CERTIFIED PUBLIC ACCOUNTANT
OPERATIONAL LEVEL EXAMINATION
DF2.2 DIGITAL FINANCE
DATE: TUESDAY 25, AUGUST 2026

SECTION A

Summary of Correct Answers - Section A

Q	Ans	Q	Ans	Q	Ans
1	**B**	11	**C**	21	**A**
2	**D**	12	**C**	22	**B**
3	**D**	13	**A**	23	**D**
4	**A**	14	**B**	24	**A**
5	**D**	15	**C**	25	**A**
6	**C**	16	**B**	26	**B**
7	**C**	17	**D**	27	**A**
8	**D**	18	**C**	28	**C**
9	**D**	19	**A**	29	**B**
10	**A**	20	**D**	30	**D**

Detailed Answers and Rationale

Question 1: Correct Answer - B

Automated on the fly reporting mechanisms

For an integrated data system aggregating epidemic data across multiple stakeholders, automation is the key enabler of both timeliness and accuracy - it removes manual delay and manual transcription errors from the reporting pipeline.

Why the other options are incorrect:

- A - A comprehensive historical data repository: supports depth/comprehensiveness of analysis but does nothing to make the ongoing aggregation of new data timely or accurate.
- C - Strict role-based access controls: this is a security/confidentiality measure; it protects who can see the data but does not improve the speed or accuracy of aggregation.
- D - Routine manual data validation: manual processes are inherently slower and more error-prone than automated ones, so this works against the 'timely' requirement.

Question 2: Correct Answer - D

(i) and (iv) - Minimising manual interaction during data validation; Employing dynamic workflows for error resolution

Minimising manual interaction speeds up processing and reduces human error (supports speed and integrity), while dynamic workflows for error resolution directly addresses error prevention.

Why the other options are incorrect:

- A - (i) and (ii): multiple ETL pipeline backups protect against data loss/failure, not against errors being introduced, so it does not address error prevention as directly as (iv).
- B - (ii) and (iii): restricting real-time validation to predefined categories actually narrows error-checking coverage, working against error prevention rather than supporting it.

- C - (iii) and (iv): restricting real-time validation (iii) undermines data integrity even though dynamic error-resolution workflows (iv) helps, making this an inconsistent pairing.

Question 3: Correct Answer - D

Keep satisfied, but not overly engaged

The shareholders described have High Power (voting rights over strategy) but Low Interest (little day-to-day interest in the IT rollout). On the Power/Interest Grid, the High Power/Low Interest quadrant calls for a 'keep satisfied' strategy.

Why the other options are incorrect:

- A - Engage closely and keep satisfied: this strategy is for High Power/High Interest stakeholders, but this group has shown little interest in the technical details.
- B - Keep informed and communicate regularly: this strategy is for Low Power/High Interest stakeholders; these shareholders have high power, not low.
- C - Monitor with minimal communication: this strategy is for Low Power/Low Interest stakeholders; these shareholders hold considerable power, so minimal engagement would be inappropriate.

Question 4: Correct Answer - A

Zachman Framework

The Zachman Framework is a classification schema (ontology) that cross-references six communication questions - What, How, Where, Who, When, Why - against six stakeholder perspectives (Planner, Owner, Designer, Builder, Sub-Contractor/Implementer, and the Functioning Enterprise).

Why the other options are incorrect:

- B - TOGAF: is a process-driven methodology (a step-by-step architecture development method), not a classification matrix of questions against perspectives.
- C - COBIT: is an IT governance and control-objectives framework, unrelated to the six-questions/six-perspectives structure described.
- D - ITIL: is a service-management framework focused on delivering and supporting IT services, not an enterprise architecture classification schema.

Question 5: Correct Answer - D

(iii) and (iv) - Transparent communication with customers during transition; Regular system monitoring and immediate error resolution

'Seamless customer experience post-deployment' points to what happens during and after go-live from the customer's perspective: keeping customers informed and promptly resolving errors as they use the live system.

Why the other options are incorrect:

- A - (i) and (ii): employee training and testing with real-world scenarios both happen before go-live; they prepare the system but are not themselves post-deployment customer-facing practices.
- B - (ii) and (iv): testing (ii) is a pre-deployment quality-assurance activity, so pairing it with monitoring (iv) mixes a 'before' activity with an 'after' one rather than focusing on the post-deployment customer experience.

- C - (i) and (iii): employee training (i) is a pre-deployment preparation step, not something that directly shapes the customer's experience once the system is live.

Question 6: Correct Answer - C

Platform as a Service (PaaS)

PaaS gives developers a ready platform (runtime, OS, database and middleware managed by the provider) so they only need to write and deploy application code - exactly what the fintech's engineers want.

