# IT Questions (Audit and Assurance)

Chartered Professional Accountants of Canada, CPA Canada, CPA
are trademarks and/or certification marks of the Chartered Professional Accountants of Canada.
© 2019, Chartered Professional Accountants of Canada. All Rights Reserved.
2021-04-19

# IT QUESTIONS (AUDIT AND ASSURANCE)

## Question 1

eShop.com is an online retailer of custom printed material, including stationery, corporate swag, and novelty items. Customers must create an account within the eShop platform, and all orders must be paid for by credit card. Credit card information is gathered at the time the order is placed, but the cardholder is not charged until the order has shipped.

eShop is planning to purchase a new accounting system, as it has outgrown the capabilities of the existing one. The managing director has asked for your advice on certain matters relating to the new computerized sales system.

The old system required AR clerks to produce sales invoices from shipping documents (usually emailed or faxed by a shipper), post them to the sales ledger, record payments received, and produce an aged analysis of accounts receivable (for orders where the credit card was rejected). The main weaknesses of the old system were that many documents, such as order confirmations or shipping notes, were either produced irregularly or contained errors.

With the new computerized sales system, the following is proposed:

- The customer sales order confirmation would be produced by eShop's online order platform, and transmitted directly to the sales system (no human processing).
- The production team accesses the order confirmations in the sales system to begin production.
- Once the goods have been printed and scanned into inventory, a delivery notification will be produced to say the goods are ready for shipment. This delivery notification will be sent to the shipping department, with a copy sent to the accounting department.
- Using the delivery notification, eShop's shipping department will prepare the goods for shipment, using the customer's preferred delivery method. The shipping department will prepare the shipping document using the new accounting system. The sales invoice will be produced by the system at the same time as the shipping document, using the information from the shipping document and prices per unit from a standing-data file. When the computer produces the sales invoice, it posts it to the sales ledger.
- After the shipping document and invoice have been produced, the customer's credit card will be charged.
- Receipt of payment from customers will be recorded on the sales ledger and in the cash receipts/disbursements journal in a similar way to the old system.

- Controls over access to the system will be by passwords and by restricting which individuals can perform certain tasks.

In view of the large number of shipments of goods to customers, the managing director wants to safeguard against credit card fraud, using as many automated controls as possible. When the computer system determines that goods should not be shipped to a customer due to a flagged fraud risk, the system will have a provision that allows the eShop's controller to manually override this decision and authorize shipment of goods to the customer.

The managing director has asked you to provide details of controls that should be implemented for the following:

1. prior to the system issuing a sales order confirmation to the customer
2. prior to the shipment of goods to the customer
3. when changes are made to customer details
4. when selling prices of products are changed

Finally, the managing director has asked what credit card fraud prevention criteria should be programmed into the system to prevent shipment of goods to fraudulent customers, and what manual procedures should be implemented to override these criteria.

**Required:**

Prepare a report for the managing director recommending the controls that should be implemented in the new computerized sales system.

**Question 2**

You are the auditor of Decora Inc, which sources home décor products from a variety of manufacturers and sells to the general public via several locations across the country.

The company comprises a corporate head office, a central warehouse, and eight shops throughout the country. Merchandise is received from manufacturers either at the individual shops or at the central warehouse. Details of the goods received are entered into the accounting system either at the shop or at the central warehouse.

The computerized purchases system operates as follows:

1. The user department (that is, the shop or central warehouse) issues a purchase requisition and sends it to the purchasing department at head office.
2. The purchasing department issues a purchase order, which it sends to the supplier, and it logs the order in the computer system.

3. When the goods are received by Decora (in the shop or at the central warehouse), they are checked and a receiving report is issued by the warehouse/receiving department. Details of the goods received are entered into the computer system and matched against the purchase order.
4. The financial accounting department at head office receives the purchase invoice. This is sent to the user department, which authorizes it and returns it to the financial accounting department. The financial accounting department enters the purchase invoice details into the system, which posts the invoice to the purchase ledger.
5. The computer system allows payment of the invoice only if the details agree to the purchase order in step 2 above and the receipt of the goods in step 3 above.
6. When the purchase invoice is due for payment, the computer prints the cheques and remittance notices to the suppliers.

