senm-answers.com

Email: customercare@senm-answers.com Tel: 254-734-053-765

CPA

Information Communication Technology

April 2026

Level: Foundation Level

Question 1

 Introduction to information communication technology (ICT), Overview of operating systems, An overview of application packages , Computer networks , Data security, Information systems in an enterprise

(a) A recent system crash disrupted operations for two days.

(i) Explain TWO roles of system recovery planning.

(ii) Recommend TWO continuity mechanisms.

Rafiki Holdings is considering virtualisation to reduce infrastructure costs.

Assess FOUR benefits of implementing virtualised environments.

(C) Analyse THREE ways in which ICT alignment with business strategy could create competitive advantage for Rafiki Holdings.

(d) The organisation is deciding between Windows Server and Linux Server environments.

Evaluate THREE critical operating system features that should influence this decision in an enterprise accounting environment.

✓ Answer for Question 1

(a) System Crash – Recovery & Continuity

(i) Roles of System Recovery Planning

System recovery planning ensures the organisation can restore operations quickly after disruptions. Key roles include:

1. **Minimising downtime**
   - Defines procedures to restore systems within acceptable time (Recovery Time Objective – RTO).
2. **Data protection and restoration**
   - Ensures backups are available and can be restored (Recovery Point Objective – RPO).
3. **Business continuity assurance**
   - Maintains critical operations even during system failure.
4. **Risk mitigation**
   - Identifies potential threats (hardware failure, cyberattacks, human error).
5. **Clear response procedures**
   - Provides step-by-step recovery actions for IT staff.
6. **Compliance and accountability**
   - Helps meet regulatory requirements (especially important in accounting environments).

(ii) Recommended Continuity Mechanisms

To avoid another 2-day disruption, Rafiki Holdings should implement:

1. **Regular data backups**
   - Daily incremental + weekly full backups
   - Offsite or cloud storage
2. **Disaster Recovery Site**
   - Hot site (immediate recovery) or warm site (partial readiness)
3. **Redundancy systems**
   - Backup servers, duplicate databases, failover systems

senm-answers.com

Email: customercare@senm-answers.com Tel: 254-734-053-765

CPA

Information Communication Technology

December 2025

Level: Foundation Level

Question 1b

 Mobile devices and applications

Highlight THREE common performance issues in mobile applications.

✓ Answer for Question 1b

Common performance issues in mobile applications:

---

1. Slow Loading Times

- Long app startup time
- Slow screen transitions or navigation delays
- Delayed response to user input (touch, gestures)

2. High Memory Usage (Memory Leaks)

- App consumes excessive RAM
- Causes crashes or forces the operating system to close background apps
- Leads to sluggish performance over time

3. Battery Drain

- Excessive CPU usage
- Poorly optimized background processes or network calls
- Frequent wake locks preventing device from sleeping

4. Network Latency and Poor Connectivity Handling

- Slow data fetching due to large payloads or inefficient APIs
- Lack of offline support or poor handling of weak/unstable network connections
- No caching strategies implemented

5. UI Lag and Stuttering

- Inefficient rendering of layouts
- Complex UI updates on the main thread causing frame drops
- Lack of smooth scrolling (e.g., in lists or grids)

senm-answers.com

Email: customercare@senm-answers.com Tel: 254-734-053-765

CPA

Information Communication Technology

August 2025

Level: Foundation Level

Question 1b

 The Internet

Identify SIX components of an e-mail header.

✓ Answer for Question 1b

1. From

- Specifies the sender's e-mail address
- May also display the sender's display name
- Example: `From: "John Doe"`

---

2. To

- Indicates the primary recipient(s) of the e-mail
- Contains the e-mail address(es) of the intended recipients
- Example: `To: jane.smith@company.com`

---

3. Subject

- Provides a brief summary or topic of the e-mail message
- Appears in the recipient's inbox list
- Example: `Subject: Quarterly Report Submission`

---

4. Date

- Indicates the date and time the e-mail was sent
- Typically displayed in a standardized format (e.g., RFC 5322)
- Example: `Date: Wed, 31 Mar 2026 14:30:15 +0300`

---

5. Cc (Carbon Copy)

- Lists recipients who receive a copy of the e-mail

senm-answers.com

Email: customercare@senm-answers.com Tel: 254-734-053-765

CPA

Information Communication Technology

August 2025

Level: Foundation Level

Question 1c

Introduction to information communication technology (ICT)

Using suitable examples, explain SIX roles of information communication technology (ICT) in shaping the modern business environment.

✓ Answer for Question 1c

1. Enhancing Operational Efficiency

Role: ICT automates routine tasks, streamlines workflows, and reduces manual effort, enabling businesses to operate more efficiently.

Example:

- A manufacturing company implements an **Enterprise Resource Planning (ERP)** system that integrates inventory management, production scheduling, and order processing
- Previously, staff manually updated spreadsheets across departments, leading to delays and errors
- The ERP system automates stock level updates when sales are made and triggers purchase orders when inventory falls below thresholds
- **Result:** Order fulfillment time reduced by 40%, stockouts eliminated, and staff freed to focus on value-added activities

---

2. Enabling Data-Driven Decision Making

Role: ICT provides tools for collecting, analyzing, and visualizing data, allowing businesses to make informed decisions based on insights rather than intuition.

Example:

- A retail chain uses **Business Intelligence (BI)** software such as Power BI or Tableau to analyze sales data across 50 stores
- Dashboards display real-time information on top-selling products, underperforming locations, and customer buying patterns
- Management identifies that certain products sell better in specific regions and adjusts inventory allocation accordingly
- **Result:** Sales increased by 15% due to optimized stock placement, and markdowns on slow-moving items reduced by 25%

senm-answers.com

Email: customercare@senm-answers.com Tel: 254-734-053-765

CPA

Information Communication Technology

April 2025

Level: Foundation Level

Question 2a

 Introduction to information communication technology (ICT)

Distinguish between “embedded computers” and “integrated computers”.

✓ Answer for Question 2a

Definitions

Embedded Computer:
A specialised computer system designed to perform one or a few dedicated functions, typically embedded as a component within a larger device or system. It is not user-programmable for general-purpose tasks.