Why the other options are incorrect:

- A - IaaS: the client is still responsible for managing the operating system, databases and middleware themselves; only the physical infrastructure/servers are outsourced, which does not match the 'developers only think about application logic' requirement.
- B - SaaS: delivers a complete, ready-to-use application to end users; it is not a platform on which a company's own developers write and deploy their own code.
- D - On-site service delivery: means the company runs and manages everything itself on its own premises, the opposite of wanting a provider to handle the underlying infrastructure.

Question 7: Correct Answer - C

Recovery Time Objective (RTO)

RTO is the target time within which a system must be restored after a disruption. The 12-hour restoration target sits inside (and is set to avoid breaching) the 24-hour Maximum Tolerable Downtime (MTD).

Why the other options are incorrect:

- A - MTD: is the outer limit (24 hours) that must not be breached; the 12-hour figure is a target set within that limit, not the MTD itself.
- B - RPO: measures the maximum acceptable amount of data loss (measured in time since the last backup), not the time taken to restore the system.
- D - SDO: relates to the level/quality of service to be restored (e.g. partial vs full functionality), not the time taken to restore it.

Question 8: Correct Answer - D

(i) and (iv) - Training procurement officers on system usage and reporting; Establishing key performance metrics and dashboards

Transparency and efficiency in year one are best built by equipping officers to use and report on the system properly (training) and by establishing KPIs/dashboards that make performance and tendering activity visible to stakeholders.

Why the other options are incorrect:

- A - (i) and (iii): supplier registration compliance (iii) supports fair participation but does not, on its own, make ongoing performance and process visible to stakeholders the way dashboards do.
- B - (ii) and (iv): mandating external audits (ii) is a periodic, retrospective control rather than a first-year adoption driver of day-to-day transparency and efficiency; it also leaves out staff capability (training).

- C - (iii) and (iv): supplier registration compliance (iii) addresses fairness of participation, not officers' ability to operate and report on the system, which training (i) directly provides.

Question 9: Correct Answer - D

Warm site

A warm site has partially configured servers and a replicated copy of data but needs some additional set-up before becoming fully operational - offered at a lower cost than a hot site or mirrored site.

Why the other options are incorrect:

- A - Mirrored/Replicated site: is fully synchronised and offers near-instantaneous failover with no set-up delay, but at a much higher cost than the bank is willing to accept.
- B - Hot site: is fully equipped and can be activated almost instantly, so it would not require 'a short period of additional set-up work' and typically costs more than a warm site.
- C - Cold site: is an empty facility with only basic infrastructure; bringing it into operation takes considerably longer than 'a short period', which contradicts the scenario.

Question 10: Correct Answer - A

Incremental backup

An incremental backup captures only the data changed since the immediately preceding backup (whether that was a full or another incremental backup), minimising daily backup time/storage, but requiring every backup in the chain to be restored in sequence.

Why the other options are incorrect:

- B - Full backup: creates a complete, independent copy of all data every time, which takes far more time and storage than capturing only the changes since the last backup.
- C - Differential backup: always backs up everything changed since the last FULL backup (not the immediately preceding backup), and restoration only needs the last full plus the latest differential - it does not require replaying every backup in sequence.
- D - Mirrored backup: keeps a continuously synchronised duplicate copy of data rather than periodic backups of changed data, so it does not match the 'daily routine capturing only changed data' description.

Question 11: Correct Answer - C

(iii) and (iv) - Ensuring hardware compatibility across legacy and new systems; Developing scalable cloud-based infrastructure

Hardware compatibility between legacy and new smart-grid devices prevents data-transmission/read errors during integration (supporting accuracy), while scalable cloud infrastructure directly delivers the scalability needed for a stable, growing network.

Why the other options are incorrect:

- A - (i) and (ii): predictive maintenance (ii) improves reliability/asset upkeep but does not, by itself, deliver the network's scalability that the scenario prioritises.
- B - (ii) and (iv): predictive maintenance (ii) is about forecasting equipment failure, not about ensuring data accuracy, so it is a weaker partner for cloud infrastructure (iv) than hardware compatibility (iii).

- D - (i) and (iii): real-time data validation (i) and hardware compatibility (iii) both support accuracy/integration, but neither directly builds the scalable infrastructure that the stem also asks for.

Question 12: Correct Answer - C

Waterfall

Fixed, regulation-driven requirements with formal sign-off of each phase (requirements, design, build, testing) before the next begins is the defining feature of the Waterfall model.

Why the other options are incorrect:

- A - Agile: is iterative and specifically designed to accommodate changing requirements through short cycles, the opposite of requirements being fixed and phases being formally closed off before moving on.
- B - Scrum: is a specific Agile framework built around short, flexible sprints and incremental delivery, not sequential, fully-signed-off phases.
- D - Hybrid rapid prototyping: combines iterative prototyping with structure, which conflicts with the strict, linear, fully-documented phase-by-phase sign-off described in the scenario.