Cheques are automatically produced at the due date after the purchase invoice has been posted to the purchase ledger.

The partner in charge of the audit has asked you to identify the controls over authorizing purchase invoices and changing suppliers' details on the computer's standing-data file. He has explained that "application controls" comprise processes exercised by the company's staff and by the computer system.

**Required:**

Prepare a memo to the audit partner discussing the following:

- the various application controls you would expect to see in operation from generating the purchase requisition to the system accepting the purchase invoice
- the various controls that should be exercised over access to the system from computers in the corporate head office and in the shops
- the various application controls that should be exercised over changing supplier details on the standing-data file on the computer, and why it is important that there should be strong controls over changing supplier details

## Question 3

The accounts payable clerk can enter a new vendor into the purchasing system and process payments. This presents doubts over the segregation of duties of a specific management role.

**Required:**

What risk to the company arises from this, and what should ideally be in place in terms of compensating controls?

## Question 4

A company has the following IT general controls:

*Access control:*

- All users have unique usernames and there are strong password controls in place, including the following:
  - minimum length of eight characters
  - alphanumeric requirement
  - no reuse of previous password
  - expiry period of 30 days

*System development control:*

- An appropriate project/program management policy is in place and is followed to ensure that the requirements for the system are appropriately captured and delivered as part of the development of the new system (the system performs its operations as expected).

*System change control:*

- System changes are authorized, tested in a controlled test environment and migrated into the live environment by an independent staff member.

*System backup and recovery control*:

- System and data backups are run every night and stored in an off-site location. Backups are recovered weekly in the test environment.

**Required:**

Outline the audit procedures that you would perform to test the design and operating effectiveness of these IT general controls.

## Question 5

What is the “data life cycle?” What happens at each stage?

## Solutions

### Solution to Question 1

### Report

**Date:** January 20, 2020
**To**: Managing director
**From:** CPA
**Subject:** Issues affecting the control of the accounting system of eShop.com

**Private and confidential**

**Index**

A. Introduction
B. Proposed controls to be implemented within the sales accounting system
C. Credit card fraud prevention and related management override procedures

**A. Introduction**

This report addresses the control procedures and related management override procedures that should be implemented in relation to the new accounting system at eShop.com

This report has been based upon information that has been provided by the managing director.

The information contained in this report is for the sole use of the managing director and eShop.com, and should not be relied upon by any other party without our prior written consent.

**B. Proposed controls to be implemented within the sales accounting system**

The following stages of the sales accounting system have been identified:

1. issuance of sales order confirmation to the customer
2. shipping authorization and procedures
3. changes to customer details
4. changes to selling prices of products

Controls for each stage have been identified in the subsequent paragraphs.

### *1. Computer issuance of sales order confirmation to the customer*

Prior to issuance of a sales order confirmation, the following controls should be implemented to prevent issuance of sales order confirmations for inaccurate, unwanted, or fictional orders that have been taken from unauthorized or fictional customers:

a) a check to ensure that the customer has provided a valid shipping address

b) a check to ensure that the customer has provided a valid credit card number for processing

c) a check that the product requested in the sales order is a recognized current inventory item in eShop's inventory listing and that there is sufficient inventory available at the company's warehouse to meet the order quantity requirements within the time frame required by the sales order

d) a check that the price of the product listed in the sales order agrees to the current standard selling price of that product, and any discounts or exceptions are agreed to the customer account details and/or current promotions

e) sales orders should be standardized documents that are prenumbered sequentially to allow sales staff to identify missing orders and to prevent duplication of orders

f) a management override function should be available for rejected sales orders (password-controlled function); any use of such a function should be monitored through the timely review of automatically generated exception reports, detailing the user responsible for the override and when it occurred, by senior sales staff

### *2. Shipping authorization and procedures*

Prior to the automated generation of a delivery notification and the authorization of the shipment of goods to customers, the controls noted below should be implemented to ensure the following:

- Goods are only shipped to genuine customers.
- Goods shipped relate to a genuine order.
- Goods shipped are of the quality and quantity required by the order.
- Shipment of the goods takes place on a timely basis in accordance with the order requirements.

