PassQueen
a.k.a dumpsqueen.com

Data Management Fundamentals

DAMA DMF-1220

Version Demo

Total Demo Questions: 75

Total Premium Questions: 750

Buy Premium PDF

https://passqueen.com

support@passqueen.com

Topic Break Down

Topic	No. of Questions
Topic 1, Data Governance	200
Topic 2, Data Architecture	60
Topic 3, Data Modeling & Design	51
Topic 4, Data Storage & Operations	41
Topic 5, Data Security	52
Topic 6, Data Integration & Interoperability	51
Topic 7, Document & Content Management	34
Topic 8, Reference & Master Data	48
Topic 9, Data Warehousing & Business Intelligence	71
Topic 10, Metadata Management	64
Topic 11, Data Quality	70
Topic 12, Mix Questions	8
Total	750

QUESTION NO: 1

E-discovery is the process of finding electronic records that might serve as evidence in a legal action.

A. TRUE

B. FALSE

ANSWER: A

Explanation:

TRUE is correct. Electronic discovery, commonly called e-discovery, is the legal process through which electronically stored information is identified, preserved, collected, reviewed, analyzed, and produced for use in litigation, investigations, regulatory matters, or other legal proceedings. The statement accurately describes the core discovery purpose: finding electronic records that may be relevant and potentially usable as evidence in a legal action.

The records involved can include email, documents, spreadsheets, database content, chat messages, collaboration-platform files, mobile-device data, audio or video, and metadata. In data management practice, e-discovery depends on knowing what data the organization holds, where it resides, who is responsible for it, and how it can be retained and retrieved without compromising its authenticity or chain of custody. This makes sound information governance, records management, retention schedules, legal holds, metadata management, and data lineage especially important.

The Electronic Discovery Reference Model describes e-discovery as a process beginning with identifying potentially relevant information and progressing through preservation, collection, processing, review, analysis, production, and presentation. See the EDRM Model and the Federal Rules of Civil Procedure, Rule 34 for authoritative context on electronically stored information in discovery.

QUESTION NO: 2

Data Governance deliverables commonly include:

A. Data value chains

B. IT methodology and practices

C. Business culture assessment

D. Roadmaps and implementation strategy

E. Regulatory requirements

ANSWER: A D

Explanation:

Data value chains and roadmaps and implementation strategy are common Data Governance deliverables because they turn governance from a set of principles into an organized, business-aligned program. A data value chain describes how data supports business capabilities and creates value as it moves through its lifecycle. This gives governance leaders a practical way to connect data responsibilities, decisions, controls, and investments to business outcomes. Roadmaps and implementation strategy define the sequenced actions needed to establish and mature governance capabilities, such as assigning accountabilities, introducing policies and standards, implementing controls, and measuring progress. Together, these deliverables provide both a target operating perspective and a realistic plan for achieving it. DAMA's Data Management Body of Knowledge treats Data Governance as the function that directs and oversees data management through decision rights, accountability, policies, and coordinated implementation. Value-chain views and implementation roadmaps support that mandate by aligning governance work with organizational priorities and by making the path to governance objectives explicit. See DAMA International's overview of the DAMA-DMBOK framework and its description of Data Governance.

QUESTION NO: 3

Databases are categorized in three general ways:

A. Warped

B. Non-relational

C. Relational

D. Accessible

E. None of the above

F. Hierarchical

ANSWER: B C F

Explanation:

Relational, non-relational, and hierarchical are valid general database categories because they distinguish databases by their principal data model and the way records and relationships are organized. A relational database represents data in tables (relations) and uses defined keys and constraints to connect and govern those tables. This model remains central to enterprise data management because it supports structured data, integrity controls, and standardized querying through SQL.

Hierarchical databases organize records in a parent-child tree structure. This is a distinct, longstanding database model and remains relevant where data naturally follows one-to-many paths or where legacy platforms use hierarchical storage. Non-relational is a broad category covering database models that do not primarily use the relational-table model, including document, key-value, graph, and wide-column approaches. These models provide flexible structures and can support data with varying shapes or relationship patterns.

Data-management practice requires understanding these categories because each affects data modeling, metadata, integration, governance, and appropriate technology selection. DAMA's body of knowledge treats data architecture and data modeling as foundational disciplines for selecting and managing data structures and platforms. See DAMA International's Body of Knowledge and IBM's description of the hierarchical database model.

QUESTION NO: 4

Layers of data governance are often part of the solution. This means determining where accountability should reside for stewardship activities and who the owners of the data are.

A. FALSE

B. TRUE

ANSWER: B

Explanation:

TRUE is correct. A core purpose of data governance is to establish decision rights, accountability, and operating responsibilities for data across the organization. Governance layers provide a practical way to assign those responsibilities at appropriate organizational levels, such as enterprise, domain, business unit, or operational teams. This structure makes clear who is accountable for a data domain, who has authority to make or approve data-related decisions, and who performs stewardship activities.

Data owners are generally accountable for ensuring that data is managed as a business asset and is fit for its intended business use. Data stewards commonly carry out the operational governance work on the owner's behalf, including coordinating definitions, addressing data-quality issues, applying policies, and escalating decisions when needed. Locating ownership and stewardship at the right governance layer helps ensure that enterprise standards can coexist with domain expertise and day-to-day operational knowledge. This alignment of ownership, stewardship, and accountability is central to the DAMA view of data governance. See the DAMA Body of Knowledge and the Data Governance overview from DATAVERSITY for further context on governance roles and accountability.