Question 13: Correct Answer - A

Reinforcement

Awareness, Desire, Knowledge and Ability have all clearly been achieved (staff understand why, and can competently operate the system), but without mechanisms to sustain the change, staff have reverted to old habits - precisely the gap addressed by ADKAR's final stage, Reinforcement.

Why the other options are incorrect:

- B - Awareness: has already been achieved - the scenario states employees 'understand why' the system was introduced.
- C - Knowledge: has already been achieved - staff 'have completed the training needed', which is how ADKAR knowledge is built.
- D - Ability: has already been achieved - staff can operate the system 'competently', which is what the Ability stage delivers.

Question 14: Correct Answer - B

Software as a Service solution

No upfront infrastructure investment, acceptance of standard (non-customised) functionality, and the ability to scale usage up and down with demand are the hallmark characteristics of SaaS.

Why the other options are incorrect:

- A - Off-the-shelf package: is typically a purchased/licensed product that may still require infrastructure to run and does not naturally flex usage up and down monthly the way a subscription cloud service does.
- C - Hybrid solution: combines custom-built and packaged/SaaS elements, which implies more development time and investment than the company (needing a solution 'immediately') is willing to commit to.

- D - Custom-built system: requires significant upfront investment and a longer development cycle, directly contradicting the need for something immediate with no upfront infrastructure cost.

Question 15: Correct Answer - C

(i) and (ii) - Real-time disease incidence mapping; Predictive modelling for outbreak hotspots

The scenario emphasises predictive analytics and data visualisation specifically. Real-time incidence mapping is the visualisation element and predictive modelling for hotspots is the predictive-analytics element - a direct match to both stated priorities.

Why the other options are incorrect:

- A - (i) and (iii): integration with international health databases (iii) is a data-sourcing/interoperability feature, not itself a predictive-analytics capability.
- B - (ii) and (iv): automated alerts (iv) are a response/notification feature that follows from analytics, but is not itself the 'data visualisation' emphasised in the stem.
- D - (iii) and (iv): neither international database integration (iii) nor automated alerts (iv) is, by itself, a predictive-analytics or data-visualisation feature, so this pairing misses both named priorities.

Question 16: Correct Answer - B

Velocity

Velocity refers to the speed at which data is generated and must be processed. A continuous, rapid stream of records arriving faster than traditional systems can process is a textbook description of Velocity.

Why the other options are incorrect:

- A - Volume: refers to the total quantity/scale of data generated, not the speed at which it arrives; the scenario emphasises speed of inflow, not sheer size.
- C - Variety: refers to the different types/formats of data (structured, unstructured, text, images, etc.), which is not what is being described here.
- D - Veracity: refers to the trustworthiness and quality/accuracy of data, not the speed at which it is generated or processed.

Question 17: Correct Answer - D

Machine Learning

A model that automatically and continuously updates itself from new data to improve its own predictive accuracy - without a programmer rewriting rules - is the defining characteristic of Machine Learning.

Why the other options are incorrect:

- A - Robotic Process Automation: automates repetitive, rule-based tasks according to fixed rules; it does not learn from data or improve its own accuracy over time.
- B - Blockchain: is a distributed ledger technology for secure, shared record-keeping; it has no self-improving predictive capability.
- C - Structured Threat Analysis: is a manual/structured method used in risk and security analysis, not an automated, self-improving predictive model.

Question 18: Correct Answer - C

(i) and (ii) - Resistance from staff unfamiliar with automated workflows; Limited compatibility with existing infrastructure

Adoption risk is most directly driven by (i) staff resistance to unfamiliar automated workflows together with (ii) limited compatibility with existing infrastructure, which causes operational friction that further undermines adoption.

Why the other options are incorrect:

- A - (i) and (iii): high costs of hardware upgrades (iii) is primarily a budgeting/financial risk to the project, not a direct driver of whether users adopt and use the system.
- B - (ii) and (iv): this pairing omits staff resistance (i), which is the most direct human/behavioural driver of adoption risk described in change-management theory.
- D - (iii) and (iv): hardware cost (iii) and unclear communication (iv) are relevant concerns, but neither captures the direct user-behaviour resistance (i) that most strongly determines whether a system is adopted.

Question 19: Correct Answer - A

Blockchain

A shared, tamper-evident (immutable) record that multiple unrelated parties can trust without a single party being able to alter it after the fact is the core value proposition of Blockchain/distributed ledger technology.