*Control procedures*

- Orders are filled and goods released to the shipping department by the production staff only when a sales order is received from the sales team (via the new accounting system).
- Segregation of duties should be implemented so that different staff are responsible for custody of inventory (production team), shipment of goods (shipping team), and updating of inventory records.

- The shipping team does not accept the filled orders from the warehouse production team unless the goods received from the warehouse match the related sales order in both quantity and quality.
- The details to be shown on the delivery notification should be agreed to those shown on the sales order (including inventory quantity, delivery address, and delivery date).
- Delivery notifications are sequentially prenumbered documents generated by the system to ensure that shipments are complete and are not duplicated.
- The shipping team does not ship the orders unless it has a matching approved sales order and delivery notification with a corresponding shipment date that agrees to the proposed date of shipment.
- The shipping team does not ship the orders unless the customer's credit card information has been verified (see additional discussion below on verification procedures).
- The inventory records should not be updated unless there is a matching approved sales order, completed delivery notification, and shipping document.
- Exception reports detailing occurrences of the following are automatically produced and reviewed on a timely basis to ensure that orders are not remaining unfulfilled and unauthorized shipments are identified and investigated:
    - sales orders that remain unmatched after the order delivery due date
    - unmatched delivery notifications
    - unmatched shipping documents

*Alterations to standing data*

The controls identified below relating to the alteration of customer details (see part 3) and selling prices of products (see part 4) should be implemented to ensure that standing data is altered only by authorized individuals who are sufficiently experienced and that the alterations made are accurate, genuine, complete, and timely.

The following controls should be implemented regarding all alterations to standing data, and are relevant to changes to customer details and selling prices of products:

- Password controls (relating to both the computers and the sales accounting program) and use of authorization tables that determine users' rights should be used to ensure only authorized individuals have edit access to the standing-data files.
- A separate password authorization control should be put in place to the confirm changes made to the customer or selling-price master file prior to the computer system updating the entry.
- Passwords should be created to allow access and confirm changes are only provided to the relevant authorized individuals permitted to update the customer or selling-price master files.

- All amendments, additions, and deletions to the data should be authorized by a responsible official (such as a sales manager), and a pro-forma document should be used to evidence such authorization.
- Amendment forms should be entered in batches with different categories of changes being entered in different batches. The batches should be sequentially numbered and recorded in a batch control book so that any gaps in the batch numbers can be investigated. The output produced by the computer should be checked to the input.
- The system should automatically generate a log of historic changes to master data files that outline which user made the changes and when the changes were made.
- The log of historic changes should be regularly reviewed by senior sales personnel to ensure that changes have been made accurately and completely, and documentary evidence of the review should be retained.
- Periodic checks to the master data file to ensure its integrity should be made; a detailed review of either the complete listing of the file or portions should be made to ensure the accuracy and completeness of the listings. Customer/sales documents (such as invoices and statements) can be used to validate the details held on file.

### *3. Changes to customer details*

Changes to customer master data could occur as a result of changes to current customer accounts, opening of new customer accounts, or closure of customer accounts. The following controls should be implemented in addition to those noted above:

- Management should implement procedures to detail the information that the customer must provide in order for a change to be made to the customer standing data, through the customer's online account. Management should ensure that staff are sufficiently trained in the procedure. An email or telephone call made to the customer in response to the request to confirm its validity prior to update can provide an extra level of control over the process. All documents relating to a customer request to update master data details should be retained on the relevant customer record.
- Where the change relates to the setting up of a new customer account, there should be a pro-forma application document that prospective customers complete to ensure that all information necessary is obtained to set up a new customer account. Critical fields should be marked as required. Without these fields completed, the new account cannot be created.
- All changes, as noted above, should be authorized by a responsible official (such as the sales manager), and a standardized pro-forma form should be used to evidence the authorization.