QUESTION NO: 5

BI tool types include:

A. BPM

B. Operational reporting

C. Data lake extraction

D. Diagnostic, self-service analytics

E. Descriptive, self-service analytics

F. Reduction of risk

ANSWER: A B D E

Explanation:

Business performance management, operational reporting, diagnostic and self-service analytics, and descriptive and self-service analytics are all valid BI tool types or capabilities. Business performance management applies BI measures, scorecards, targets, and performance monitoring to help an organization manage progress toward strategic and operational objectives. Operational reporting delivers timely, detailed information that supports routine business processes and day-to-day decisions. Descriptive analytics presents and summarizes what has happened, commonly through reports, dashboards, visualizations, and key performance indicators. Diagnostic analytics extends that capability by helping users investigate why an outcome occurred, including through drill-down, filtering, comparison, and ad hoc analysis. Self-service analytics gives business users governed access to data and analytical tools so they can explore information and create their own reports or visualizations without depending on technical teams for every request. Together, these capabilities represent common BI functions across operational, performance-management, reporting, and analytical use cases. IBM describes BI as encompassing reporting, analysis, dashboards, and performance management, while Microsoft describes self-service BI as enabling users to create reports and derive insights independently. See IBM: What is business intelligence? and Microsoft Learn: Self-service BI.

QUESTION NO: 6

There are three recovery types that provide guidelines for how quickly recovery takes place and what it focuses on.

A. Immediate recovery

B. Intermittent recovery

C. Critical recovery

D. Translucent recovery

E. BMT recovery

F. Non-critical recovery

ANSWER: A C F

Explanation:

Immediate recovery, Critical recovery, and Non-critical recovery are the three recovery types used to establish recovery expectations according to urgency and business impact. Immediate recovery applies where an interruption cannot be tolerated for more than a very short period; recovery actions are therefore initiated at once to restore essential data-management services and protect operations. Critical recovery covers capabilities that must be restored promptly after the most immediate needs have been addressed, because continued unavailability would create substantial operational, financial, regulatory, or customer impact. Non-critical recovery applies to services and data resources whose restoration can be deferred until higher-priority capabilities are available, allowing recovery teams to sequence work and use resources effectively.

These categories provide a practical basis for contingency and disaster-recovery planning: they connect recovery timing with the importance of the affected service, data, and business process. Establishing such priorities supports documented recovery procedures, recovery objectives, and testing that reflect organizational risk. NIST contingency-planning guidance similarly emphasizes identifying system and business-process priorities and defining recovery strategies that meet those priorities. See NIST SP 800-34 Rev. 1, Contingency Planning Guide for Federal Information Systems and the DAMA Body of Knowledge resources.

QUESTION NO: 7

As an often-overlooked aspects of basic data movement architecture, Process controls include:

A. Consistency logging

B. Exception logs

C. Database activity logs

D. Alerts

E. Exception logs

F. All of the above

ANSWER: A B C D E F

Explanation:

Process controls are essential operational safeguards in a data movement architecture. They make transfers, transformations, and loads observable, traceable, and manageable, rather than treating a completed job status as sufficient evidence of a reliable result. Consistency logging records control information that helps confirm data movement occurred as expected and supports reconciliation of processing results. Exception logs capture errors, rejected records, and unexpected processing conditions so that they can be investigated, remediated, and, where appropriate, reprocessed. Database activity logs provide an audit trail of relevant activity in the systems participating in movement and processing. Alerts provide timely notification when a process fails, breaches a threshold, or requires intervention. Together, these controls support monitoring, issue management, operational continuity, and confidence in the integrity of moved data. The repeated occurrence of “Exception logs” does not change its status as a valid process control. Because each listed control is included, “All of the above” is also correct. DAMA’s data-management guidance treats operational metadata, monitoring, auditability, and control of data integration processes as core concerns; see the DAMA-DMBOK reference information and DAMA International’s Body of Knowledge resources.

QUESTION NO: 8

Most document programs have policies related to:

A. Scope and compliance audits

B. Proper destruction of records

C. Proper construction of records

D. Identification and protection of vital records

E. Partition tolerance

F. All of the above

ANSWER: A B D

Explanation:

Most document and records management programs establish policy for their operational scope, compliance monitoring, records disposition, and the identification and protection of records essential to continued operations. Scope policies define which business areas, record types, repositories, and lifecycle activities fall under the program's authority. Compliance audits provide evidence that the policy is being followed and identify gaps requiring remediation. Proper destruction of records is a core disposition control: records should be destroyed in an authorized, secure, and documented manner once approved retention requirements have been met and no legal hold or other preservation obligation applies. Identification and protection of vital records is also fundamental because these records support the resumption of critical business functions and protection of legal and financial rights following a disruption. Together, these policy areas give a document program accountable governance across the record lifecycle while supporting regulatory, legal, operational, and business-continuity needs. The U.S. National Archives describes records disposition as including authorized destruction and emphasizes managing records through their lifecycle; its vital-records guidance addresses records needed during emergency operations. See NARA Records Scheduling and Disposition and NARA Vital Records.

QUESTION NO: 9

Dimensions of data quality include:

A. Validity

B. Privacy

C. Innovation

D. Accessibility

E. Currency

F. All of the above

ANSWER: A D E

Explanation:

Validity, accessibility, and currency are recognized data-quality dimensions. Validity concerns whether a data value conforms to the defined business rules, formats, allowable ranges, domains, and other constraints for that data element. For example, a date of birth must be a valid date and must meet any agreed business constraints. Accessibility addresses whether authorized users can obtain and use the data when needed; data cannot adequately serve its business purpose if it is unavailable or unusable to the people and processes entitled to access it. Currency concerns whether data is sufficiently up to date for its intended use, often closely associated with timeliness. A current customer address, account status, or inventory balance is necessary for reliable operational and analytical decisions. DAMA's data-quality practice treats quality as fitness for purpose and evaluates data through defined dimensions, measures, rules, and monitoring. The precise dimension set can be tailored to organizational context, but validity, accessibility, and currency are well-established measures of fitness for use. See the DAMA Data Management Body of Knowledge and ISO/IEC 25012's overview of data quality characteristics.