Why the other options are incorrect:

- B - Robotic Process Automation: automates repetitive process tasks; it has no inherent capability to create a shared, unalterable multi-party ledger.
- C - Business Intelligence: is used to analyse and report on data for decision-making; it does not provide a tamper-proof shared transaction record.
- D - Security Information and Event Management (SIEM): is a security monitoring and event-logging tool, not a mechanism for creating a trusted, immutable shared ledger among independent parties.

Question 20: Correct Answer - D

Lack of public access to real-time bidding status

Since the specific goal being tested is transparency, the factor most directly undermining transparency is the public's inability to see real-time bidding information.

Why the other options are incorrect:

- A - Complexity in verifying bidder credentials: this is more of an operational/due-diligence challenge affecting efficiency and compliance verification, not the public's ability to see the process.
- B - Inconsistent data formats from legacy systems: this is a data-integration/efficiency issue that hampers system performance, rather than a direct barrier to public visibility of the process.
- C - Insufficient training for procurement officers: this affects how well officers can operate/report on the system (an efficiency/capability issue) rather than being the main obstacle to public transparency.

Question 21: Correct Answer - A

(i) and (ii) - Real-time runway availability tracking; Automated invoicing for landing fees

The MIS is described as focusing on two things - landing scheduling and fees. Real-time runway tracking directly supports scheduling efficiency, and automated invoicing directly supports efficient fee administration.

Why the other options are incorrect:

- B - (ii) and (iv): standardised communication templates (iv) support general ATC communication but do not address scheduling efficiency as directly as runway availability tracking does.
- C - (i) and (iii): weather monitoring integration (iii) supports safety/operational awareness rather than the fee-administration half of the stem's stated focus.
- D - (iii) and (iv): neither weather integration (iii) nor communication templates (iv) directly addresses automated fee invoicing, missing one of the two elements explicitly named in the stem.

Question 22: Correct Answer - B

Data residency

Data residency concerns the physical/geographic location in which data is stored and which jurisdiction's laws therefore govern it - precisely the issue raised when a bank's customer data sits on servers in another country.

Why the other options are incorrect:

- A - Data classification: is about categorising data according to its sensitivity level (e.g. public, confidential, restricted), not about which country's laws apply based on server location.
- C - Data enrichment: is the process of enhancing existing data with additional information from other sources; it has nothing to do with jurisdiction or storage location.
- D - Data warehousing: refers to consolidating data for storage and reporting/analysis purposes, not to the legal jurisdiction governing where that data physically resides.

Question 23: Correct Answer - D

Best of Breed approach

Selecting the specific specialised software that best fits each department's unique needs - accepting extra integration complexity for deeper functionality - is the definition of a Best of Breed approach.

Why the other options are incorrect:

- A - Enterprise Resource Planning (ERP): is a single integrated system used across departments, the opposite of each department choosing its own separate specialised software.
- B - Integrated Financial Management Information System (IFMIS): is also an integrated, unified system (typically for public financial management), not a collection of separately chosen specialised systems.
- C - Robotic Process Automation: automates repetitive tasks within a process; it is not a system-selection strategy for choosing between integrated and specialised software.

Question 24: Correct Answer - A

(i) and (iv) - Complex user interface difficult for non-technical staff; Inadequate training for faculty

User acceptance is most directly hindered by usability problems (a complex interface non-technical staff struggle with) combined with inadequate training - both are direct barriers to users being willing and able to use the system.

Why the other options are incorrect:

- B - (ii) and (iii): lack of integration with legacy systems (ii) and update delays during peak periods (iii) are technical/operational challenges affecting system performance, rather than direct drivers of whether users personally accept and adopt the system.
- C - (i) and (iii): pairing interface complexity (i) with update delays (iii) leaves out the training gap (iv), which is one of the most direct and well-established causes of poor user acceptance.
- D - (ii) and (iv): integration gaps (ii) are a technical issue rather than a user-facing acceptance barrier, making this a weaker pairing than interface complexity (i) with training (iv).

Question 25: Correct Answer - A

Cloud-based data storage solutions

Cloud-based storage is elastic by design, allowing capacity to expand rapidly on demand during a pandemic surge - the clearest strategy for ensuring scalability.

Why the other options are incorrect:

- B - Regular stress testing for high user loads: verifies how the system behaves under load and identifies weaknesses, but does not itself provide the extra capacity needed to scale.
- C - Open-source development for community contributions: can broaden development resources and features over time, but does not directly ensure the system can scale to handle sudden surges in demand.
- D - On-premise server-based infrastructure: has fixed, finite capacity that is costly and slow to expand, making it the opposite of a scalable solution for responding to future pandemic surges.

Question 26: Correct Answer - B

Identify

Cataloguing critical assets and then compiling a list of threats/vulnerabilities affecting them - before any controls are deployed - is precisely the Identify stage of the security lifecycle.