Integrated Computer:
A computer system where the processing unit, memory, storage, and peripherals are combined into a single unit, often sharing a common housing or chassis. The term may also refer to computers built into other products but retaining general-purpose computing capabilities.

Embedded Computer

Key Characteristics:

- Designed for a specific, dedicated task or function
- Typically runs firmware rather than a full operating system
- Optimised for low power consumption, small size, and low cost
- Often operates in real-time with strict timing constraints
- User does not interact with it as a general-purpose computer
- Not user-programmable for different applications

Examples:

- Microcontroller in a microwave oven controlling cooking time and power
- Engine control unit (ECU) in a car managing fuel injection and ignition timing
- Processor inside a digital watch
- Controller in a washing machine managing cycles and water levels
- Firmware in a printer managing paper feed and ink distribution

Typical Users:

senm-answers.com

Email: customercare@senm-answers.com Tel: 254-734-053-765

CPA

Information Communication Technology

April 2025

Level: Foundation Level

Question 2b

Systems analysis and design

Discuss FOUR techniques used to measure the effectiveness of system maintenance.

✓ Answer for Question 2b

Techniques for Measuring Maintenance Effectiveness

1. Mean Time Between Failures (MTBF)

Description:
MTBF measures the average time elapsed between system failures. It is calculated by dividing total operating time by the number of failures during that period.

Formula:
MTBF = Total Operating Time ÷ Number of Failures

What it indicates:
A higher MTBF indicates more reliable systems and effective preventive maintenance. A decreasing MTBF suggests maintenance is not adequately preventing failures.

Example:
A server operates for 2,000 hours and experiences 4 failures. MTBF = 2,000 ÷ 4 = 500 hours between failures.

2. Mean Time to Repair (MTTR)

Description:
MTTR measures the average time required to repair a failed system and restore it to normal operation. It includes detection, diagnosis, repair, and restart time.

Formula:
MTTR = Total Downtime Due to Failures ÷ Number of Failures

What it indicates:
A lower MTTR indicates effective corrective maintenance, skilled technicians, good diagnostic tools, and efficient repair procedures.

senm-answers.com

Email: customercare@senm-answers.com Tel: 254-734-053-765

CPA

Information Communication Technology

December 2024

Level: Foundation Level

Question 3

 Introduction to information communication technology (ICT), Overview of operating systems, An overview of application packages , Data security

(a) Outline FOUR potential risks of using outdated software.

(b) Highlight FOUR environmental impacts of Information Communication Technology (ICT) in business.

(c) Discuss THREE roles of source document integration in computerised accounting systems.

(d) Examine SIX reasons why an operating system is deemed crucial for the proper functioning of a computer system.

✓ Answer for Question 3

(a) Potential Risks of Using Outdated Software

1. Security Vulnerabilities

- Outdated software contains known security flaws that attackers actively exploit
- Vendors stop releasing security patches for older versions
- Unpatched vulnerabilities can lead to data breaches, malware infections, and ransomware attacks

2. Incompatibility with Other Systems

- Newer hardware, operating systems, or file formats may not work with outdated software
- Inability to open files from partners or customers using modern applications
- Integration failures with cloud services and modern APIs

3. Non-Compliance with Regulations

- Outdated software may not support required security or privacy controls
- Violations of data protection laws (e.g., Kenya's Data Protection Act, GDPR, HIPAA)
- Penalties, fines, and legal liability for non-compliance

4. Lack of Technical Support

- Vendors discontinue support for older versions
- No access to help desks, knowledge bases, or bug fixes
- Organisations must rely on internal expertise or unsupported workarounds

5. Performance Degradation

- Older software may be inefficient, slow, or resource-intensive on modern hardware
- Lack of optimisation for newer processors, memory, and storage technologies

- Reduced productivity due to lag, crashes, and delays

6. Increased Maintenance Costs

- Keeping outdated software running requires expensive workarounds and custom fixes
- Higher IT support costs for troubleshooting compatibility issues
- Opportunity cost of IT staff time spent on legacy systems instead of innovation

7. Data Corruption and Loss

- Older software may have undetected bugs that corrupt data
- File formats may become obsolete, making data inaccessible
- Backup and recovery features may be inadequate or unreliable

8. Reduced Productivity and User Frustration

- Missing modern features that competitors use for efficiency
- Cumbersome user interfaces compared to modern alternatives
- Employee frustration leads to lower morale and potential turnover

9. Lack of Integration with Modern Tools

- Cannot connect to cloud storage, collaboration platforms, or mobile devices
- Manual data transfers instead of automated workflows
- Inability to leverage artificial intelligence, automation, or analytics

---

(b) Environmental Impacts of Information Communication Technology (ICT) in Business

Negative Environmental Impacts

1. Electronic Waste (E-Waste)

- Rapid obsolescence leads to discarded computers, servers, phones, and peripherals

senm-answers.com

Email: customercare@senm-answers.com Tel: 254-734-053-765

CPA

Information Communication Technology

August 2024

Level: Foundation Level

Question 4

Computer networks , Systems analysis and design , Legal, ethical and social issues in information systems

(a) Explain TWO circumstances that would necessiate an organisation to use the outsourcing method to acquire an information system.

(b) Highlight FOUR limitations of cloud computing.

(c) Explain THREE circumstances that could necessitate setting up of a Local Area Network (LAN) in an organisation.

(d) Highlight SIX measures that could be used to minimise unethical ICT practices in an orgnisation.

✓ Answer for Question 4

(a) Circumstances That Would Necessitate an Organisation to Use the Outsourcing Method to Acquire an Information System

Definition of Outsourcing:
The practice of contracting with an external vendor or service provider to develop, host, or manage an information system rather than building or operating it internally.

Circumstances:

1. Lack of Internal Technical Expertise

- Organisation does not have staff with required programming, database, or security skills
- Recruiting and training specialists would take too long or cost too much
- Complex technologies (e.g., artificial intelligence, blockchain, ERP) require rare expertise
- Outsourcing provides immediate access to skilled professionals

2. Cost Constraints for Internal Development

- Building an in-house system requires significant upfront investment (hardware, software, hiring)
- Outsourcing converts capital expenditure to operational expenditure (pay-as-you-go)
- Small and medium enterprises may not afford internal development
- Fixed-price contracts provide budget certainty

3. Time Constraints (Faster Delivery)

- Internal development may take months or years
- Outsourcing vendors have existing frameworks, templates, and experienced teams
- Shorter time-to-market for competitive advantage

(b) Limitations of Cloud Computing

Definition of Cloud Computing:

Delivery of computing services (servers, storage, databases, networking, software) over the internet on a pay-as-you-go basis.