QUESTION NO: 10

Temporal aspects usually include:

A. Valid time

B. Transmitting time

C. Transaction time

D. Value time

ANSWER: A C

Explanation:

Temporal data management commonly distinguishes **valid time** and **transaction time**. Valid time records the period during which a fact is true in the real-world domain being modeled. For example, an employee's departmental assignment may be valid from its effective start date through its end date, including dates that may be planned in advance or learned retrospectively. This supports accurate historical and effective-dated business reporting.

Transaction time records when the fact was stored, updated, or otherwise known by the information system. Maintaining it enables an organization to reconstruct what its database contained at a particular point in time, which is important for auditability, traceability, correction of previously recorded facts, and reproducible reporting. When both dimensions are retained, the resulting bitemporal view can distinguish a change in the business world from the date on which the system captured that change. This distinction is foundational to temporal database design and aligns with standard descriptions of system-versioned and application-time periods. See the ISO/IEC 9075-2 SQL standard overview and IBM's temporal tables documentation.

QUESTION NO: 11

Primary deliverables of the Data Warehouse and Business Intelligence context diagram include:

A. Data Products

B. Data Stewardship

C. Governance Activities

D. Release Plan

E. Load Tuning Activities

F. BI Activity Monitoring

ANSWER: A C D E F

Explanation:

Within the DAMA Data Warehouse and Business Intelligence knowledge area, **Data Products** are the central business-facing deliverables: curated, integrated, and consumable data assets and analytical outputs that support decisions. A **Release Plan** is also a key delivery artifact because warehouse and BI capabilities must be deployed in controlled, coordinated increments. **Governance Activities** provide the decision rights, standards, prioritization, and accountability needed to ensure that delivered data products remain aligned with enterprise requirements. **Load Tuning Activities** support the operational delivery of reliable and timely data by maintaining the performance of ingestion, transformation, and loading processes. **BI Activity Monitoring** supplies operational and usage information that enables teams to manage BI service performance, adoption, capacity, and ongoing improvement. Taken together, these items reflect that Data Warehouse and Business Intelligence is not limited to creating reports or storing data; it delivers governed data products through managed releases and sustained operational practices. DAMA describes the body of knowledge and its knowledge areas at DAMA International: Body of Knowledge. Additional DAMA-DMBOK context is available from Technics Publications: DAMA-DMBOK.

QUESTION NO: 12

What key components make up the Data Governance Charter?

A. Vision/Mission Statement, Data Governance data principles, Business drivers

B. Data Stewardship Metrics, Data Governance, Business Drivers

C. Vision/Mission statement, Data quality framework, Data stewardship metrics

D. Data processes, data principles and the timeframe for implementation

E. The Enterprise data architecture, data security practices and industry regulations

ANSWER: A

Explanation:

Vision/Mission Statement, Data Governance data principles, Business drivers is correct because a Data Governance Charter establishes the purpose, direction, and organizational rationale for the governance program. The vision or mission statement expresses the intended business outcome and long-term purpose of governing data. Data Governance principles define the foundational commitments that guide decisions and behaviors, such as treating data as an enterprise asset, assigning accountability, and managing data consistently across domains. Business drivers connect the charter to practical organizational needs, including regulatory obligations, risk reduction, improved decision-making, operational efficiency, customer outcomes, or digital transformation.

Together, these elements make the charter an authoritative statement of why Data Governance exists and the principles under which it will operate. They give sponsors, data owners, stewards, and other stakeholders a shared basis for prioritizing governance work and making decisions. The charter can then be expanded with operating details such as scope, roles, decision rights, funding, measures, and implementation planning. DAMA's Body of Knowledge identifies Data Governance as the function that sets authority, control, and decision-making for data management, while the Data Governance Institute emphasizes that governance must be grounded in business value and organizational direction. See DAMA International Body of Knowledge and Data Governance Institute's Data Governance Framework.

QUESTION NO: 13

Why is the GDPR called the most important change in data and data privacy regulation in 20 years?

A. Because most Europeans say they want the same data protection rights across the EU and regardless of where their data is processed

B. Because most Europeans don't want their data used by any country but the one in which they live

C. Because most Europeans don't care if EU companies have their data but they don't want it shared with non-EU companies

D. Because most Europeans are on social media because they don't want their data exposed

E. Because most Europeans believe other countries are stealing their data

ANSWER: A

Explanation:

Because most Europeans say they want the same data protection rights across the EU and regardless of where their data is processed is the best answer because it captures the central regulatory change brought by the General Data Protection Regulation: a directly applicable, harmonized data-protection framework for the European Union, paired with broad territorial reach. The GDPR replaced a directive-based approach that could be implemented differently by individual Member States with common rules and enforceable rights across the EU. Those rights include transparency about processing, access to personal data, rectification, erasure in relevant circumstances, restriction, portability, and objection. The regulation also reaches many organizations outside the EU when they offer goods or services to people in the EU or monitor their behavior, helping ensure that protection does not disappear merely because processing occurs elsewhere. This combination of consistent individual rights, common obligations for controllers and processors, stronger accountability, and cross-border applicability is why GDPR is widely regarded as a landmark change in privacy regulation. The European Commission describes the GDPR as setting rules for the processing of personal data and applying to organizations established in the EU as well as certain organizations outside it. See the European Commission's GDPR overview and the official GDPR text in EUR-Lex.