### *4. Changes to selling prices of products*

The risk of not implementing adequate selling-price change controls is that sales could be made at incorrect prices, which may adversely impact the company's profit margins or become a source of dispute with customers. In addition to the general standing-data controls, the following specific procedures should be implemented:

- Pro-forma authorization input forms should be completed to evidence changes to selling-price standing data.
- The pro-forma input forms should be authorized by the sales director prior to input.
- An exception report detailing unchanged sales prices should be provided to ensure that the update of selling prices is complete.

## C. Credit card fraud prevention and related management override procedures

The following credit card fraud prevention controls should be programmed into the computer system to prevent shipment of goods to fraudulent customers or fraudulent charges applied to customer credit cards:

*Fraudulent shipment of goods*

Almost all credit cards provide the following automated screening tools for card-not-present transactions:

- address verification services
- card verification number (a three-digit security number printed on the back of credit cards to help validate that a customer is in possession of the card at the time of an order)
- postal address validation services

Using some (or all of these) will help validate that the customer physically possesses the card and that the shipping address is the same as the billing address noted on the cardholder's credit account.

Do not accept any transaction that has been declined by the credit card's automated processes.

Additional security checks can be completed in house for higher-dollar orders by eShop staff, such as:

- two-factor phone authentication (order confirmation by phone)
- Google Maps lookup, to verify the address provided
- telephone number verification or reverse lookup, to verify the contact information provided

- maintaining key attributes of previously identified fraudulent transactions, including:
  - IP address
  - cardholder name
  - phone number
  - email address
  - shipping address
  - social networking sites, to verify the name/address of the information provided
  - credit history checks

*Fraudulent charges applied to customer credit cards*

- Limit access to system components and cardholder data to only those individuals whose job requires such access.
- Formalize an access control policy that includes a list of who gets access to specified cardholder data and systems.
- Deny all access to anyone who is not specifically allowed to access cardholder data.
- Employ at least one of these to authenticate all users: something you know, such as a password or passphrase; something you have, such as a token device or smart card; or something you are, such as a biometric. Use strong authentication methods and render all passwords/passphrases unreadable during transmission and storage using strong cryptography.

***Manual override procedures***

The system should retain a function that allows management to override the computer evaluation of the customer account where there are valid reasons for breach of credit card control criteria. Reasons for which management should be permitted to use the override function on an account that was deemed suspicious by the system should be outlined in the company's sales procedures and will include the following situations:

- where additional verification procedures have been satisfactorily completed
- where refunds were processed in error

The management override function should only be available to individuals of sufficient expertise and seniority. The credit controller is a suitable candidate to be given override responsibilities. A pro-forma document to evidence the reasons for the override should be completed and authorized prior to the action being undertaken.

Note that the system should maintain an exception report of all occurrences of management override (including who initiated the override procedure and when). Timely review of the exception report by a sufficiently senior member of the sales team should

be undertaken to ensure that the override function is being used appropriately and according to company procedure.

**Solution to Question 2**

**Memorandum**

**Date:** January 15, 2020
**To:** Audit partner
**From:** CPA
**Subject:** Decora Inc. — purchase systems controls

Decora Inc. has a good process flow for its purchases. It does, however, need to review the controls at each step of the process. Below are some indicators and examples of key application and general controls that Decora must consider or strengthen.

