instead of using sampling in some areas, auditors could potentially use block chain technology to test entire populations of transactions for the year. This could lead to increased levels of assurance

Information technology and data analysis

Organizations today have more transactional data than they have ever had before, about their customers, suppliers and their operations. The ability to capture and store all of this data has been made possible by advances in information technology.

The growth of the internet, multimedia, wireless networks, smartphones, social media, sensors and other digital technology are all helping to fuel a data revolution. In the so-called 'Internet of Things', sensors embedded in physical objects such as mobile phones, motor vehicles, smart energy meters, RFID tags and tracking devices all create and communicate data which is shared across wired and wireless networks that function in a similar way to the internet

Data analytics

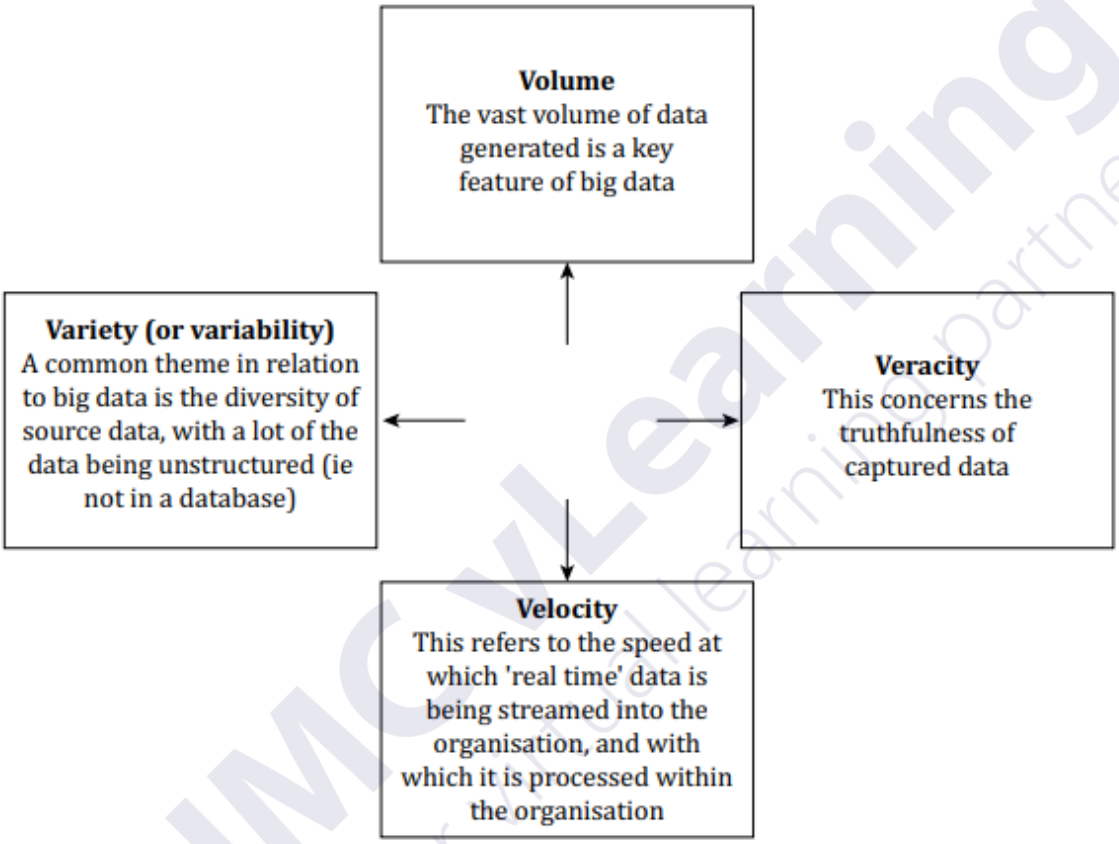
Data analytics is the examination of data to try to identify patterns, trends or correlations

It is important to note that data on its own is useless unless it can be analyzed in some way. Data analytics is the examination of data to try to identify patterns, trends or correlations. As the quantity of data has increased, it has become more and more necessary to evolve ways of processing and

making sense of it. The aim of data analytics software is to extract insights from unstructured data or from large volumes of data

Big Data

Big Data is a broad term for the larger, more complex datasets that can be held by modern computers. The term refers to a shift in the amount of data that is available in comparison with the past



Opportunities and threats of Big Data

Big Data presents organizations with significant opportunities but these need to be matched against the threats posed by its use