QUESTION NO: 14

The ethics of data handling are complex, but is centred on several core concepts. Please select the correct answers.

A. Impact on machines

B. Impact on people

C. Potential for data management

D. Potential for misuse

E. Economic value of ethics

F. Economic value of data

ANSWER: B D F

Explanation:

Data-handling ethics is centred on the effects that data practices have on people, the possibility that data can be misused, and the economic value associated with data. **Impact on people** is fundamental because collection, sharing, analysis, and automated decision-making can affect an individual's privacy, autonomy, opportunities, reputation, and ability to obtain fair treatment. Ethical data management therefore requires practitioners to consider human consequences throughout the data lifecycle, not merely technical feasibility.

Potential for misuse is also a core concern. Data that is collected for a legitimate purpose can be repurposed, disclosed, combined with other data, or used in ways that cause harm. Ethical handling includes anticipating these risks and applying safeguards such as purpose limitation, access controls, transparency, accountability, and appropriate governance.

Economic value of data matters because data is an organizational asset that can generate commercial and social value. Ethical decisions must recognize how that value is created, who benefits from it, and how incentives may influence collection, use, sharing, and stewardship decisions. DAMA's professional ethics framework emphasizes responsible conduct and the protection of people affected by data practices; see the DAMA International Code of Ethics. Broader privacy principles supporting responsible use are described by the OECD Privacy Guidelines.

QUESTION NO: 15

Industry is struggling to distinguish the accountabilities of CDO and CIO. The definition of their responsibilities may specify parts of:

A. Financial management functions

B. Metadata functions

C. Data security functions

D. Data architecture functions

E. Business intelligence functions

ANSWER: A B C D E

Explanation:

Financial management functions, metadata functions, data security functions, data architecture functions, and business intelligence functions can all be included when an organization defines the respective accountabilities of a Chief Data Officer and Chief Information Officer. The boundaries are not universal: they depend on the organization's operating model, data strategy, reporting lines, scope of technology ownership, and the maturity of its data-management program. A CDO commonly leads or coordinates enterprise data governance and strategic data capabilities, while a CIO is commonly accountable for information technology delivery, platforms, operations, and associated investment management. In practice, the two roles must explicitly allocate or share responsibility for data architecture, metadata, security controls, analytics and business-intelligence capabilities, and the funding, prioritization, and cost management required to sustain those capabilities. Financial management is therefore relevant because data and technology initiatives require budget ownership and investment decisions, even when the CDO and CIO have different levels of authority over them. DAMA's body of knowledge treats data management as an enterprise-wide discipline that requires defined decision rights, accountability, and stewardship across these interconnected functions. See DAMA International's Data Management Body of Knowledge overview and the CDMP certification information for its data-management framework and role context.

QUESTION NO: 16

Lack of automated monitoring represents serious risks, including:

A. Administrative and audit risks

B. Risk of non-compliance

C. Detection and recovery risks

D. Risk of reliance on inadequate native tools

ANSWER: A B C D

Explanation:

A lack of automated monitoring creates several interconnected operational, governance, and control risks. **Administrative and audit risks** arise because teams must manually collect evidence, review system activity, and demonstrate that required controls operated consistently. This increases effort and makes audit evidence less timely and less complete. **Risk of non-compliance** is material because control failures, policy violations, or retention exceptions may not be identified early enough to meet regulatory or internal requirements.

Detection and recovery risks are also significant: without continuous alerts and measurement, abnormal conditions, data-quality degradation, security events, and service failures can remain undiscovered, increasing their impact and extending restoration time. Finally, a **risk of reliance on inadequate native tools** exists where built-in platform monitoring does not provide sufficient cross-system visibility, alerting, retention, correlation, or reporting for enterprise governance needs. Effective monitoring should therefore be automated, measurable, and capable of producing reliable evidence for oversight and remediation. NIST describes continuous monitoring as maintaining ongoing awareness of information-security and risk status in SP 800-137; its guidance on centralized monitoring evidence is also covered in SP 800-92.

QUESTION NO: 17

Many people assume that most data quality issues are caused by data entry errors. A more sophisticated understanding recognizes that gaps in or execution of business and technical processes cause many more problems that mis-keying.

A. TRUE

B. FALSE

ANSWER: A

Explanation:

TRUE is correct. DAMA's data quality perspective treats data quality as an outcome of the full data lifecycle and of the business and technical processes that create, transform, store, exchange, and use data. Consequently, recurring defects commonly originate upstream: unclear business definitions, incomplete requirements, inadequate controls, inconsistent integration mappings, poorly designed process handoffs, delayed updates, or failures in system processing. These causes can introduce defects systematically and at scale, affecting many records repeatedly rather than only isolated values entered by an individual.

This understanding is important because effective data-quality improvement begins with identifying root causes and assigning accountability to the process, system, or rule that produced the issue. Correcting individual records may temporarily improve a dataset, but durable improvement requires preventive controls, well-defined data requirements, monitoring, and remediation of the responsible process. DAMA International frames data quality management around planning, control, assurance, and improvement activities across organizational processes. The broader principle is also reflected in ISO's data-quality guidance, which emphasizes managing data quality throughout data processing rather than treating it solely as an input-error problem. See DAMA International's Data Management Body of Knowledge resources and ISO 8000-8 data-quality information and data quality management.

