



FNSACC426

Set up and operate computerised accounting systems

Assessment 1 of 4

Short Answer Questions

ASSESSOR GUIDE



Assessment Instructions

Task overview

This assessment task is divided into nine [9] short answer questions. Read each question carefully before typing your response in the space provided.

Additional resources and supporting documents

To complete this assessment, you will need:

- Learning Material



Assessment Information

Submission

You are entitled to three [3] attempts to complete this assessment satisfactorily. Incomplete assessments will not be marked and will count as one of your three attempts.

All questions must be responded to correctly to be assessed as satisfactory for this assessment.

Answers must be typed into the space provided and submitted electronically via the LMS. Hand-written assessments will not be accepted unless previously arranged with your assessor.

Reasonable adjustment

Students may request a reasonable adjustment for assessment tasks.

Reasonable adjustment usually involves varying:

- the processes for conducting the assessment [e.g. allowing additional time]
- the evidence gathering techniques [e.g. oral rather than written questioning, use of a scribe, modifications to equipment]

However, the evidence collected must allow the student to demonstrate all requirements of the unit.

Refer to the Student Handbook or contact your Trainer for further information.



Please consider the environment before printing this assessment.

Question 1

List and describe four [4] key features commonly found in computerised accounting systems.

Assessor instructions: Students must list and describe four [4] key features commonly found in computerised accounting systems

The acceptable responses must:

- Be within the specified word limit.
- Reflect the characteristics described in the exemplar answer.

Benchmark answers are provided below.

Key Feature	Description (Approximate word count: 20 – 50 words)

Assessor instructions: Students can choose to list and describe any four [4] of the nine [9] key features provided below:

- **Automation of Transactions:** Automated data entry for recurring transactions reduces manual input, minimising errors and saving time. This includes automated invoicing, billing, and payment processing.
- **Real-Time Data Processing:** Immediate updating of accounts and financial statements as transactions occur, providing up-to-date financial information at any moment, which is crucial for timely decision-making.
- **Integration Capabilities:** Ability to integrate with other business systems such as payroll, inventory management, and customer relationship management (CRM) systems. This integration ensures that all data across the organisation is synchronised and consistent.
- **Multi-User Access:** Provides access to multiple users with various levels of permissions, ensuring that employees can work simultaneously while maintaining data integrity and security.
- **Comprehensive Reporting:** Generation of a wide range of financial reports such as profit and loss statements, balance sheets, and cash flow statements. Customisable reporting capabilities allow users to create reports that meet specific management or financial analysis needs.
- **Audit Trail:** Records detailed information about every financial transaction, including the date, time, and user who made the transaction. This feature is critical for tracking changes, ensuring accountability, and facilitating audits.
- **Scalability:** Systems can be scaled to accommodate the growth of a business, from small operations to large enterprises, without needing to switch to a different platform.
- **Tax Compliance and Calculation:** Automated tax calculations and compliance features that adapt to regional tax regulations and rates, simplifying the process of preparing returns and reducing the likelihood of errors.
- **Security Features:** Robust security measures such as data encryption, secure login protocols, and access controls to protect sensitive financial information from unauthorised access or breaches.

Question 2

In the table below, explain the methods provided to establish and maintain computerised accounting systems.

Assessor instructions: Students must explain the methods provided to establish and maintain computerised accounting systems.

The acceptable responses must:

- Be within the specified word limit.
- Reflect the characteristics described in the exemplar answer.

Benchmark answers are provided below.

Method	Explanation [Approximate word count: 40 – 80 words]
System Selection and Customisation	<ul style="list-style-type: none">• Assess Requirements: Identify the specific needs of your business, including transaction volume, regulatory requirements, and any industry-specific functionalities.• Choose Appropriate Software: Select a computerised accounting system that best fits these requirements, focusing on features, scalability, and user-friendliness.• Customisation: Tailor the system to meet the unique needs of your business, such as custom reports, specific tax setups, or integration with other operational software.
Implementation and Data Migration	<ul style="list-style-type: none">• Project Planning: Create a detailed implementation plan including timeline, budget, and resource allocation.• Data Migration: Carefully plan and execute the migration of historical financial data to the new system, ensuring data integrity and accuracy. This often involves data cleansing and formatting to fit the new system's requirements.
Training and User Adoption	<ul style="list-style-type: none">• Comprehensive Training: Conduct training sessions for all users to ensure they are proficient in using the new system. This includes training on entering transactions, generating reports, and understanding system alerts.• Support Channels: Establish ongoing support channels, such as IT helpdesk or access to vendor support, to assist users with any issues they may encounter.
Regular Updates and Compliance	<ul style="list-style-type: none">• Software Updates: Regularly update the software to take advantage of new features and security enhancements and comply with changes in financial regulations.