Why the other options are incorrect:

- A - Protect: involves implementing safeguards (access controls, encryption, firewalls) - but the scenario states 'no protective controls have yet been deployed', so this stage has not yet begun.
- C - Detect: involves monitoring the environment for signs of incidents (e.g. via SIEM, intrusion detection) once controls are in place - the team here has not reached ongoing monitoring, only initial cataloguing.
- D - Respond: involves taking action to contain and mitigate an actual incident, which is not relevant since no incident or protective control is described in this scenario yet.

Question 27: Correct Answer - A

(i) and (iv) - Implementing blockchain technology for secure transaction records; Conducting periodic third-party data audits

Data integrity is best supported by a technology that makes records tamper-evident (blockchain) together with independent verification that records remain accurate and unaltered (periodic third-party audits).

Why the other options are incorrect:

- B - (ii) and (iii): regularly updating records (ii) keeps data current, and restricting access (iii) protects confidentiality, but neither directly verifies or guarantees that records have not been altered - the core meaning of integrity.
- C - (i) and (ii): blockchain (i) supports integrity well, but regular updates (ii) alone do not provide independent verification of accuracy, which periodic audits (iv) add.
- D - (iii) and (iv): restricting access (iii) is a confidentiality control rather than a direct integrity-verification mechanism; it is a weaker partner for audits (iv) than the tamper-evident record-keeping blockchain (i) provides.

Question 28: Correct Answer - C

15%

Shortfall = 99.9% − 99.6% = 0.3%. At 5% credit per 0.1% shortfall, that is (0.3 ÷ 0.1) × 5% = 3 × 5% = 15%.

Why the other options are incorrect:

- A - 5%: this is the credit for only a single 0.1% shortfall increment, but the actual shortfall of 0.3% represents three such increments.
- B - 0.3%: this is simply the uptime shortfall itself (99.9% − 99.6%), not the service credit percentage that shortfall translates into.
- D - 0.1%: this is the size of one shortfall increment used in the SLA formula, not the total credit percentage owed for the month.

Question 29: Correct Answer - B

SOC 2 report

A SOC 2 report is a standardised, independently produced assurance report evaluating a service organisation's controls over security, availability, processing integrity, confidentiality and/or privacy - exactly what is needed when a client cannot inspect a vendor's data centre directly.

Why the other options are incorrect:

- A - Business Impact Assessment: is an internal analysis of the impact of disruptions on the requesting organisation's own operations, not an independent third-party assurance report on a vendor's controls.
- C - MoSCoW analysis: is a requirements-prioritisation technique (Must have/Should have/Could have/Won't have), unrelated to vendor control assurance.
- D - RACI matrix: is a responsibility-assignment tool (Responsible/Accountable/Consulted/Informed) used for organising project roles, not a vendor assurance report.

Question 30: Correct Answer - D

(ii) and (iii) - Intermittent network connectivity in remote areas; Limited capacity of utility staff to manage new meters

Successful implementation of automated prepaid metering is most directly hindered by operational/technical constraints - unreliable connectivity in remote areas and insufficient staff capacity to manage the new meters.

Why the other options are incorrect:

- A - (i) and (iii): consumer resistance due to installation costs (i) is more of an adoption/acceptance issue than a direct operational barrier to implementation, unlike connectivity (ii).
- B - (ii) and (iv): data breaches during meter readings (iv) is a security risk that could arise after implementation, rather than a challenge to getting the rollout itself successfully implemented.
- C - (i) and (iv): neither consumer cost resistance (i) nor data breach risk (iv) speaks to the practical operational challenges of rolling out the technology (connectivity and staff capacity) described as the priority in the stem.

SECTION B

QUESTION 31

(a) Explain how RRA could apply descriptive and predictive analytics to achieve these two objectives. (5 Marks)

Marking Guide

- 1 mark - Defines/explains descriptive analytics (analysing historical and current data to understand what has happened / identify patterns).
- 1 mark - Correct application of descriptive analytics to the scenario: analysing historical VAT, income tax and customs filing data to identify inconsistent filing patterns and flag categories of taxpayers likely to be under-declaring income.
- 1 mark - Defines/explains predictive analytics (using statistical techniques, data mining and machine learning on historical data to forecast future outcomes).
- 1 mark - Correct application of predictive analytics to forecasting revenue collection targets for the coming year using historical trends and patterns.
- 1 mark - Correct application of predictive analytics to guiding the deployment of audit staff (risk-scoring/predicting which taxpayers or segments are most likely to under-declare).
- (Maximum 5 marks. Award marks for any well-explained, relevant application even if presented differently from the points above.)