Limitations:

1. Internet Dependency

- Cloud services require reliable, high-speed internet connection
- Internet outages make cloud applications inaccessible
- Remote or rural areas with poor connectivity cannot use cloud effectively
- Latency-sensitive applications (real-time gaming, video editing) suffer from network delays

2. Data Security and Privacy Concerns

- Storing sensitive data on third-party servers raises security risks
- Data breaches at cloud provider affect all customers
- Multi-tenant environments risk data leakage between customers
- Unclear physical location of data may violate data residency laws

3. Limited Control and Customisation

- Organisations cannot customise cloud infrastructure beyond provider's offerings
- Limited visibility into provider's security practices and employee access
- Software as a Service (SaaS) offers no access to underlying code or database
- Organisations must adapt processes to software, not vice versa

4. Vendor Lock-In

- Migrating data and applications between cloud providers is difficult and costly
- Proprietary APIs, data formats, and services make switching providers challenging

- Uploading terabytes of data to cloud can take days or weeks over standard internet
- Some providers offer physical data transfer appliances, but this adds complexity
- Large datasets may be impractical to move to cloud

10. Limited Integration with Legacy Systems

- Older on-premise systems may not integrate easily with cloud services
- Custom integration development adds cost and complexity
- Hybrid cloud environments require additional management tools

11. Contractual and Service Level Agreement (SLA) Limitations

- SLAs typically cover uptime but not performance or response times
- Remedies for SLA violations are often service credits, not cash refunds
- Provider may change terms or discontinue services with limited notice

12. Long-Term Cost for Stable Workloads

- For predictable, steady workloads, cloud may be more expensive than on-premise
- Running servers 24/7 for years may cost less when purchased outright
- Cloud advantage diminishes for constant, predictable usage patterns

---

(c) Circumstances That Could Necessitate Setting Up of a Local Area Network (LAN) in an Organisation

Definition of LAN:
A Local Area Network connects computers and devices within a limited geographic area (office, building, campus) to share resources, data, and applications.

Circumstances:

1. Need for Resource Sharing (Printers, Scanners, Storage)

- Multiple employees need access to the same printers, scanners, or copiers

13. Cost Reduction Through Shared Peripherals

- High-end scanner, plotter, or video conferencing equipment can be shared
- LAN eliminates need to purchase duplicate peripherals for each department

14. Enhanced Security Compared to Individual Computers

- Individual computers are harder to secure and monitor
- LAN with centralised security (firewall, intrusion detection) provides better protection
- Access logs track who accessed which resources

15. Support for Voice over IP (VoIP) Phone Systems

- Organisation wants to replace traditional phone system with VoIP
- LAN provides network for both data and voice
- Lower phone costs and advanced features (conferencing, forwarding)

(d) Measures to Minimise Unethical ICT Practices in an Organisation

Definition of Unethical ICT Practices:
Actions involving information technology that violate moral principles, organisational policies, or laws, such as software piracy, data theft, privacy violations, cyberbullying, or unauthorised access.

Measures:

1. Establish a Written ICT Code of Conduct

- Develop formal policy document defining acceptable and unacceptable ICT behaviours
- Cover areas: internet usage, email, social media, software installation, data handling, password sharing
- Specify consequences for violations (verbal warning, written warning, suspension, termination, legal action)
- Require all employees to sign acknowledgement of understanding

senm-answers.com

Email: customercare@senm-answers.com Tel: 254-734-053-765

CPA

Information Communication Technology

April 2024

Level: Foundation Level

Question 5

 Overview of operating systems, Data security, e-Commerce , Systems analysis and design

(a) Outline SIX core processes for software development.

(b) Explain TWO reasons why a major operating system must evolve over time.

(c) Examine THREE methods that could be used to prevent social engineering related attacks.

(d) Explain TWO advantages and TWO disadvantages of digital wallets as an ecommerce payment method.

✓ Answer for Question 5

(a) Core Processes for Software Development

Definition:
Software development core processes are the fundamental activities that transform a concept into a working software product. These are typically organised within a Software Development Life Cycle (SDLC).

Core Processes:

1. Requirements Gathering and Analysis

- Identify and document what the software must do
- Interview stakeholders, users, and subject matter experts
- Define functional requirements (features) and non-functional requirements (performance, security)
- Create use cases, user stories, or requirement specifications
- Validate requirements with stakeholders and obtain sign-off

2. System Design and Architecture

- Define the overall structure and components of the software
- Create architectural diagrams, data models, and interface designs
- Select appropriate technologies, frameworks, and platforms
- Design database schemas, APIs, and user interfaces
- Produce detailed design specifications for developers

3. Implementation (Coding)

- Write source code based on design specifications
- Follow coding standards and best practices
- Use version control systems (e.g., Git) to manage code changes
- Conduct code reviews to ensure quality
- Develop unit tests for individual components

4. Testing and Quality Assurance

- Verify that the software meets requirements and is free of defects
- Perform unit testing (individual components)
- Conduct integration testing (components working together)
- Execute system testing (end-to-end functionality)
- Carry out user acceptance testing (UAT) with real users
- Test non-functional aspects (performance, security, usability)

5. Deployment and Release

- Package and prepare software for production environment
- Set up servers, databases, and infrastructure
- Migrate data from legacy systems if applicable
- Execute deployment plan (cutover, pilot, phased, or parallel)
- Verify successful deployment with smoke testing

6. Maintenance and Support

- Fix bugs and issues discovered after release
- Provide technical support to users
- Apply security patches and updates
- Make minor enhancements and improvements
- Refactor code to improve maintainability

7. Project Management

- Plan and track project activities, timelines, and resources
- Manage risks, issues, and changes
- Communicate with stakeholders and report progress
- Ensure project stays within budget and schedule
- Coordinate team activities and resolve conflicts

8. Configuration and Change Management

- Manage changes to requirements, design, and code
- Track versions of software components
- Control access to development and production environments
- Document changes and maintain audit trail

9. Documentation

- Create user manuals and help guides
- Document technical specifications and API references
- Maintain system architecture and design documents
- Produce operational procedures (backup, recovery, deployment)

10. Quality Assurance and Process Improvement

- Establish and enforce development standards
- Conduct process audits and reviews
- Measure quality metrics (defect rates, test coverage)
- Implement continuous improvement initiatives

(b) Reasons Why a Major Operating System Must Evolve Over Time

Definition:
Operating system evolution refers to the continuous development and release of new versions, updates, and patches to meet changing technological, security, and user demands.