Opportunities offered by Big Data to organisations	Threats associated with Big Data
Processing greater quantities of data should allow organisations to **identify new trends and patterns** relevant to the organisation's success. Patterns may give deeper understanding of customer requirements. Data can be captured from both internal and external sources to reveal insights not previously known. For example, as more customers use the internet, smartphones and social media in their everyday lives, these can now also be sources of data for organisations alongside any data they may capture internally – for example, from customer loyalty cards or the transactions recorded in EPOS tills.	Capturing and storing greater quantities of data increases the scope for things to go wrong. Attempts by **hackers** to access organisational data sets are on the increase as such groups look to exploit the value of the data held. The widespread use of IT infrastructures in capturing and storing data in digital form presents a challenge in keeping it safe from the threats posed by computer **viruses**. This is a significant threat for those organisations whose business model is heavily dependent on transferring data over the internet, such as an online retailer. Viruses which **corrupt** organisational data may potentially have a devastating impact. The threats posed by hackers and viruses raise legal considerations, especially if stolen or corrupted data relates to individual consumers. The organisation may **face legal action** if it is found that its measures for protecting data were not deemed sufficient.

Opportunities offered by Big Data to organisations	Threats associated with Big Data
The ability to process large data sets in real time allows organisations to **respond to changing conditions faster**. For example, online retailers are able to compile records of each click and interaction a customer makes while visiting a website, rather than simply recording the final sale at the end of a customer transaction. Moreover, retailers who are able to utilise information about customer clicks and interactions quickly – for example, by recommending additional purchases – can use this speed to generate **competitive advantage**.	The use of Big Data increases the danger that an organisation's management spends longer trying to determine the value and patterns within the vast amounts of data they have captured, instead of concentrating on running the organisation. The possession of lots of data **does not guarantee** that its analysis will identify any trends or patterns of any commercial use. Furthermore, there is a focus on finding correlations between data sets and **less of an emphasis on causation**. Critics suggest that it is easier to identify correlations between two variables than to determine what is actually causing the correlation.
Organisations increasingly have access to more diverse types of data. Historically data has tended to be in structured form (ie can be stored in databases), however there has been a growth in **unstructured data** (ie not in a database) which organisations have access to. For example, keywords from conversations people have on Facebook or Twitter and content which they share through media files (tagged photographs, or online video postings) could be sources of unstructured data. Such data provides organisations with a range of **new opportunities**, including understanding what customers are saying about the organisation's products and services and monitoring consumer reactions to competitor's products.	The diverse types of data available present a challenge to organisations as they need to find ways of capturing, storing and processing the data. If data is too big, moves too fast, or doesn't fit within an organisation's existing information systems then, in order to gain value from it, an organisation needs to find an alternative way to process that data. As a result organisations may feel compelled to invest in upgrading their IT infrastructures to capture and store more data, even if **the benefits of such an approach have not been fully considered**. The **technical and financial costs** imposed by regularly upgrading the organisation's hardware may be prohibitive for smaller organisations.

Artificial intelligence and automation

Artificial intelligence is when computer systems perform tasks that would usually require human intelligence

Artificial intelligence (AI) takes things a step further on from data analytics. This is when computer systems perform tasks that would usually require human intelligence. In order to perform these tasks, the computer essentially needs to 'learn'

Machine learning is the construction of AI algorithms that learns from a series of inputs and outputs. As a result of this 'learning' a final algorithm is generated that can predict an answer when provided with input

There are numerous examples of AI being used in business and everyday life including:

- ✓ Sales and business forecasting
- ✓ Analysis of transactions and data from numerous sources
- ✓ Smart personal assistants (for example Siri, Cortana and Alexa)
- ✓ Process automation:
- ✓ Email spam filters which block emails or divert them
- ✓ Voice to text software
- ✓ Automated responders and online customer support
- ✓ Automated insights, especially for data-driven industries (eg financial services or e-commerce)
- ✓ Fraud detection and prevention for online transactions
- ✓ Dynamic price optimization (based on machine learning)
- ✓ Robotic Process Automation (RPA) (covered in the next section)

Robotic process automation

Robotic process automation (RPA) is the use of AI to handle high-volume, repetitive tasks that humans would previously have performed such as calculations, queries and maintenance of records or transactions

Robotic Process Automation (RPA) uses software (often referred to as 'robots' or 'bots') to capture, learn from and then mimic the way humans use and enter data to applications. RPA is best suited for processes with repeatable, predictable tasks carried out in IT applications

Accounting
Companies can use RPA for general ledger entry, budgeting and transactional reporting.
Financial services
RPA can be used for foreign exchange payments or processing insurance claims.
Human resources
RPA can automate certain HR tasks such as updating employee data and timesheet related tasks.
Procurement and supply chain management
RPA can be used to automate order processing, payments, and to monitor inventory levels.