	<ul style="list-style-type: none"> • Audit and Compliance Checks: Periodically review the system to ensure it complies with accounting standards and regulatory requirements. This might involve internal audits or third-party compliance reviews.
Security Measures and Backup Procedures	<ul style="list-style-type: none"> • Security Protocols: Implement strong security measures to protect sensitive financial data. This includes setting up firewalls, using encryption, and managing user access levels. • Regular Backups: Establish a routine for regular backups of financial data to prevent loss due to system failures, cyberattacks, or other unforeseen events. Ensure backups are stored securely and are easily recoverable.

Question 3

In the table below, explain the methods for processing the following transactions in an integrated accounting system:

- BPAY
- credit card payments
- direct debit
- invoices
- petty cash
- balance day adjustments

Assessor instructions: Students must explain the methods for processing the following transactions in an integrated accounting system:

- BPAY
- credit card payments
- direct debit
- invoices
- petty cash
- balance day adjustments

The acceptable responses must:

- Be within the specified word limit.
- Reflect the characteristics described in the exemplar answer.

Benchmark answers are provided below.

Financial Transaction	Processing Method
	[Approximate word count: 60 – 120 words]
BPAY	

	<p>When a BPAY payment is made, the integrated system records the transaction by automatically debiting the relevant expense or creditor account and crediting the bank account from which the payment is made. The transaction details typically include the BPAY biller code, reference number, and the amount paid. The system may also provide options for scheduling payments and setting up recurring BPAY transactions, ensuring timely payments.</p>
Credit Card Payments	<p>Credit card transactions are entered into the system by recording the purchase details directly against the credit card account. For instance, when a purchase is made, the system debits the expense account related to the purchase and credits the credit card liability account. Payments made to settle the credit card balance are recorded by debiting the credit card liability account and crediting the bank account from which the payment is made, thus reducing the outstanding balance.</p>
Direct Debit	<p>For direct debit arrangements, the system needs to be set up with the details of the recurring payment, including the payee's information, amount, and payment intervals. When a payment is due, the system automatically debits the relevant expense account and credits the bank account. This process ensures that payments are made automatically on their due dates, reducing the risk of late payments.</p>
Invoices	<p>Invoices issued to customers are entered into the system by creating a new invoice entry, which includes details such as customer name, invoice number, items or services billed, total amount, and due date. This action increases accounts receivable. Upon receipt of payment, the system records the payment by debiting the cash or bank account and crediting accounts receivable, thereby closing the invoice.</p>
Petty Cash	<p>Petty cash transactions are handled by setting up a petty cash fund in the system. Expenses paid from petty cash are recorded by debiting the appropriate expense accounts and crediting the petty cash account. When the petty cash fund is replenished, the system records a debit to the petty cash account and a credit to the bank account, reflecting the transfer of funds to replenish the petty cash.</p>
Balance Day Adjustments	<ul style="list-style-type: none"> • Accruals: For expenses incurred but not yet paid, the system records an accrual by debiting the relevant expense account and crediting the corresponding liability account. • Prepayments: For expenses paid in advance, the system debits the prepayment asset account and credits the cash or bank account. In subsequent periods, the expense is recognised by debiting the expense account and crediting the prepayment account.

	<ul style="list-style-type: none"> • Depreciation: Fixed assets' depreciation is recorded by debiting the depreciation expense account and crediting the accumulated depreciation account. • Allowances for Doubtful Debts: This adjustment involves debiting bad debt expenses and crediting allowance for doubtful accounts to reflect potential losses from unpaid receivables.
--	--

Question 4

List and describe the features and functions of the common reports relevant to operating accounting systems provided in the table below.

Assessor instructions: Students must list and describe the features and functions of the common reports relevant to operating accounting systems provided in the table below.

The acceptable responses must:

- Be within the specified word limit.
- Reflect the characteristics described in the exemplar answer.

Benchmark answers are provided below.