**Application controls relating to generating purchase requisitions and accepting the purchase invoice**

The main risk in relation to purchase orders is that unauthorized orders can be made that result in unnecessary expenditures and the acquisition of unwanted goods or services. Application controls should be put in place to ensure that this risk is mitigated. The following application controls would be expected to be in operation in the stages of the purchase cycle from generating the purchase requisition to the computer accepting the purchase invoice. These may be considered to be parts of a vendor management system that Decora would need to manage its purchasing process effectively:

1. Controls for segregation of duties should be put in place to ensure that generating purchase requisitions and purchase orders is undertaken by separate individuals. This will prevent fraudulent orders being placed because it ensures that employees are not able to initiate unauthorized purchases. This will also improve the efficiency of the purchasing process through the centralization of purchasing in the purchasing department. This control does appear to be in place at Decora because the user department initiates the requisition and the purchasing department issues a purchase order.
2. Purchase requisition forms should be prepared in a sequentially prenumbered, electronic standardized format and should be completed by the user department. An alphabetic prefix to the number would allow easy identification of the relevant department. The requisition should be authorized by the individual in the department with budgetary responsibility, prior to transmission to the purchasing department. A copy of the purchase requisition should remain within the relevant department. It is not clear whether purchase requisitions are currently serially numbered and tracked. These controls must be put in place at Decora to ensure that all purchase requisitions are appropriately issued.

3. The purchasing department should generate a purchase order only on receipt of a properly approved and complete purchase requisition form. The purchasing department should also have a formal list of the individuals within each department who have appropriate requisitioning authority and their related purchase authorization limits. The department should ensure that each requisition has been approved in accordance with this listing. Although it is mentioned that the user department issues the purchase requisition, it is unclear whether the purchase requisition is required to be appropriately authorized before being sent to the purchase department.
4. The purchasing department should have an approved list of merchandise suppliers from whom purchases may be ordered. Ideally this list should be programmed into the purchasing system so that when electronically generating an order, the system can be programmed to identify when unapproved suppliers are entered. Presently, we do not know if any such approved list of vendors exists at Decora. Decora must use this as an opportunity to assess vendors using metrics that are key to Decora's objectives.
5. There should be a standard list of negotiated prices for routine purchases. This would also be part of the vendor assessment referred to above.
6. The purchasing department should ensure that the purchase orders contain a precise description of the goods and services required and information including quantities, price, delivery instructions, and the supplier's name and address. The purchase order should be an electronic pro-forma document that is sequentially prenumbered to allow the team to identify omissions and prevent duplicate purchase orders being made. A pro-forma document is used to ensure that the order information is complete. The accounting program should be able to identify certain types of errors in the purchase order (such as unauthorized suppliers or delivery addresses) and cause the order to be blocked until authorization is obtained from a senior member of the purchasing department (by entering an override password). In addition, this process could be used to highlight high-value purchase orders (such as capital items) that require additional authorization.
7. Prior to release, the purchase order must be approved by an authorized purchasing department official. This could be done either via authorization password on the computer or, for hard-copy forms, with a signature. The purchasing department should have an approved signatory listing with authorization limits for each individual. Where electronic authorization is implemented, the formal authorization listing could be incorporated into the purchases order system so that the computer can automatically stop a user from authorizing a purchase outside their official limit.
8. Once the purchase order is authorized, copies of the purchase order should be sent to the supplier, the warehouse/receiving department, the financial accounting department, and the originating department.

## General controls relating to control of access to the main computer

Decora must control the access to its computer hardware, which in turn entails controlling access to the company software, programs, and data. General IT controls relating to access to the computer environment fall into two broad categories:

- physical access controls
- logical access controls

### *Physical access controls*

Decora must physically restrict access to the computer area and programs by locating the computers in secure areas (such as a dedicated room with permissible access via a physical key and/or password-driven keypad locks). Where a separate secure area is not available, the computer should be locked to the desk where it is located, to prevent removal of the equipment. Access to programs should be physically limited by restricting the software that is installed.

### *Logical access controls*

Logical access controls primarily involve the use of passwords and authorization tables to limit individual users' access rights. Authorization tables should be set up to define each user's rights with regard to the level of computer access permitted. These tables should specify which data files may be accessed by each user and whether the user is able to read, write, or edit each file. Typically, users' authorization tables are also linked to a user ID (a unique name for each user) that can be generally known. To verify that the individual entering the user ID is genuine, a unique password known only to the individual and to the system itself should be entered by the user. This will assist in controlling access to both the computer and the various programs and data. Different passwords should be requested to permit access to different systems, programs, and data. Users should be required to change their passwords on a regular basis, and the computer system should not display the password while it is being entered to prevent other individuals finding it out. Users should also be instructed to memorize their passwords and not write them down. Note that access to the authorization tables should itself be password protected.