Model Answer

Descriptive analytics involves analysing historical and current data to summarise and understand what has already happened, identifying patterns, trends and anomalies in the data. RRA generates large volumes of structured and unstructured data from its VAT, income tax and customs systems. By applying descriptive analytics to this data, RRA can compare filing patterns across different categories of taxpayers, industries and regions, and identify inconsistencies - such as declared income that is unusually low relative to sector norms, sudden drops in reported turnover, or mismatches between VAT and income-tax declarations for the same taxpayer. This directly supports management's suspicion that some businesses may be under-declaring income, by turning raw transaction data into a clear picture of where filing behaviour looks abnormal.

Predictive analytics goes further, using statistical algorithms and machine learning to analyse historical data and forecast future outcomes. RRA can build predictive models that assign a risk score to taxpayers or taxpayer segments based on historical non-compliance patterns, helping senior management decide where to deploy audit staff for maximum impact rather than auditing at random or reactively. The same predictive techniques can be applied to historical collection data, seasonal patterns and economic indicators to forecast revenue collection targets for the coming year. Together, this allows the Commissioner General's office to move away from static, year-end summary reporting and instead use continuously updated, forward-looking insights to guide ongoing strategic decisions on audit deployment and revenue forecasting.

(b) State THREE benefits RRA would gain from adopting a data-driven approach to decision-making. (3 Marks)

Marking Guide

- 1 mark for each distinct, valid benefit stated (up to 3). Acceptable benefits include (any three):
- More accurate, objective decision-making (decisions based on evidence rather than assumption or intuition).
- More efficient allocation of scarce audit resources/staff to higher-risk taxpayers.
- Improved revenue forecasting and collection, and earlier detection of under-declaration/non-compliance.
- Greater transparency and accountability in how strategic decisions are made.
- Faster, more agile response to emerging filing/compliance trends.

Model Answer

1. Improved decision-making: Decisions on audit deployment and revenue targets are grounded in objective evidence from actual taxpayer data rather than assumption, improving accuracy and reducing bias.

2. Efficient use of resources: Audit staff and other scarce resources can be targeted at the taxpayer segments identified as highest-risk, improving productivity and the return on audit effort.

3. Increased revenue collection and compliance: Earlier and more reliable detection of under-declaration, combined with more accurate revenue forecasting, helps RRA close compliance gaps and meet collection targets.

QUESTION 32

(a) Explain TWO data collection methods the hospital could use to ensure accurate and reliable data capture from its suppliers. (4 Marks)

Marking Guide

- 2 marks for each method explained (1 mark for correctly naming/identifying the method, 1 mark for explaining how it improves accuracy/reliability over the current manual paper process). Maximum 4 marks for any two valid methods, which may include:
- Electronic Data Interchange (EDI) / automated system-to-system data capture between the supplier and the hospital's system.
- An online supplier portal for suppliers to enter delivery data directly into the system.
- Barcode/RFID scanning of stock at the point of receipt into the central pharmacy store.
- Automated data validation checks/mandatory fields built into the electronic capture forms.

Model Answer

1. Electronic Data Interchange (EDI) or an automated supplier portal: Instead of suppliers submitting delivery records manually on paper, the hospital could require suppliers to transmit delivery and invoice data electronically (via EDI) or to enter it directly into a supplier web-portal linked to the supply chain system. This removes the manual re-keying step that was causing errors, creates a digital audit trail, and ensures data is captured at the source in a consistent format.

2. Barcode/RFID scanning with built-in validation checks: Each batch of pharmaceuticals could be tagged with a barcode or RFID label that is scanned on receipt at the central pharmacy and again when stock moves out to wards. The system can enforce mandatory fields and validation rules (e.g. rejecting quantities or expiry dates that fall outside expected ranges) at the point of capture, ensuring data is complete, consistent and reliable before it enters the stock records.

(b) Describe TWO due diligence steps the hospital should undertake when selecting pharmaceutical suppliers for this system. (4 Marks)

Marking Guide

- 2 marks for each due diligence step described (1 mark for identifying the step, 1 mark for describing what it involves/why it matters for this scenario). Maximum 4 marks for any two valid steps, which may include:
- Financial stability and viability check (reviewing financial records, credit history and bank references).
- Legal and regulatory compliance check (verifying licences/certifications to supply pharmaceuticals, and compliance with relevant health/quality standards).
- Reputation and track record check (references from other health facilities, history of on-time/accurate deliveries, any past disputes).
- Operational capacity assessment (ability to reliably deliver the required volumes on schedule).

Model Answer

1. Financial stability and viability assessment: The hospital should review each supplier's financial records, credit history and bank references to confirm the supplier has the financial resources to reliably fulfil supply contracts on an ongoing basis. This reduces the risk of stock-outs caused by a supplier being unable to sustain deliveries because of financial difficulty - a particular concern given the hospital's long-serving suppliers were never formally evaluated.