Report	Features [Approximate word count: 20 – 50 words]	Functions [Approximate word count: 20 – 50 words]
Balance Sheet	<ul style="list-style-type: none"> • Categorises assets into current and non-current. • Separates liabilities into short-term and long-term. • Provides a clear view of the equity held by shareholders. 	<ul style="list-style-type: none"> • Shows the financial position of a company at a specific point in time. • Assists in liquidity analysis by highlighting current assets and liabilities. • Helps in assessing the capital structure and financial stability.
Profit and Loss Statement (P&L)	<ul style="list-style-type: none"> • Details revenue streams and types of expenses. 	<ul style="list-style-type: none"> • Measures financial performance over a specific period.

	<ul style="list-style-type: none"> • Often segmented to show gross profit, operating profit, and net profit. • Includes adjustments for tax and extraordinary items. 	<ul style="list-style-type: none"> • Provides insights into revenue efficiency and expense management. • Supports tax preparation and financial planning.
Cash Flow Statement	<ul style="list-style-type: none"> • Segregates cash flows related to operating, investing, and financing activities. • Highlights changes in cash and cash equivalents over the period. • Provides a reconciliation from net income to net cash provided by operating activities. 	<ul style="list-style-type: none"> • Demonstrates the liquidity and solvency of the business by tracking cash movements. • Helps in understanding the cash impact of business operations. • Supports investment decisions and financial strategy formulation.
Accounts Receivable and Payable Reports	<ul style="list-style-type: none"> • Includes aging schedules that categorise receivables and payables by their due dates. • Lists individual debtor and creditor details. a) Often integrates with inventory and sales data to provide a comprehensive view. 	<ul style="list-style-type: none"> b) Manages credit risk by monitoring the age of receivables and payables. c) Assists in cash flow forecasting by showing expected cash inflows and outflows. d) Enhances relationship management with customers and suppliers through timely follow-up.
Budgetary Reports	<ul style="list-style-type: none"> e) Compares actual financial results to budgeted figures. f) Includes variance analysis for each line item. 	<ul style="list-style-type: none"> • Facilitates financial control by comparing actual spending to budgets. • Aids in adjusting financial strategies

	<ul style="list-style-type: none"> Often broken down by departments or cost centres. 	<ul style="list-style-type: none"> based on performance deviations. Supports departmental accountability and operational efficiency.
--	---	--

Question 5

List and describe three [3] organisational policies and procedures relating to setting up and operating a computerised accounting system provided in the table below.

Assessor instructions: Students must list and describe three [3] organisational policies and procedures relating to setting up and operating a computerised accounting system provided in the table below.

The acceptable responses must:

- Be within the specified word limit.
- Reflect the characteristics described in the exemplar answer.

Benchmark answers are provided below.

Organisational Policy and Procedures	Description [Approximate word count: 60 – 120 words]

Assessor instructions: Students can choose to list and explain any three [3] of the seven [7] organisational policies and procedures provided below:

- Data Security Policy:** This policy outlines the measures and protocols to protect sensitive financial data from unauthorised access, breaches, and other security threats. It includes requirements for strong passwords, multi-factor authentication, regular security audits, and the use of secure networks. The policy also details how data breaches should be handled, including immediate actions, notification procedures, and remedial measures.
- Data Entry and Integrity Policy:** Establishes standards for accuracy and consistency in financial data entry. This policy specifies the procedures for entering transactions into the system, including validation checks to ensure data integrity. It may also detail roles and responsibilities for data entry, data review, and the correction of errors to maintain high-quality financial records.
- Backup and Recovery Policy:** Specifies the procedures for backing up financial data and restoring it in the event of data loss or system failure. This policy typically includes the frequency of backups, the type of backup [e.g., full, incremental], storage locations for backups [both on-site and off-site], and the steps to recover data. It ensures business continuity and the availability of financial information under all circumstances.
- Software Update and Maintenance Policy:** Outlines the protocols for updating and maintaining the accounting software. This includes scheduling regular updates to ensure the system is running the latest software versions with all necessary security patches and features. The policy covers how updates should be tested and implemented without disrupting normal business operations.