An additional level of access control should be set up on the system so that when an incorrect password is entered three times in one login attempt, the computer, user account, program, or data file (depending on what is being accessed) is disabled to prevent further access attempts. The IT department should retain the ability to remove the disabled status once it has verified whether access should be permitted.

### *Monitoring controls*

Decora must consider controls to monitor the use of computer time. The systems should only be used during working hours, and there should be a formal authorization process put in place to permit system access outside of normal hours. In addition, the following exception reports should be generated by the system to ensure that there is no unauthorized access to the computer system:

- use of invalid passwords (time, location, and by which user) to access
- occurrences where user accounts have been disabled due to use of invalid passwords
- occurrences where computers have been disabled due to use of invalid passwords
- occurrences of a single user logged in to multiple computers
- log of all significant downloads of data

All reports should be regularly reviewed by a responsible official at Decora, and any anomalous entries should be investigated promptly.

### *Application controls relating to changing/updating supplier standing-data details*

*Standing-data change controls*

The following controls should be implemented regarding all changes to standing data and are also relevant to changes to supplier details:

- The system should use password controls and authorization tables that determine users' rights to ensure only authorized individuals have editing access to the standing-data files.
- A separate password authorization control to confirm changes made to the supplier master file should be required prior to the computer system updating the entry.
- Passwords to allow access and confirm changes should be provided only to the relevant authorized individuals permitted to update the supplier master files.
- All amendments, additions, and deletions to data should be authorized by a responsible official (such as the purchasing department manager), and a standardized pro-forma form should be used to evidence such authorization.
- Amendment forms should be entered in batches, with different categories of changes being input in different batches. The batches should be sequentially numbered and recorded in a batch control book so that any gaps in the batch numbers can be investigated. Following input, the output produced by the computer should be checked to the input.
- The computer system should automatically generate a log of historic changes to master data files that outlines which user made the changes and when the changes were made.

- The log of historic changes to supplier standing data should be regularly reviewed by senior purchasing department personnel (such as the purchasing department manager) to ensure that changes have been made accurately and completely.
- Periodic checks to the master data file to ensure its integrity should be made; a detailed review of either the complete listing of the file or portions thereof should be made to ensure the accuracy and completeness of the listings. Suppliers' documents (such as invoices or statements) can be used to validate the details held on file.
- An exception report identifying all supplier accounts on which there has been no movement for a set period of time (such as six or 12 months) should be generated to enable the purchasing department to identify obsolete accounts that should be closed. Accounts that the purchasing department has identified as accounts for closure that retain a balance should not be closed until the liability is paid. However, a system flag should be put against the account to indicate that it should be closed after final settlement.

It is important for Decora to have strong data-change controls. Where data-change controls are weak, there is the risk that the supplier standing data is inaccurate as a result of error or fraud. Inaccurate supplier details may result in errors in paying genuine suppliers; this could cause disintegration of the relationship between Decora and its suppliers, which could ultimately result in the loss of suppliers. Decora pays its suppliers in cheque form, and thus examples of payment issues caused by inaccurate standing data may include the following:

- cheques being made out to the wrong supplier name, which may result in the bank refusing to cash the cheque to allow the supplier to recover the money owed
- cheques being sent to the wrong supplier address, resulting in loss of the cheque and a delay in payment

As noted above, weak controls relating to supplier details may also provide an opportunity for Decora staff to perpetrate a fraud (such as setting up a fictitious supplier to whom Decora makes payments). Most commonly, this would result in misappropriation of company assets.

**Solution to Question 3**

Control weakness: Lack of segregation of duties can lead to the potential concealment of fraud. Therefore, the same individual performing more than one function that should be segregated can lead to the misappropriation of assets and the concealment of that misappropriation. The accounts payable clerk could create a fictitious vendor and process payments to pay that vendor.