Reasons:

1. Security Vulnerabilities

- New security threats and attack methods emerge constantly
- Hackers discover vulnerabilities in existing code
- Patches and updates are required to fix known vulnerabilities
- Failure to evolve leaves users exposed to malware, ransomware, and data breaches

2. Hardware Advancements

- New processors (CPU architectures, more cores, 64-bit vs 32-bit)
- New storage technologies (SSDs, NVMe, optane)
- New memory technologies (DDR4, DDR5, HBM)

- New peripheral interfaces (USB-C, Thunderbolt, Bluetooth versions)
- OS must evolve to support and optimise for new hardware

3. New Software and Application Demands

- Applications require new OS capabilities (APIs, services, libraries)
- Modern programming languages and frameworks need OS support
- Cloud-native and containerised applications demand new features
- Mobile and cross-platform apps require consistent OS interfaces

4. User Experience and Interface Improvements

- User expectations change over time (touch, voice, gesture)
- Accessibility requirements evolve (screen readers, voice control)
- Visual design trends change (flat design, dark mode, translucency)
- Productivity demands drive interface efficiency improvements

5. Performance Optimisation

- New algorithms and techniques improve speed and efficiency
- Better memory management reduces resource consumption
- Improved scheduling algorithms enhance multitasking
- Faster boot times and wake-from-sleep responsiveness

6. Support for New File Systems

- Larger storage capacities require new file system designs
- Improved data integrity features (checksums, copy-on-write)
- Better handling of small files or massive directories
- Snapshots, compression, and deduplication capabilities

7. Networking Advancements

- New network protocols (IPv6, QUIC, HTTP/3)
- Higher bandwidth (5G, Wi-Fi 6/7, 10/40/100 GbE)
- Lower latency requirements (real-time applications, gaming)
- Improved security (WPA3, TLS 1.3)

8. Regulatory and Compliance Requirements

- New data protection laws require OS-level privacy controls
- Accessibility laws mandate certain features
- Export controls and encryption regulations
- Industry-specific compliance (healthcare, finance, government)

9. Energy Efficiency and Power Management

- Mobile devices require better battery life
- Environmental concerns drive energy efficiency improvements
- New power management states and transitions
- Optimised background activity and wake-up patterns

10. Bug Fixes and Stability Improvements

- Undiscovered bugs are found over time
- Driver conflicts and hardware compatibility issues arise
- Edge cases cause crashes or data corruption
- Continuous improvement in system stability

11. Scalability Requirements

- Systems need to support more memory (TB instead of GB)
- More processor cores (hundreds instead of dozens)
- More storage devices and larger capacities
- More concurrent users and processes

12. Integration with Cloud Services

- Cloud storage integration (OneDrive, iCloud, Google Drive)
- Single sign-on and identity management
- Remote desktop and virtualisation
- Backup and synchronisation across devices

13. Obsolescence of Legacy Features

- Older hardware and software are no longer used
- Removing deprecated features simplifies code
- Reduces attack surface (removing unnecessary code)

- Focuses development effort on modern features

Example:
Windows has evolved from Windows 95 (16/32-bit hybrid, no internet security) to Windows 11 (64-bit only, integrated security, touch support, cloud integration). Each version addressed limitations of previous versions and adapted to new technologies.

(c) Methods to Prevent Social Engineering Related Attacks

Definition:
Social engineering attacks manipulate people into revealing confidential information or performing actions that compromise security, rather than exploiting technical vulnerabilities.

Prevention Methods:

1. Security Awareness Training

- Train all employees to recognise phishing emails, suspicious links, and attachments
- Educate on common social engineering tactics (urgency, authority, fear, trust)
- Teach employees to verify requests before providing information
- Make training mandatory and recurring (not one-time)
- Test knowledge with quizzes and assessments

2. Simulated Phishing Exercises

- Send fake phishing emails to employees to test their awareness
- Provide immediate feedback when employees fail (click link or download attachment)
- Track metrics (click rates, report rates) to measure improvement
- Repeat exercises regularly to maintain vigilance
- Reward employees who report suspicious messages

3. Clear Verification Procedures

- Establish and enforce procedures for verifying requests for sensitive information
- Require call-backs to known numbers (not numbers provided in request)
- Use out-of-band verification (different communication channel)
- Require in-person confirmation for high-risk actions (large payments, access changes)
- Document verification steps and train all staff

4. Least Privilege Access

- Grant users only the minimum access required for their job duties
- No single person should have complete control over critical processes
- Separate duties so multiple approvals required for sensitive actions
- Regularly review and revoke unnecessary access rights
- Limit administrative privileges to essential personnel only

5. Multi-Factor Authentication (MFA)

- Require MFA for all system access, especially remote access
- Stolen passwords alone are insufficient for attackers
- Use authenticator apps, hardware tokens, or biometrics
- MFA prevents many social engineering attacks even if credentials are stolen

6. Email Filtering and Security

- Deploy email filtering to block known phishing and spam messages
- Use link protection (rewrite links to scan for malicious content)
- Implement DMARC, DKIM, and SPF to prevent email spoofing
- Block executable attachments and macros
- Display warning banners for external emails

7. Strong Password Policies

- Enforce minimum length (12+ characters) and complexity requirements
- Prohibit common, easily guessed passwords

- Require regular password changes (with care to avoid counterproductive frequency)
- Implement password managers to reduce password reuse
- Block compromised passwords using breach databases

8. Physical Security Measures

- Secure sensitive areas (server rooms, finance department) with access controls
- Require ID badges for all employees and visitors
- Challenge unrecognised individuals in secure areas
- Report tailgating (following authorised person through door)
- Lock workstations when away from desk