5. **Access Control Policy:** Defines who can access the computerised accounting system and what levels of access individuals have. This policy includes the creation of user profiles based on roles and responsibilities, ensuring that employees only have access to the parts of the system necessary for their job functions. It helps to prevent unauthorised access and reduces the risk of internal fraud.
6. **Compliance and Reporting Policy:** Ensures that the accounting system complies with relevant financial regulations and standards, such as Australian Accounting Standards, GST compliance, and other tax obligations. This policy also dictates how and when financial reports should be generated and reviewed, including statutory financial statements and internal management reports.
7. **Audit Trail Policy:** Establishes requirements for maintaining a detailed log of all transactions and changes made within the accounting system. This policy is critical for traceability and accountability, enabling auditors and management to review the history of financial transactions and verify their accuracy and legitimacy.

Question 6

Case study

Background: GreenLeaf Distributors, a large distributor of organic food products, uses a computerised accounting system to manage its extensive inventory, sales transactions, and customer invoicing. The company recently implemented new features in its accounting software to handle increased transaction volumes and introduced mobile access for sales representatives in the field.

Situation: After the new software update, the finance department noticed an increase in system downtime and slow performance, especially during peak business hours. Concerns were raised about the potential for data loss and the impact on order processing and financial reporting.

Which organisational policy should GreenLeaf Distributors review and possibly update to address the system performance issues and risks identified after the software update?

Choose one of the options provided and explain your choice in the table below.

Options:

- A. Software Update and Maintenance Policy
- B. Data Security Policy
- C. Backup and Recovery Policy
- D. Audit Trail Policy

Assessor instructions: Students must choose one of the four options and provide an explanation in the table below.

The acceptable responses must:

- Be within the specified word limit.
- Reflect the characteristics described in the exemplar answer.

Benchmark answers are provided below.

Correct answer	Correct Answer: A. Software Update and Maintenance Policy
Explanation (Approximate word count: 40 – 70 words)	The Software Update and Maintenance Policy is most relevant in this scenario as it addresses the need for careful planning and execution of software updates to avoid performance issues. This policy should ensure that updates are tested in a non-production environment to gauge their impact on system performance and stability and that there are measures in place to quickly resolve any issues that arise post-update.

Question 7

List and explain three [3] financial services industry legislation relating to information privacy when using computerised accounting systems.

Assessor instructions: Students must list and explain three [3] financial services industry legislation relating to information privacy when using computerised accounting systems.

The acceptable responses must:

- Be within the specified word limit.
- Reflect the characteristics described in the exemplar answer.

Benchmark answers are provided below.

Legislation	Explanation (Approximate word count: 40 – 70 words)

Assessor instructions: Students can choose any three [3] of the five [5] pieces of legislation provided below:

1. **Privacy Act 1988 (Cth):** This act is the primary law governing data protection in Australia. It includes the Australian Privacy Principles [APPs], which set out how personal information must be collected, used, stored, and disclosed. For financial services, this includes securing personal financial details processed through accounting systems. The Act applies to all organisations and government entities in Australia, requiring them to manage personal information responsibly.
2. **Notifiable Data Breaches (NDB) scheme:** Under the Privacy Act, the NDB scheme requires organisations to notify individuals and the Office of the Australian Information Commissioner [OAIC] when a data breach occurs that is likely to result in serious harm. This includes breaches involving personal financial information that could lead to identity theft or financial loss.
3. **Australian Securities and Investments Commission Act 2001 [ASIC Act]:** While primarily focused on market integrity and consumer protection, the ASIC Act has provisions that impact financial data management. It mandates accurate and honest dealing in financial services, including the maintenance and handling of financial records in computerised systems, ensuring they are kept securely and free from manipulation.
4. **Corporations Act 2001:** This act outlines requirements for financial management and reporting that affect computerised accounting systems. It includes stipulations for maintaining financial records

that correctly record and explain transactions and financial positions, which must be kept secure and private in compliance with the Privacy Act.

5. **Anti-Money Laundering and Counter-Terrorism Financing Act 2006 (AML/CTF Act):** This legislation requires financial institutions to maintain records of financial transactions to prevent and detect money laundering and terrorism financing. It includes requirements for the secure management of personal and financial data used in these transactions, which must be protected in computerised accounting systems.

Question 8

Case Study

Background: Fusion Financials is a financial advisory firm that offers personal financial planning services and manages investment portfolios for clients. They recently upgraded their computerised accounting system to enhance functionality and data analytics capabilities. The system stores a vast amount of sensitive client data, including personal identifiers, financial statuses, and transaction histories.