QUESTION NO: 18

Examples of transformation in the ETL process onclude:

A. De-duping

B. Structure changes

C. Hierarchical changes

D. Re-ordering

E. Semantic conversions

F. None of the above

ANSWER: A B C D E

Explanation:

ETL transformation applies business rules and technical rules to make extracted data suitable for its target use. **De-duping** is a transformation because it identifies and resolves repeated representations of the same entity, improving the quality of the integrated result. **Structure changes** transform how data is represented, such as splitting a source attribute into multiple target attributes, combining attributes, or mapping records between normalized and denormalized structures. **Hierarchical changes** also qualify because ETL commonly needs to reshape parent-child relationships, levels, or paths so that source hierarchies can be represented correctly in the target model.

Re-ordering is a transformation when record or attribute ordering is required by a target interface, file format, load process, or downstream rule. **Semantic conversions** transform meaning or business interpretation, such as mapping codes to standard values, converting units of measure, harmonizing classifications, or applying reference-data rules. These operations illustrate the DAMA data-integration principle that data movement must include the transformations needed to achieve a consistent, usable representation rather than merely copying source values. DAMA identifies data integration and interoperability as a core data-management knowledge area; see DAMA International's Body of Knowledge overview. Practical ETL platforms likewise define transformations as operations that modify, cleanse, aggregate, merge, or otherwise reshape data before loading; see Microsoft's Integration Services transformation documentation.

QUESTION NO: 19

Data security includes the planning, development and execution of security policies and procedures to provide authentication, authorisation, access and auditing of data and information assets.

A. TRUE

B. FALSE

ANSWER: A

Explanation:

TRUE is correct. In the DAMA data-management framework, Data Security is concerned with protecting data and information assets by establishing, implementing, and operating security policies, standards, procedures, and controls. Those controls support the core security functions named in the statement: authentication establishes the identity of a user or system; authorisation determines the permitted actions or data access for that authenticated identity; access controls enforce those permissions; and auditing records activity to support accountability, monitoring, investigation, and compliance.

The statement also correctly frames data security as an ongoing management discipline rather than a purely technical product or one-time implementation. Effective security requires planned governance, documented procedures, operational execution, and evidence that controls are functioning. This aligns with the principle that protection of information assets must be integrated into their full lifecycle and managed according to organisational risk and obligations. The DAMA International body of knowledge identifies Data Security as a core data-management knowledge area: DAMA Body of Knowledge. The security-control concepts of identification, authentication, access enforcement, and audit/accountability are also reflected in the NIST Security and Privacy Controls.

QUESTION NO: 20

When data is classified as either security data or regulatory data, the result will be:

A. Business employees are restricted from viewing the data but technical employees can store the data in databases

B. Employees will never see classified data for any reason

C. Employees know they have to aggregate the data

D. Employees, both business & technical know the sensitivity of the data

E. Employees know they cannot use the data because it has been classified

ANSWER: D

Explanation:

Employees, both business & technical know the sensitivity of the data is correct because data classification communicates the nature, sensitivity, and handling significance of data to everyone who creates, uses, manages, stores, or protects it. A security classification identifies data whose unauthorized disclosure, alteration, loss, or unavailability could create security risk. A regulatory classification identifies data subject to externally imposed obligations, such as privacy, retention, confidentiality, or reporting requirements. In each case, the classification acts as understandable metadata that supports consistent decisions about appropriate access, use, protection, storage, sharing, retention, and disposal. The classification itself does not inherently mean that no employee may access or use the data; rather, it enables business and technical personnel to recognize that safeguards and handling rules appropriate to the identified sensitivity must be applied. This shared awareness is essential to effective data governance because business personnel make decisions about legitimate use and technical personnel implement controls in systems and platforms. NIST describes security categorization as a basis for selecting appropriate security controls and protecting information and information systems. See NIST FIPS 199 and NIST's Guide for Mapping Types of Information and Information Systems to Security Categories.

QUESTION NO: 21

A staff member has been detected inappropriately accessing client records from

usage logs. The security mechanism being used is an:

A. Access

B. Audit

C. Entitlement

D. Authorisation

E. Authentication

ANSWER: B

Explanation:

Audit is correct because usage logs provide an audit trail: a chronological record of activity involving information systems and data. In this case, the organization used recorded access events to identify that a staff member viewed client records inappropriately. This is a detective security mechanism, supporting accountability by making it possible to review who performed an action, when it occurred, and which records or resources were involved. Effective audit logging is an important data-management and data-protection practice because it supports monitoring, investigation, incident response, and evidence gathering. For client records, logs commonly capture identifiers for the user, the accessed record or system, timestamps, the action performed, and relevant source or session details. The U.S. National Institute of Standards and Technology describes log management as the processes for generating, transmitting, storing, analyzing, and disposing of log data, emphasizing its role in identifying inappropriate or suspicious activity. Its glossary also defines an audit trail as a chronological record that enables tracing of activities related to a system or transaction. See NIST SP 800-92, Guide to Computer Security Log Management and the NIST definition of audit trail.

QUESTION NO: 22

There are several methods for masking data:

A. Substitution

B. Temporal variance

C. Temporal stagnation

D. Value stagnation

E. Value variance

F. All of the above

ANSWER: A B E

Explanation:

Substitution, **Temporal variance**, and **Value variance** are recognized forms of data masking because each alters sensitive data while retaining a useful form for testing, development, analysis, or other authorized secondary use. Substitution replaces an original value with a realistic alternative, such as replacing an actual name or account identifier with a consistently generated surrogate. This supports privacy protection while preserving expected format, data type, and—in well-designed implementations—referential consistency across related records.