9. Clear Security Policies and Consequences

- Document acceptable use, data handling, and information sharing policies
- Clearly state consequences for policy violations
- Enforce policies consistently across all employees
- Include security responsibilities in job descriptions and performance reviews

10. Incident Reporting Mechanisms

- Provide easy, anonymous ways to report suspected social engineering
- Encourage reporting without fear of punishment
- Investigate all reports promptly
- Share lessons learned (anonymised) with the organisation

11. Limit Information Available to Attackers

- Minimise employee information on public websites (email addresses, job titles, phone numbers)
- Be cautious about sharing organisational structure or department contacts
- Review social media presence for information that could be used in attacks
- Use generic email addresses for public-facing roles (info@, support@)

12. Technical Controls to Limit Damage

- Implement data loss prevention (DLP) to block unauthorised data transfers

- Use endpoint detection and response (EDR) to identify compromised devices
- Segment networks to limit lateral movement after compromise
- Implement zero-trust architecture (never trust, always verify)

13. Executive and VIP Protection

- Executives are prime targets for social engineering (CEO fraud, whaling)
- Provide specialised training for executives and their assistants
- Implement additional verification for executive requests (especially financial)
- Limit public disclosure of executive schedules and activities

14. Regular Security Audits and Assessments

- Conduct social engineering penetration tests (phishing simulations, tailgating tests)
- Assess employee vulnerability to phone-based (vishing) attacks
- Review and update security policies annually
- Test incident response procedures

Example of an Attack and Prevention:
An attacker calls an employee pretending to be from IT, claiming there is a security issue and asking for their password. Prevention methods include: training employees never to share passwords, verification procedures (call back known IT number), technical controls (MFA makes stolen password useless), and reporting mechanisms (employee reports suspicious call).

(d) Advantages and Disadvantages of Digital Wallets as an E-Commerce Payment Method

Definition:
A digital wallet (e-wallet) is a software-based system that securely stores payment information (credit/debit cards, bank accounts, cryptocurrency) and enables electronic transactions via smartphone, computer, or wearable device.

Advantages:

1. Convenience and Speed

- No need to enter card details for every transaction
- One-click or one-tap checkout process
- Reduces checkout time from minutes to seconds
- Lowers cart abandonment rates in e-commerce

2. Enhanced Security

- Payment information is tokenised (not shared with merchant)
- Biometric authentication (fingerprint, face recognition) required for transactions
- Card details not stored on merchant servers (reduces breach risk)
- Remote wipe capability if phone is lost or stolen

3. Contactless Payments

- No physical contact with payment terminals (hygienic)
- Faster than inserting chip card or swiping
- Increasingly accepted at physical stores as well as online
- Particularly valuable in post-COVID environment

4. Storage of Multiple Payment Methods

- Store multiple credit cards, debit cards, bank accounts, and loyalty cards
- Switch between payment methods easily
- Reduces wallet clutter (no physical cards to carry)
- Manage all payments from single app

5. Loyalty and Rewards Integration

- Automatically apply loyalty points, coupons, and offers
- Earn cashback or rewards on transactions
- Track rewards balance and redemption history
- Personalised offers based on purchase history

6. Transaction Tracking and Budgeting

- Automatically record all transactions in one place

- Categorise spending for budgeting purposes
- Real-time transaction notifications
- Easier expense tracking and reconciliation

7. International Transactions

- Many digital wallets support multiple currencies
- Lower currency conversion fees than credit cards (sometimes)
- No need to carry multiple currencies when travelling
- Can be used for cross-border e-commerce

8. Accessibility for Unbanked Populations

- Mobile money wallets (e.g., M-Pesa) serve people without bank accounts
- Enable e-commerce participation for previously excluded populations
- Lower barriers to entry for online selling
- Facilitate remittances and peer-to-peer payments

Disadvantages:

1. Technology Dependency

- Requires smartphone, internet connectivity, and battery
- Cannot transact if phone is lost, damaged, or out of battery
- Not usable in areas with poor network coverage
- Older phones may not support latest wallet apps

2. Security Risks if Device Compromised

- If phone is stolen and unlocked, wallet may be accessible
- Malware on phone could intercept transactions
- Sim-swapping attacks can compromise mobile wallets
- User negligence (weak PIN, no biometrics) increases risk

3. Limited Merchant Acceptance

- Not all e-commerce websites accept all digital wallets
- Smaller merchants may not support digital wallets
- International merchants may accept only certain wallets

- User may need multiple wallets for different merchants

4. Transaction Fees

- Some digital wallets charge fees for certain transactions
- Currency conversion fees for international purchases
- Withdrawal fees to transfer balance to bank account
- Fees can be higher than traditional payment methods

5. Privacy Concerns

- Wallet provider collects data on all transactions
- Purchase history can be analysed and shared (anonymised or not)
- Location tracking if wallet uses GPS
- Privacy policies may allow data sharing with third parties

6. Dispute Resolution Challenges

- Chargeback processes are less established than credit cards
- Disputing fraudulent or incorrect charges may be difficult
- Customer protection varies by wallet provider
- Resolution times may be longer than credit cards

7. Technical Issues and Downtime

- Wallet app may crash or be unavailable
- Server outages prevent transactions
- Updates may introduce bugs or change interface
- Connectivity issues at checkout cause frustration

8. Dependency on Third-Party Provider

- Wallet provider could go out of business or change terms
- Provider may suspend account for perceived policy violations
- Funds could be frozen if provider suspects fraud
- Limited recourse if provider fails

9. Setup and Learning Curve

- Initial setup requires linking cards or funding source
- Verification process (KYC) may require uploading documents
- Some users find technology intimidating
- Elderly or less tech-savvy users may struggle

10. Regulatory Uncertainty

- Digital wallet regulations vary by country
- Rules on consumer protection, fund safeguarding, and dispute resolution differ
- Cross-border transactions face complex regulatory landscape
- Regulations may change, affecting wallet operation

11. Potential for Overspending

- One-click payments reduce friction, potentially increasing impulse spending
- Less awareness of spending (no physical cash or card handling)
- Budget tracking requires discipline
- May lead to financial mismanagement for some users

Examples of Digital Wallets:

- Apple Pay, Google Pay, Samsung Pay (NFC-based)
- PayPal, Venmo (online and peer-to-peer)
- M-Pesa (mobile money, dominant in Kenya)
- Alipay, WeChat Pay (dominant in China)

senm-answers.com

Email: customercare@senm-answers.com Tel: 254-734-053-765

CPA

Information Communication Technology

December 2023

Level: Foundation Level

Question 6

 Introduction to information communication technology (ICT), An overview of application packages , Legal, ethical and social issues in information systems

(a) Explain the term “proofreading” as used in a word processing program.