Situation: Shortly after the system upgrade, Fusion Financials experienced a cyber attack where unauthorised access was gained to their client database. An investigation revealed that the breach could potentially lead to identity theft and financial fraud affecting several clients. The company needs to address this breach in compliance with Australian law.

Which Australian law most directly requires Fusion Financials to take action following the data breach involving potential identity theft and financial fraud?

Choose one of the options provided and explain your choice in the table below.

Options:

- A. Privacy Act 1988 (Cth)
- B. Australian Securities and Investments Commission Act 2001 (ASIC Act)
- C. Corporations Act 2001
- D. Anti-Money Laundering and Counter-Terrorism Financing Act 2006 (AML/CTF Act)

Assessor instructions: Students must choose one of the four options and provide an explanation in the table below.

The acceptable responses must:

- Be within the specified word limit.
- Reflect the characteristics described in the exemplar answer.

Benchmark answers are provided below.

Correct answer	
	Correct Answer: A. Privacy Act 1988 (Cth)

Explanation [Approximate word count: 50 – 100 words]	<p>The Privacy Act 1988, particularly through the Notifiable Data Breaches (NDB) scheme, directly requires Fusion Financials to notify both the affected individuals and the Office of the Australian Information Commissioner about the data breach because it is likely to result in serious harm to the clients involved. This response is crucial for managing the breach responsibly and mitigating potential damage to the clients and the firm.</p> <p>This case study and question help students apply theoretical knowledge to practical scenarios, enhancing their understanding of compliance responsibilities in managing computerised accounting systems.</p>
--	--

Question 9

Explain the methods to substantiate financial transactions and record retention requirements for audit and substantiation purposes in the table provided below.

Assessor instructions: Students must explain the methods to substantiate financial transactions and record retention requirements for audit and substantiation purposes in the table provided below.

The acceptable responses must:

- Be within the specified word limit.
- Reflect the characteristics described in the exemplar answer.

Benchmark answers are provided below.

Method	Substantiation [Approximate word count: 30 – 50 words]	Retention [Approximate word count: 15 – 35 words]
Documentation	Maintain comprehensive and accurate records of all financial transactions, including invoices, receipts, contracts, and bank statements. These documents provide the necessary evidence to support each transaction's validity and accuracy.	These documents should be retained for a minimum period as required by law, typically 5 to 7 years, to ensure they are available for review during any financial audits or legal inquiries.
Authorisation and Approval Processes	Implement a robust system for the authorisation of transactions, where different levels of transactions require corresponding levels of approval. This method helps prevent unauthorised transactions and ensures each	Keep records of approvals and authorisations, including electronic logs or signed documents, to provide an audit trail that substantiates the legitimacy of each transaction.

	financial activity is justified and verified.	
Reconciliation	Regularly reconcile accounts to ensure the balances match supporting documentation such as bank statements and ledger entries. This practice helps identify and correct discrepancies, ensuring financial data integrity.	Retain all reconciliation reports and related corrections or adjustment documents to support the accuracy of financial statements.
Audit Trails	Maintain detailed logs that record the chronology of all financial activities and modifications. These logs should include the date, nature of the transaction, parties involved, and the user making the entry.	Audit trail records should be preserved for the same duration as the financial records they pertain to, providing a clear path from financial statements back to original entries.
Secure Storage and Access Controls	Use secure storage solutions and access controls to protect financial records from unauthorised access, alteration, or destruction. This includes both physical security for paper records and cybersecurity measures for digital data.	Implement data backup systems and disaster recovery plans to ensure the preservation and recovery of financial records. Regularly test these systems to confirm they are effective in maintaining data integrity over time.
Compliance with Legal and Regulatory Standards	Adhere to applicable laws and regulations governing financial transactions and reporting. Compliance helps ensure that the methods and practices used in financial management are legally sound and acceptable.	Understand and follow specific legal requirements related to the retention periods, formats, and management of records, as these can vary by jurisdiction and industry.

Assessment checklist:

Students must have completed all questions within this assessment before submitting. This includes:

1	Nine [9] short answer questions to be completed in the spaces provided.	<input type="checkbox"/>
---	---	--------------------------



Congratulations you have reached the end of Assessment [1]!

© UP Education Online Pty Ltd 2021

Except as permitted by the copyright law applicable to you, you may not reproduce or communicate any of the content on this website, including files downloadable from this website, without the permission of the copyright owner.