Temporal variance masks date- and time-related attributes by shifting or otherwise varying dates and timestamps. Applying a consistent temporal offset can preserve intervals, ordering, seasonality, and process-duration patterns without disclosing the original event dates. Value variance similarly changes numeric or other sensitive values within defined rules or ranges so that useful distributions, relationships, and analytic behavior can be retained without exposing the precise source values. These approaches align with data-management practice: masking should be selected according to the sensitivity of the data and the business properties that downstream users must retain. NIST discusses de-identification techniques and the need to manage re-identification risk in NIST SP 800-188. The UK ICO also describes pseudonymisation and related privacy-enhancing approaches in its pseudonymisation guidance.

QUESTION NO: 23

Effectiveness metrics for a data governance programme includes: achievement of goals and objectives; extend stewards are using the relevant tools; effectiveness of communication; and effectiveness of education.

A. FALSE

B. TRUE

ANSWER: B

Explanation:

TRUE is correct because these are meaningful effectiveness measures for a data governance programme. Governance exists to achieve defined business and data-management outcomes, so measuring achievement of stated goals and objectives demonstrates whether the programme is delivering its intended value. Data stewards operationalize governance policies, standards, issue management, and decision rights; therefore, adoption and appropriate use of the relevant governance tools is an important indicator that governance processes are embedded in day-to-day work. Communication and education are also core programme-enablement activities. Their effectiveness can be assessed through measures such as stakeholder awareness, training completion and comprehension, participation, feedback, and the timely reach of governance communications. Together, these measures assess outcomes, operational adoption, and organizational capability rather than merely counting governance activities. DAMA's Data Management Body of Knowledge identifies Data Governance as a discipline concerned with exercising authority and control over data, which requires defined roles, processes, communication, and performance measurement. See DAMA-DMBOK reference information from Technics Publications and DAMA International's Body of Knowledge resources.

QUESTION NO: 24

The impact of the changes from new volatile data must be isolated from the bulk of the historical, non-volatile DW data. There are three main approaches, including:

A. All of the above

B. Streaming

C. Messaging

D. Technology

E. Data

F. Trickle Feeds

ANSWER: B C F

Explanation:

Streaming, Messaging, and Trickle Feeds are the three approaches used to handle newly arriving, volatile data while protecting the stable historical core of a data warehouse. These approaches enable more timely movement and processing of changes without forcing frequent, disruptive reloads of the warehouse's large non-volatile data stores.

Streaming processes a continuing flow of events or records, allowing data to be captured and acted on with low latency. Messaging provides a decoupled, reliable means for applications and data producers to publish changes for downstream consumers, supporting asynchronous integration. Trickle Feeds apply small, frequent incremental loads rather than large batch updates, reducing the operational impact of data refreshes and keeping warehouse information relatively current. Together, these patterns support controlled integration of operational changes with analytical data management practices, including data quality checks, transformation, reconciliation, and governed loading.

This distinction between volatile incoming data and stable historical data is consistent with the data-warehousing focus on integrating and preserving information for analysis while managing refresh processes separately. See DAMA International's Data Management Body of Knowledge and Oracle's overview of data warehousing concepts.

QUESTION NO: 25

Which of these is NOT likely in the scope of Data Governance and Stewardship?

A. Data asset valuation in order to allocate priority to data quality management

B. Ensure the privacy needs of stakeholders are enforced and audited

C. To train staff on data governance principles, embedding them in everyday decision making

D. To adjust the definitions of items in the chart of accounts to improve financial management

E. Monitor compliance to record management policies

ANSWER: D

Explanation:

To adjust the definitions of items in the chart of accounts to improve financial management is the activity least likely to be within the scope of Data Governance and Stewardship. A chart of accounts is fundamentally an accounting and financial-management structure used to classify transactions and support financial reporting. Decisions to alter its accounts are made to meet finance, accounting, reporting, control, and operational-management requirements. Those business decisions belong primarily to the accountable finance function.

Data Governance and Stewardship can establish the controls around financial data: for example, identifying accountable data owners and stewards, documenting definitions and metadata, setting quality rules, controlling changes, and ensuring that approved chart-of-account values are consistently represented and used across data systems. However, governing the

data does not mean assuming responsibility for the underlying financial-policy decision to redesign the chart of accounts in order to improve financial management. Governance provides decision rights, oversight, standards, and accountability for data, while the relevant business domain retains accountability for its business structures and policies. This distinction aligns with DAMA's treatment of Data Governance as the exercise of authority and control over data management, described in the DAMA-DMBOK2 reference and by the Data Management Association International.

QUESTION NO: 26

The best preventative action to prevent poor quality data from entering an organisation include:

A. Institute a formal change control

B. Define and enforce rules

C. Implement data governance and stewardship

D. None of the above

E. Train data procedures

F. Establish data entry controls

ANSWER: A B C E F

Explanation:

Preventing poor-quality data at the point of creation or acquisition is a core Data Quality practice. **Institute a formal change control** helps ensure that changes to data definitions, structures, interfaces, reference values, and business processes are assessed, approved, tested, and communicated before they create defects in production data. **Define and enforce rules** establishes the business and technical requirements—such as permitted values, required fields, format requirements, and cross-field validations—that data must meet before it is accepted.

Implement data governance and stewardship assigns accountability for data definitions, quality expectations, issue resolution, and ongoing monitoring. This provides the decision rights and oversight needed to sustain preventative controls rather than treating quality as a one-time cleansing exercise. **Train data procedures** supports consistent execution by ensuring people who create, maintain, or handle data understand required processes, standards, and their responsibilities. **Establish data entry controls** operationalizes quality rules directly in capture processes through validation, defaults, controlled lists, mandatory-field checks, and other input controls. Together, these measures prevent defects upstream, where correction is generally less costly and more reliable. DAMA's body of knowledge identifies Data Quality and Data Governance as interrelated disciplines: DAMA International Body of Knowledge. Practical input-validation controls are also described in NIST's Privacy Framework resources.