2. Regulatory compliance and reputation check: The hospital should verify that each supplier holds the required licences/certifications to supply pharmaceuticals and complies with applicable quality and safety regulations, and should check references and past performance with other health facilities. This ensures medicines are sourced from properly licensed, reputable suppliers with a demonstrated record of reliable, accurate deliveries, directly addressing the Procurement Manager's mandate to properly vet new and continuing suppliers.

QUESTION 33

(a) Explain FOUR factors the authority should consider when deciding whether to buy an off-the-shelf system or develop the system in-house. (4 Marks)

Marking Guide

- 1 mark for each relevant factor correctly identified and briefly explained (up to 4). Acceptable factors include (any four):
- Cost/budget available (custom build generally requires higher upfront investment than a package).
- Time available before go-live (an off-the-shelf system is typically faster to implement than a six-month custom build).

- Degree of customisation/control needed (whether the authority's billing rules and reconciliation needs are standard or unique).
- Availability of in-house technical skills/capacity to build and maintain a custom system.
- Level of risk tolerance and data-security/control requirements.
- Ease of integration with existing property-ownership/payment records and future scalability/maintenance needs.

Model Answer

1. Cost and available budget: A custom build generally requires a larger upfront investment in development and specialist resources than purchasing a ready-made package, so the authority must weigh what it can afford against council-approved funding.

2. Time available before go-live: With only six months to go-live, an off-the-shelf solution is normally quicker to procure and configure than developing and testing a system from scratch in-house, which is a significant factor given the tight deadline.

3. Degree of customisation required: The authority should assess whether its billing rules, rate structures and reconciliation needs are largely standard (favouring an off-the-shelf package) or unique to its context (favouring an in-house build that can be tailored exactly to its requirements).

4. In-house technical capacity: The authority should consider whether its IT department has the skills, staffing and experience to design, build, test and subsequently maintain a custom billing system, or whether this capacity gap makes a vendor package the safer choice.

(b) Describe FOUR change management activities the authority should undertake to support successful adoption of the new system. (4 Marks)

Marking Guide

- 1 mark for each relevant, clearly described change management activity (up to 4). Acceptable activities include (any four):
- Building awareness/communicating the reasons for the change to staff and property owners.
- Training staff (and, where relevant, informing property owners) on how to use the new system/process.
- Engaging key stakeholders (staff, property owners, council) early in the planning process to build buy-in and reduce resistance.
- Piloting/testing the system with a subset of records or users before full go-live.
- Putting in place post go-live support and reinforcement mechanisms (help-desk, monitoring, feedback channels) to sustain the new way of working.

Model Answer

1. Awareness and communication campaign: The authority should communicate clearly to staff and property owners why the manual process is being replaced and what the benefits (fewer errors, faster billing, easier reconciliation) will be, well ahead of go-live.

2. Staff training: District office staff who currently rely on the manual, paper-based registers need structured training on the new automated billing system so they are competent and confident to operate it from day one.

3. Stakeholder engagement: The project team should engage staff and property owners early - for example through consultations or pilot feedback sessions - so their concerns are addressed and they feel ownership of the change, reducing resistance.

4. Post-go-live support and reinforcement: The authority should establish a help-desk/support mechanism and monitor usage after go-live to resolve issues quickly and reinforce the new process, preventing staff from reverting to the old manual registers.

QUESTION 34

(a) Recommend and justify an appropriate data presentation approach for branch managers and for the Board. (4 Marks)

Marking Guide

- 2 marks for branch managers (1 mark recommendation, 1 mark justification).
- 2 marks for the Board (1 mark recommendation, 1 mark justification).
- Branch managers: an automated dashboard/BI tool (e.g. Power BI/Tableau) presenting portfolio KPIs, with drill-down detail, replacing manual compilation of raw transaction extracts - saves time, reduces error, and gives operational-level detail.
- Board: a concise, high-level executive summary/scorecard with key trends and KPIs presented visually - appropriate given the Board's limited meeting time and need for quick, digestible insight rather than lengthy printed reports.

Model Answer

For branch managers: An automated BI dashboard (e.g. built in Power BI or Tableau) that draws directly from the transaction data and automatically compiles the required portfolio performance metrics is recommended, rather than manually compiled reports. This is justified because branch managers currently spend time manually compiling reports from raw e-mailed extracts, which is slow and error-prone; a dashboard would save time, reduce transcription errors, and give managers the ability to drill down into the operational-level detail they need to manage their portfolios day to day.

For the Board: A concise executive summary/scorecard presenting high-level KPIs and trend charts (rather than lengthy printed reports) is recommended for the Board. This is justified by the Board's limited meeting time and its need for strategic, digestible insight rather than granular transaction-level detail - a small number of clear visuals and headline figures allow directors to quickly grasp portfolio performance and focus discussion on strategic implications.