(b) State the unit of measuring a computer’s clock speed, RAM size, Hard disk size and monitor size.

(c) Discuss THREE challenges associated with the use of external hard drives.

(d) Examine FOUR legal issues associated with the use of information systems.

✓ Answer for Question 6

(a) Explain the Term "Proofreading" as Used in a Word Processing Program

Definition: Proofreading is the process of carefully reviewing a document to identify and correct errors in spelling, grammar, punctuation, formatting, and consistency before the document is finalised or shared.

Key Activities in Proofreading:

Checking Spelling – Identifying misspelled words, typos (e.g., "teh" instead of "the"), homophones (there/their/they're), and proper names

Checking Grammar – Identifying subject-verb agreement errors, incorrect verb tenses, sentence fragments, run-on sentences, and incorrect article usage (a, an, the)

Checking Punctuation – Ensuring correct placement of commas, periods, question marks, exclamation points, apostrophes, quotation marks, colons, semicolons, and parentheses

Checking Formatting Consistency – Ensuring consistent font type, size, colour, heading styles, spacing (line and paragraph), alignment, and bullet/numbering format

Checking Capitalisation – Ensuring proper capitalisation of sentences, proper nouns (names, places, brands), and headings (title case vs sentence case)

Checking Page Layout – Verifying correct margins, page breaks, section breaks, headers and footers, and page numbering

Checking Tables and Figures – Ensuring table and figure captions are correct and numbered sequentially, data is accurate, and cross-references are correct

Checking Consistency of Terminology – Ensuring same term is used throughout (e.g., "customer" not mixed with "client"), consistent abbreviation

usage (define on first use), and consistent spelling (e.g., "organisation" vs "organization")

How Word Processing Programs Support Proofreading:

- **Spell Check** – Underlines misspelled words in red and suggests corrections
- **Grammar Check** – Underlines grammatical errors in blue and suggests corrections
- **AutoCorrect** – Automatically corrects common typos as you type
- **Thesaurus** – Suggests alternative words to avoid repetition
- **Find and Replace** – Finds all instances of a word or phrase and can replace with corrected version
- **Track Changes** – Allows proofreader to make suggestions that author can accept or reject
- **Comments** – Allows proofreader to ask questions or explain corrections
- **Read Aloud** – Text-to-speech feature helps catch errors by listening
- **Zoom** – Allows proofreader to enlarge text for closer examination
- **Show/Hide Formatting Marks** – Reveals hidden characters (spaces, tabs, paragraph marks)

Proofreading vs Editing:

- **Proofreading** focuses on surface errors (spelling, grammar, punctuation, formatting) and is done after editing, before final submission. It corrects errors without changing meaning and works word-by-word.
- **Editing** focuses on content, structure, clarity, flow, and tone. It is done after drafting, before proofreading, and may restructure sentences, paragraphs, or sections at the overall document level.

Tips for Effective Proofreading:

- Read the document aloud to catch errors your eyes might miss
- Read backwards (from last sentence to first) to focus on individual sentences
- Use a ruler or blank sheet to cover lines below the one you are reading
- Proofread a printed copy (errors are often easier to see on paper)
- Take breaks between writing and proofreading (fresh eyes catch more errors)

- Read slowly and deliberately, not quickly

(b) State the Unit of Measuring a Computer's Clock Speed, RAM Size, Hard Disk Size and Monitor Size

Clock Speed – Measured in Hertz (Hz). Common multiples are Megahertz (MHz) for 1 million cycles per second and Gigahertz (GHz) for 1 billion cycles per second. Typical range is 1.0 GHz to 5.5 GHz. Higher clock speed generally means faster processing.

RAM Size – Measured in Bytes (B). Common multiples are Gigabytes (GB) and Terabytes (TB). 1 GB = approximately 1 billion bytes. Typical range is 4 GB to 128 GB. More RAM allows more programs to run simultaneously and larger files to be processed.

Hard Disk Size – Measured in Bytes (B). Common multiples are Gigabytes (GB), Terabytes (TB), and Petabytes (PB). Typical range is 256 GB to 4 TB for consumer drives. Larger capacity allows more files (documents, photos, videos, software) to be stored.

Monitor Size – Measured in Inches (in) diagonally from one corner of the screen to the opposite corner. Does not include the bezel (plastic frame) – only the actual display area. Typical sizes include 13-inch (laptop), 24-inch (desktop), 27-inch, 32-inch, and 49-inch (ultrawide). Aspect ratio (16:9, 16:10, 21:9) affects width and height for a given diagonal measurement.

Important Notes:

- Clock speed is not directly comparable across different processor families (e.g., an older 3.0 GHz processor may be slower than a newer 2.5 GHz processor due to architectural improvements)
- RAM and hard disk sizes are typically advertised using decimal gigabytes (1 GB = 1,000,000,000 bytes) while computers use binary gigabytes (1 GB = 1,073,741,824 bytes), causing apparent discrepancy
- Monitor size alone does not indicate resolution (e.g., a 24-inch monitor could be 1920x1080 or 3840x2160)

(c) Challenges Associated with the Use of External Hard Drives

Definition: An external hard drive is a portable storage device that connects to a computer via USB, Thunderbolt, or other interfaces to provide additional storage, backup capability, or data portability.

Physical Damage and Fragility – External hard drives (especially HDD types) contain moving parts. Dropping, bumping, or shaking while operating can cause head crashes and data loss. SSDs are more shock-resistant but still vulnerable.

Data Loss from Failure – All hard drives have finite lifespan (typically 3-5 years for HDDs). Sudden failure without warning can cause complete data loss. Recovery from failed drives is expensive (hundreds to thousands of dollars).