QUESTION NO: 27

Data handling ethics are concerned with how to procure, store, manage, use and dispose of data in ways that are aligned with ethical principles.

A. TRUE

B. FALSE

ANSWER: A

Explanation:

TRUE is correct. Data handling ethics concerns the responsible treatment of data throughout its full lifecycle: acquisition or collection, storage, management, access, use, sharing, retention, and disposal. Ethical data practice requires more than satisfying technical requirements; it requires organizations and data professionals to make choices consistent with principles such as fairness, transparency, accountability, privacy, respect for individuals, and avoidance of harm. For example, ethical procurement considers whether data was obtained with appropriate authority and notice, while ethical use considers whether

a use is consistent with the purposes communicated to data subjects. Secure retention and defensible disposal also help protect people from unnecessary exposure or misuse of their information. These responsibilities align with DAMA's view of data management as a business discipline that establishes policies, practices, and controls for managing data as a valuable organizational asset. The DAMA International Code of Ethics specifically emphasizes professional responsibility, integrity, and protecting privacy and confidentiality in data work. See the DAMA International Code of Ethics and the DAMA Data Management Body of Knowledge overview.

QUESTION NO: 28

Where does the ethical responsibility lie with respect to managing data to reduce risks of misrepresentation, misuse, or misunderstanding?

A. Business owns the data and is therefore ethically responsible for managing data across the data lifecycle

B. Everybody that makes use of data within the organization is responsible for the ethical use of the data

C. Data modellers carry responsibility to ensure that data handling ethics are achieved by design

D. The ethical responsibility lies with Data Management professionals to manage data and to manage the associated risks

E. Risk Management is responsible for ethical data management

ANSWER: B

Explanation:

Everybody that makes use of data within the organization is responsible for the ethical use of the data is correct because ethical data management is an organization-wide responsibility, rather than an activity delegated solely to a specialist function. Every person who creates, collects, accesses, analyzes, shares, interprets, or acts on data can affect whether it is represented accurately, used for an appropriate purpose, protected adequately, and understood in its proper business and technical context. Ethical conduct therefore requires each data user to apply appropriate care, respect confidentiality and applicable obligations, avoid misleading interpretation or presentation, and raise concerns when data quality, provenance, consent, or use may create harm.

This shared-accountability principle aligns with the DAMA view of data management as a business discipline supported by defined roles, governance, policies, and controls, while recognizing that responsible behavior must be practiced throughout the data lifecycle. Data professionals and governance structures enable and guide ethical use, but ethical responsibility remains with all organizational users of data. DAMA International's professional ethics resources emphasize the individual responsibilities of data-management practitioners and the importance of responsible professional conduct; see the DAMA International Code of Ethics. The broader DMBOK framework and its data-management knowledge areas are described by the publisher at The DAMA-DMBOK Guide.

QUESTION NO: 29

The most common drivers for initiating a Mater Data Management Program are:

A. Metadata insecurity

B. Managing data quality

C. Reducing risk

D. Managing the costs of data integration

E. Meeting organizational data requirements

F. Reducing latency

ANSWER: B C D E

Explanation:

Managing data quality, reducing risk, managing the costs of data integration, and meeting organizational data requirements are common business drivers for establishing a Master Data Management program. MDM provides governed, consistent, and reusable master data for critical entities such as customers, products, suppliers, locations, and employees. That foundation helps an organization address inconsistent definitions, duplicate records, incomplete values, and unreliable relationships across systems, directly supporting improved data quality.

MDM also reduces business, operational, regulatory, and decision-making risk by establishing accountable stewardship, common standards, controls, and authoritative records for shared data. Because master data is frequently replicated and transformed across applications, a managed source of trusted data can reduce the effort, complexity, and ongoing expense associated with point-to-point integration and repeated reconciliation. Finally, an MDM program is initiated to satisfy enterprise requirements for reliable reporting, operational processes, analytics, compliance, and cross-functional data sharing. These drivers align with DAMA's emphasis on data quality, governance, integration, and the business value of managing data as an organizational asset. See the DAMA Body of Knowledge resources and IBM's overview of Master Data Management.

QUESTION NO: 30

If the target system has more transformation capability than either the source or the intermediary application system, the order of processes may be switched to ELT â€“ Extract Load Tranform.

A. TRUE

B. FALSE

ANSWER: A

Explanation:

TRUE is correct. ELT is an architectural variation of ETL in which data is first extracted from its source and loaded into the target data platform, with transformations subsequently performed within that target. This sequence is appropriate when the target environment—such as a cloud data warehouse, lakehouse, or database platform—provides substantial scalable compute, SQL processing, storage, and transformation capabilities. Using the target's processing engine can reduce dependence on a separate transformation server or intermediary application, avoid unnecessary data movement between platforms, and allow transformations to operate directly on data after it has been loaded. The choice is therefore driven by the capabilities and intended role of the destination platform, as well as practical factors such as data volume, performance, governance, and transformation complexity. IBM describes ELT as loading raw data into the destination before transformation and notes that modern cloud data warehouses commonly support this approach. AWS likewise distinguishes ELT by placing transformation in the target data store. See IBM: What is ETL? and AWS: ETL vs. ELT.

QUESTION NO: 31

DAMA International's Certified Data Management Professional (CDMP) certification required that data management professionals subscribe to a formal code of ethics, including an obligation to handle data ethically for the sake of society beyond the organization that employs them.