Best practice: Master data file functions (including creating new vendors, or changing payment information for existing vendors) should be appropriately segregated from the payment functions.

Mitigating/manual control: Changes to the vendor master file should be documented on a change request form and approved by a manager before processing by a separate function. A system-generated listing of all changes made to the vendor master file during a given period should be reviewed by the controller against appropriate vendor exception/change forms.

If, due to system limitations, a person had the ability to set up vendors and process the payments, a compensating control could be an automated alert that notified the purchasing manager or controller if that person set up a new vendor.

**Solution to Question 4**

| IT general control | Audit procedures to test design and operating effectiveness |
|---|---|
| *Access*: All users have unique usernames, and there are strong password controls in place, including the following:<br>• minimum length of eight characters<br>• alphanumeric requirement<br>• no reuse of previous password<br>• expiry period of 30 days | Obtain a user listing from the system and inspect the listing to determine if there are generic usernames (such as “Finance” or “Admin”). Discuss with client any exceptions to understand the purpose of such usernames. The design is considered ineffective if there is unnecessary and excessive use of such generic IDs.<br><br>Obtain a screenshot of the password parameter settings from the system and inspect this against best practices. Observe a staff member trying to change a password to a single character, a blank space, or some other unacceptable password and determine if it is accepted by the system. If it is accepted, the control is considered to be operating ineffectively. |

| IT general control | Audit procedures to test design and operating effectiveness |
|---|---|
| *System development*: An appropriate project/program management policy is in place and is followed to ensure that the requirements for the system are appropriately captured and delivered as part of the development of the new system (the system performs its operations as expected). | Inspect the project/system management policy and assess whether the controls will ensure that the system performs as expected.<br>Obtain evidence to prove that the policy is followed. For example:<br>• Inspect system specification documents for review and approval (proof requirements were appropriately captured, and development approved by authorized personnel).<br>• Inspect results of program testing (proof that testing has occurred).<br>Ask end users if they have been sufficiently trained on the system. |
| *System change*: System changes are authorized, tested in a controlled test environment, and migrated into the live environment by an independent staff member. | For a sample of program changes:<br>• Obtain the request form and inspect for appropriate sign-offs (proof of approval).<br>• Inspect results of program testing (proof that testing has occurred).<br>• Ask client staff which users have the ability to migrate changes and develop programs. Confirm migration was completed by these users (proof of restricted access). |
| *System backup and recovery*: System and data backups are run every night and stored in an off-site location. Backups are recovered weekly in the test environment. | • Inspect the backup logs to verify the backups are run daily.<br>• Inspect the off-site location.<br>• Observe the recovery of one of the backups (to ensure the backup protocol is working as described).<br>• Inspect the recovery logs to verify backups are restored weekly in the test environment. |

## Solution to Question 5

The data life cycle is the sequence of stages that a particular unit of data goes through from its initial generation or capture (often called “collection”) to its eventual deletion at the end of its useful life.

There are five accepted stages:

**Collection**: In this phase, data comes into an organization, usually through data entry, acquisition from an external source, or signal reception, such as transmitted sensor data.

**Maintenance**: In this phase, data is processed prior to its use. The data may be subjected to processes to detect and prevent incorrect processing of transactions, or to eliminate “dark” data that has no value.

**Data usage**: In this phase, data is used to support the organization’s objectives and operations. Data is transformed into information that the entity requires to run and manage itself.

**Storage** (for active data) **and archiving** (for inactive data): In this phase, active data (data used to make decisions) is stored in multiple locations to ensure adequate access and backups. Once this data is no longer needed, it can be archived. In this sub-stage, data is removed from all active production environments. It is no longer processed, used, or published but is stored in case it is needed again in the future

**Purging**: In this phase, every copy of data is deleted. Typically, this is performed on data that is already archived and only occurs when an entity determines that the information will never be needed again.