Speed Limitations (USB Bottlenecks) – External drives are limited by the speed of the connection interface. USB 2.0 is very slow (480 Mbps). Even USB 3.x may be slower than internal drive speeds. Large file transfers can take hours.

Portability Risks (Loss or Theft) – Small size makes external drives easy to lose or have stolen. Unencrypted drives expose all data to anyone who finds them. No remote wipe capability (unlike cloud storage).

Connection and Compatibility Issues – Different devices use different USB connector types. May require adapters or different cables. Different operating systems use different file formats (NTFS for Windows, APFS for Mac, ext4 for Linux). May need reformatting to work across different OS, which erases existing data.

Power Requirements – Some external drives require external power adapters (not bus-powered). Bus-powered drives may draw more power than some ports can supply (especially laptops). Insufficient power causes drive not to be recognised or to disconnect.

File System Corruption – Removing drive without safely ejecting can corrupt file system. Power loss during write operation can cause corruption. Corrupted drives may need reformatting (data loss) or repair (time-consuming). Cross-platform use increases corruption risk.

Fragmentation (HDD only) – Files become fragmented over time, slowing read/write speeds. Defragmentation takes time and requires free space. Frequent deletion and addition of files accelerates fragmentation. SSDs do not suffer from fragmentation.

Heat Generation – External drives generate heat during operation. Enclosed cases may trap heat, reducing lifespan. Sustained heavy use causes overheating, which accelerates component wear and failure.

Noise (HDD only) – Spinning platters create audible whirring sound. Read/write head movement creates clicking sounds. May be distracting in quiet environments.

Limited Lifespan – HDDs typically last 3-5 years under normal use. SSDs have limited write cycles (though high for consumer use). No warning before failure in many cases. Regular replacement is necessary.

Backup Discipline Required – External drives require manual backup initiation (unless software scheduled). Users may forget to back up regularly. Drive must be connected for scheduled backups to run. Offsite protection requires physically moving drive.

Malware and Virus Vulnerability – External drives can become infected when connected to infected computers. Malware can spread from external drive to other computers. Infected backups may restore malware after system clean.

Encryption and Security Management – Encrypting external drive protects data if lost but adds complexity. Forgotten encryption keys make data permanently inaccessible. Performance penalty when reading/writing encrypted data.

Obsolescence – Interface standards change (USB-A to USB-C, USB 3.0 to USB 3.2 to USB4). Older drives may not work with newer computers without adapters. Very old drives may be completely unusable with modern computers.

Cost per Gigabyte – Portable drives have higher cost per GB than desktop external drives. SSD external drives cost significantly more per GB than HDD. Cloud storage may be cheaper for small amounts of data over time.

Cable and Port Wear – USB cables fray or fail over time. Ports can become loose with frequent plugging/unplugging. Cable loss renders drive unusable until replaced.

Mitigation Strategies:

- Use external SSDs instead of HDDs for better shock resistance
- Encrypt sensitive data on external drives
- Follow 3-2-1 backup rule: 3 copies, 2 media types, 1 offsite
- Always safely eject drive before disconnecting
- Regularly check drive health using S.M.A.R.T. monitoring tools
- Replace drives every 3-5 years or at first sign of problems
- Use cloud storage as complement to (not replacement for) external drives

---

(d) Legal Issues Associated with the Use of Information Systems

Definition: Legal issues in information systems are the statutory, regulatory, and common law obligations and liabilities that arise from the development, deployment, and use of information technology in organisations.

1. Data Protection and Privacy Laws

Organisations must comply with laws governing collection, storage, use, and sharing of personal data. Key laws include Kenya Data Protection Act (DPA) 2019 and GDPR for EU citizen data. Obligations include obtaining informed consent, collecting only necessary data, implementing security measures, notifying authorities and affected individuals within 72 hours of a breach, allowing individuals to access and correct their data, and registering as data controller with ODPC. Consequences include fines up to KES 5 million or 1% of annual turnover, GDPR fines up to €20 million or 4% of global turnover, civil lawsuits, and reputational damage.

2. Intellectual Property Rights

Information systems involve software, digital content, databases, and creative works protected by copyright, patents, trademarks, and trade secrets. Obligations include not installing unlicensed software (software piracy), not

using copyrighted images or text without permission, respecting open source licence terms, and protecting the organisation's own IP. Consequences include lawsuits, statutory damages, injunctions, and criminal penalties for wilful infringement.

3. Computer Crime and Cybercrime Laws

Kenya's Computer Misuse and Cybercrimes Act 2018 prohibits unauthorised access (hacking), unauthorised data interception, unauthorised data modification or deletion, computer fraud, cyber harassment and stalking, and distribution of malware. Consequences include criminal prosecution, imprisonment (up to 10 years for some offences), fines, and civil liability to victims.

4. Electronic Transactions and Digital Signatures

Kenya Information and Communications Act recognises electronic signatures and electronic contracts as legally valid if properly authenticated. However, certain documents (wills, trusts, some property transfers) may require physical signatures. Organisations must retain electronic records as required by law. Consequences include unenforceable contracts, inadmissible evidence in court, and regulatory penalties.

5. Employment and Workplace Monitoring Laws

Employers may monitor employee use of company systems but must have written acceptable use policies, inform employees that monitoring may occur, limit monitoring to legitimate business purposes, and not monitor personal accounts (personal email, social media) even on company devices in many jurisdictions. Consequences include invasion of privacy lawsuits, labour disputes, unfair dismissal claims, and inadmissible evidence.

6. Accessibility Laws (Digital Inclusion)

Kenya's Persons with Disabilities Act 2003 and constitutional non-discrimination rights require that websites and digital services be accessible (WCAG 2.1 standards). Organisations must provide reasonable accommodations for employees with disabilities. Consequences include discrimination complaints, lawsuits, and regulatory action.

7. E-Commerce and Consumer Protection Laws

Consumer Protection Act 2012 requires clear disclosure of total price, accurate product descriptions, clear refund and return policies, right to cancel within specified period (cooling-off period), and secure payment processing. Consequences include refunds to affected customers, fines from Competition Authority of Kenya, civil lawsuits, and reputational damage.