RPA and auditing

RPA can be used to assist both internal and external auditors. Areas to which it could be applied:

- ✓ Data gathering, including extracting the data to be used by auditors.
- ✓ Automation of the risk assessment process.
- ✓ Sampling and initial evidence gathering for standard evidence for controls
- ✓ Bots can run controls testing for control areas that are standardized

Cybersecurity

Cybersecurity is concerned with the protection of systems, networks and data in cyberspace. Cyberspace is the environment in which communication over IT networks takes place

The frequency of 'cyber attacks' on the IT systems used by organizations is continuing to rise at an alarming rate and has highlighted the need for improved cybersecurity. The increased emphasis on cybersecurity requires organizations to change their approach to protecting data and the steps that must be taken in the event that their data is breached

However, cybersecurity measures increasingly need to take account of the external threats:

- ❑ Threats now emerge from different parts of the world, and often involve criminal groups, corporate espionage and hackers.
- ❑ 'Phishing' emails may be used to attract people to visit a website where they are asked to update secure information, such as a passwords, credit card details, social security details, or bank account numbers, that the legitimate organization already has.
- ❑ The heavy dependence on IT systems in modern business has proliferated the need for organizations to link their IT systems together throughout their supply chains. The growing number of servers, mobile devices and cloud computing applications which are used increases the number of ways in which hackers can gain access to data.
- ❑ Security failures can have far wider implications than only affecting the organization's IT systems; these may include reputation damage, loss of intellectual property and disruption to operations

To address the challenges presented by such threats senior management are having to do more to promote an awareness of cybersecurity throughout the organization. This may involve:

- ❑ Making cybersecurity issues for those not working in the organization's IT department easier to understand. All too often the language used among IT professionals is of a technical nature, which makes it harder for other employees to understand. Communicating the need for all employees to play their part in combating cyber risks is crucial.
- ❑ Employing a Chief Information Security Officer to help communicate the threats posed by cyber risks should help other employees understand their role when using the organization's IT/IS infrastructure.
- ❑ Reorganizing roles and responsibilities to ensure that there is accountability for cybersecurity matters within the organization. This should help ensure that in the event of

a cyber-attack there is a team of individuals with the required responsibility to address the matter.

- Determining accountability for cyber risks at the strategic apex. A member of the board should be assigned responsibility for heading up cybersecurity matters. Having a member of the board in this role should help promote 'buy in' among all employees that the senior management take the issue seriously. This should help to create a cybersecurity-conscious culture.
- Learning from past security breaches. Following a security breach, senior management should use this as an opportunity to promote the importance of cybersecurity throughout the organization and should look to put in place measures to address the weaknesses that permitted security breaches to occur in the past.
- Determining the organization's tolerance to the cyber risks is an important step in designing management strategies. Such an exercise may lead to the conclusion that additional funding is required to enhance the cybersecurity features of the organization's IT/IS infrastructure.
- Ensuring that non-executive board members play an active role in promoting cybersecurity during their interactions with the board. This may involve keeping their knowledge about the evolving nature of cyber risks up to date and challenging the executive directors about the need for following best practice in cybersecurity

Chapter review questions

1. Inventory controls may lack _____ effectiveness and _____ effectiveness

2. What are the consequences of an ineffective internal control?

3. List three inherent weaknesses in internal controls

4. Documents that may be used to help with identifying weaknesses in internal controls are an _____ and an _____

5. Who may advise about weaknesses in internal controls?

6. Which one of the following is an IT application control?
   A. Password protection for access to a computer system
   B. Keeping back-up copies of files on a cloud computing system
   C. Testing all new applications software before its operational implementation
   D. Identity code verification for input data records to an IT system

7. Which of the following best describes Robotic process automation
   A. The environment in which communication over IT networks takes place
   B. The examination of data to try to identify patterns, trends or correlations
   C. New applications of digital financial technology
   D. The use of AI to perform repetitive tasks that humans would previously have performed

8. Which 4 V's can be used to define Big Data?