(b) Explain TWO measures the bank should implement to protect the sensitive customer data used in producing these reports. (4 Marks)

Marking Guide

- 2 marks for each measure explained (1 mark for identifying the measure, 1 mark for explaining how it protects the data in this context). Maximum 4 marks for any two valid measures, which may include:
- Encryption of data at rest and in transit as it is extracted and shared across departments.

- Role-based access controls (restricting access to income/collateral data to only those who need it).
- Data masking/anonymisation of sensitive fields where full detail is not required for the report.
- Audit logging/monitoring of who accesses or extracts the data.

Model Answer

1. Encryption: Customer income and collateral data should be encrypted both at rest (in storage) and in transit (when extracted and shared between departments), so that even if the data is intercepted or accessed without authorisation, it remains unreadable and unusable. This directly addresses the Head of IT's concern that data is not adequately protected as it moves across departments.

2. Role-based access control (RBAC): Access to sensitive fields such as income details and collateral records should be restricted based on job role, so that only staff who genuinely need this information to produce or use the reports (e.g. relevant risk/finance staff) can view it. This limits the number of people who can access sensitive data and reduces the risk of internal misuse or accidental disclosure.

QUESTION 35

(a) Explain the steps in the risk assessment process the company should follow to evaluate the risks introduced by the new mobile application. (5 Marks)

Marking Guide

- 1 mark - Risk Identification: systematically identifying the risks introduced by the app (e.g. via review, workshops, testing) covering data privacy and payment-related risks.
- 1 mark - Risk Analysis: analysing the likelihood and potential impact of each identified risk, considering the company's risk appetite/tolerance (inherent vs residual risk).
- 1 mark - Risk Evaluation: comparing the analysed risks against the company's risk appetite/tolerance/capacity to prioritise which risks most urgently need addressing.
- 1 mark - Risk Treatment: developing and implementing a plan to mitigate, transfer, avoid or accept the identified risks (e.g. before extending the app to life insurance claims).
- 1 mark - Recognising that the process is an ongoing/cyclical one that should be reviewed regularly as the app's use expands (e.g. to life insurance claims), and/or overall clarity and logical sequencing of the answer.

Model Answer

The company should follow a structured, four-stage risk assessment process:

1. Risk Identification: The Head of Risk should lead a systematic exercise (e.g. workshops with IT, claims, compliance and risk teams, review of the app's data flows, and testing) to identify all the risks the mobile application introduces - particularly around the personal customer data it collects and the payment-related information it processes, such as data breaches, unauthorised access, and fraudulent claims.

2. Risk Analysis: Each identified risk should then be analysed to determine the likelihood of it occurring and the potential impact if it does, taking into account the company's risk appetite and tolerance. This should distinguish between inherent risk (before any controls) and residual risk (after existing controls, if any, are considered), using qualitative (high/medium/low) or quantitative methods as appropriate.

3. Risk Evaluation: The analysed risks should be evaluated against the company's risk appetite, tolerance and capacity, allowing the company to prioritise which risks are most significant and require urgent attention - for example, risks around payment data are likely to rank as high priority.

4. Risk Treatment: Finally, the company should develop and implement a risk mitigation plan for the prioritised risks - mitigating (e.g. through new security controls), transferring (e.g. insurance), avoiding, or accepting each risk as appropriate. This treatment plan should be completed and reviewed before the application is extended to cover life insurance claims, and the whole risk assessment process should be treated as an ongoing cycle that is revisited as the app's functionality and risk profile evolve.

(b) Recommend THREE risk control measures the company could adopt to mitigate the identified risks. (3 Marks)

Marking Guide

- 1 mark for each distinct, valid risk control measure (up to 3). Acceptable measures include (any three):
- Encryption of personal data and payment information (at rest and in transit).
- Multi-factor authentication (MFA) for customer access to the app.
- Secure, PCI-DSS-compliant payment gateway/tokenisation for processing payment-related information.
- Regular security/penetration testing of the application.
- Role-based access controls and monitoring/logging of access to customer data.
- Staff/customer awareness on secure use of the app and incident-response planning.

Model Answer

1. Encryption: Encrypt personal customer data and payment-related information both at rest and in transit, so that intercepted or improperly accessed data cannot be read or misused.

2. Multi-factor authentication (MFA): Require MFA for customers logging into the app, reducing the risk of unauthorised access to accounts and the personal/claims data they contain.

3. Secure payment processing and regular security testing: Use a secure, PCI-DSS-compliant payment gateway (with tokenisation, so the app itself never stores raw card data) and conduct regular penetration testing of the application to identify and close vulnerabilities before the app is extended to life insurance claims.