8. Defamation and Online Content Liability

Organisations may be liable for defamatory content posted on their websites or social media. Defamation (libel) involves false statements that harm reputation. Safe harbour provisions protect platforms that promptly remove illegal content upon notice. Obligations include establishing content moderation policies, responding promptly to defamation complaints, and removing illegal content when notified. Consequences include defamation lawsuits, damages awarded to plaintiffs, and injunctions.

9. Data Retention and Destruction Laws

Laws require organisations to retain certain records for specified periods. Tax records: 5-7 years. Employment records: 3-5 years after employment ends. Healthcare records: minimum retention periods (e.g., 20 years under Kenya Digital Health Act). Proper destruction (shredding, degaussing, secure wipe) prevents data breaches. Consequences include penalties for destroying records too early, penalties for retaining records beyond required period, and liability for data breach from improper destruction.

10. Export Control and Data Transfer Laws

Data Protection Act 2019 restricts transfer of personal data to countries without adequate protection. ODPC may approve transfers with appropriate safeguards (binding corporate rules, standard contractual clauses). Obligations include assessing adequacy of destination country, implementing appropriate safeguards, and notifying data subjects of international transfers. Consequences include fines from ODPC, suspension of data transfers, and liability for breaches occurring in recipient country.

11. Jurisdiction and Applicable Law

Information systems often operate across national boundaries, creating uncertainty about which laws apply. Questions include: if server is in Country A, company in Country B, customer in Country C – which law applies? Can

foreign law enforcement access data stored in another country? Consequences include multiple lawsuits in multiple jurisdictions, conflicting legal obligations, and difficulty predicting legal exposure.

12. Liability for System Failures

Organisations may be liable for damages caused by information system failures, errors, or security breaches under legal theories of negligence (failed to exercise reasonable care), breach of contract (system does not meet specifications), or product liability (defective software or hardware). Consequences include lawsuits for financial losses, damages for business interruption, legal costs, and reputational damage.

Mitigation Strategies for Legal Compliance:

- **Data protection** – Appoint Data Protection Officer; register with ODPC; implement privacy policy; conduct Data Protection Impact Assessments (DPIA)
- **Intellectual property** – Use licence management tools; conduct regular software audits; implement IP protection strategy
- **Cybercrime** – Implement security controls; conduct employee training; maintain incident response plan
- **Electronic transactions** – Use secure digital signature solutions; retain records as required; comply with e-commerce regulations
- **Workplace monitoring** – Establish written policies; disclose monitoring; limit to legitimate purposes
- **Accessibility** – Follow WCAG guidelines; conduct accessibility testing; provide alternative formats
- **Consumer protection** – Clear terms and conditions; transparent pricing; fair return policies
- **Defamation** – Content moderation policy; prompt takedown procedures; legal review of sensitive content
- **Data retention** – Implement retention schedule; secure destruction procedures; document compliance
- **Cross-border data** – Assess adequacy; implement standard contractual clauses; binding corporate rules

- **Jurisdiction** – Specify governing law in terms of service; limit data collection where possible
- **System liability** – Maintain professional indemnity insurance; document testing and quality assurance; use disclaimers where appropriate

senm-answers.com

Email: customercare@senm-answers.com Tel: 254-734-053-765

CPA

Information Communication Technology

August 2023

Level: Foundation Level

Question 7

 Overview of operating systems, Computer networks , Information systems in an enterprise , Systems analysis and design

(a) Explain TWO ways in which an operating system acts as a resource manager.

(b) Highlight FOUR benefits of Internet of Things (IoT) in smart home.

(c) Outline SIX instances when you would recommend prototypes during system development.

(d) Examine SIX benefits associated with business processes integration.

✓ Answer for Question 7

(a) Ways an Operating System Acts as a Resource Manager

An operating system (OS) ensures efficient allocation and use of computer resources:

- **CPU management (Process scheduling)**
  Allocates CPU time to different processes using scheduling algorithms (e.g., multitasking).
- **Memory management**
  Allocates and deallocates RAM to programs; prevents one program from interfering with another.
- **File system management**
  Organizes, stores, and retrieves data on storage devices (files, directories, permissions).
- **Device management**
  Controls hardware devices (printers, disks, keyboard) via drivers and coordinates their use.
- **I/O management**
  Manages input/output operations and buffering to improve efficiency.
- **Security and access control**
  Ensures only authorized users/processes access resources.
- **Resource allocation and prioritization**
  Assigns resources based on priority to ensure optimal system performance.

(b) Benefits of Internet of Things (IoT) in a Smart Home

- **Automation of tasks**
  Devices like lights, thermostats, and appliances operate automatically.

- **Energy efficiency**
  Smart systems optimize electricity usage (e.g., auto-switching off unused devices).
- **Remote control**
  Home devices can be controlled from anywhere via smartphones.
- **Enhanced security**
  Smart cameras, alarms, and door locks improve home safety.
- **Convenience and comfort**
  Personalized settings (lighting, temperature) improve living conditions.
- **Real-time monitoring**
  Users can monitor home conditions (temperature, motion, energy usage).
- **Cost savings**
  Reduced energy consumption lowers utility bills.

(c) Instances Where Prototypes Are Recommended in System Development

Use prototyping when:

- **User requirements are unclear or evolving**
  Helps users visualize and refine their needs.
- **High user interaction systems**
  (e.g., mobile apps, websites) where usability is critical.
- **New or innovative systems**
  Where there is no existing model to follow.
- **Complex systems**
  Helps break down complexity and test parts early.
- **To get user feedback early**
  Reduces risk of developing the wrong system.
- **When time constraints exist**
  Quick models can be built to demonstrate concepts.
- **To test system feasibility**
  Confirms whether ideas are practical before full development.

(d) Benefits of Business Process Integration

- **Improved efficiency**
  Eliminates duplication of tasks across departments.
- **Better data flow**
  Seamless sharing of information between systems/functions.
- **Enhanced decision-making**
  Managers access accurate and real-time data.
- **Cost reduction**
  Reduced operational and administrative costs.
- **Improved customer service**
  Faster response and consistent service delivery.
- **Increased productivity**
  Employees spend less time on manual or repetitive tasks.
- **Greater organizational coordination**
  Departments work in sync toward common goals.
- **Competitive advantage**
  Faster, smarter operations improve market positioning.