A. TRUE

B. FALSE

ANSWER: A

Explanation:

TRUE is correct. DAMA International frames data management as a professional discipline with responsibilities that extend beyond an employer's immediate commercial or operational interests. Its ethical principles recognize that data professionals can affect individuals, communities, institutions, and society through decisions about data collection, quality, access, use, retention, protection, and disclosure. Accordingly, a formal professional commitment includes acting with integrity, respecting privacy and confidentiality, avoiding misuse, and considering the broader consequences of data-management work.

For CDMP certification, adherence to professional ethics is part of the expected conduct of a certified data management professional. This reflects the fact that data can create substantial public benefit but can also cause harm when it is handled carelessly, unfairly, deceptively, or without appropriate safeguards. The obligation is therefore not limited to following an employing organization's instructions; professional judgment must account for ethical duties to data subjects and the wider public. DAMA International's ethics materials describe this profession-wide responsibility, while CDMP is DAMA's certification program for demonstrating data-management knowledge and professional standing. See DAMA International's Code of Ethics and the CDMP certification site.

QUESTION NO: 32

There are several reasons to denormalize data. The first is to improve performance by:

A. Creating smaller copies of fata to reduce costly run-time calculations and/or table scans of large tables.

B. None of the above

C. Pre-calculating and sorting costly data calculations to avoid runt-time system resource competition.

D. Making tables more readable when no foreign key exists

E. Combining data from multiple other tables in advance to avoid costly run-time joins

F. All of the above

ANSWER: A C E

Explanation:

Denormalization is a deliberate physical-design technique used when the performance cost of repeatedly reconstructing normalized data is greater than the cost of storing selected redundant or derived data. Creating smaller copies of fata to reduce costly run-time calculations and/or table scans of large tables is a valid approach because purpose-built summary, reporting, or aggregate structures can reduce the volume of data read for common workloads. Pre-calculating and sorting costly data calculations to avoid runt-time system resource competition is also appropriate: materialized aggregates, derived values, and precomputed reporting results shift expensive work away from interactive query execution and can make response times more predictable. Combining data from multiple other tables in advance to avoid costly run-time joins is a central denormalization pattern, particularly in analytical systems where users frequently need the same integrated view of multiple entities. These practices should be driven by demonstrated access patterns and performance requirements, with refresh, lineage, consistency, and data-quality controls defined for every derived or duplicated structure. Oracle describes materialized views as query results stored for faster access and explains that they can improve query performance through query rewrite. DAMA-oriented data-management practice likewise treats denormalization as a controlled design trade-off between redundancy and performance. See Oracle Database Data Warehousing Guide: Materialized Views and DAMA International Body of Knowledge.

QUESTION NO: 33

Lack of automated monitoring represents serious risks, including:

A. Administrative and audit duties risk

B. Risk of compliance

C. Direction and recovery risk

D. Risk of reliance on inadequate native

ANSWER: A B C D

Explanation:

Automated monitoring is a foundational control for operating and governing data systems because it continuously observes data processes, control conditions, exceptions, and service performance. "Administrative and audit duties risk" is correct

because automated evidence collection, alerting, and reporting reduce the operational burden of demonstrating that controls were performed and that relevant events can be traced. “Risk of compliance” is correct because organizations need timely visibility into control failures, access anomalies, retention issues, and other conditions that can affect regulatory or policy obligations. “Direction and recovery risk” is correctly associated with the loss of prompt detection and response capability: monitoring provides signals that support incident triage, corrective action, and recovery. “Risk of reliance on inadequate native” is also a valid concern where built-in platform monitoring is insufficient for enterprise-wide oversight, correlation, retention of evidence, or required control reporting. DAMA’s Data Management Body of Knowledge treats governance, data quality, metadata, security, and operational controls as interconnected disciplines; monitoring supplies the information needed to manage those controls effectively. NIST similarly identifies continuous monitoring as a means to maintain ongoing awareness of security and risk conditions. See DAMA International’s Body of Knowledge and NIST Continuous Monitoring.

QUESTION NO: 34

Data flows map and document relationships between data and:

A. Locations where local differences occur

B. Situations where local differences occur

C. Network segments

D. Applications within a business process

E. None of the above

F. All of the above

ANSWER: A C D

Explanation:

Data-flow documentation describes how data moves through an organization and connects data to the operational context in which it is created, transformed, stored, and consumed. **Locations where local differences occur** is correct because movement across geographic, organizational, or operational locations can introduce local implementations, controls, formats, timing, ownership, or regulatory requirements that must be visible in the flow. **Network segments** is correct because technical routing and boundary crossings are relevant to how data is transferred, secured, and made available between environments. Mapping these segments supports an understanding of interfaces, transfer mechanisms, and control points. **Applications within a business process** is also correct because data flows identify the applications that exchange or process data as a business process proceeds. This provides traceability from business activity to the systems and integration points that support it. Together, these relationships make data-flow maps useful artifacts for integration design, impact analysis, operational support, governance, and control design. DAMA’s body of knowledge treats data integration and interoperability as a core discipline concerned with moving and consolidating data across organizational systems and boundaries. See DAMA International’s Body of Knowledge overview and IBM documentation on data flows.

QUESTION NO: 35

Effective data management involves a set of complex, interrelated processes that enable an organisation to use its data to achieve strategic goals.

A. TRUE

B. FALSE

ANSWER: A

Explanation:

TRUE is correct because data management is not a single activity or technology; it is a coordinated set of interdependent business, governance, architectural, operational, and technical practices. DAMA’s data-management body of knowledge describes multiple knowledge areas, including data governance, data architecture, data quality, metadata, data integration,

master and reference data, data warehousing and business intelligence, and data security. These disciplines must work together because decisions in one area affect the effectiveness of the others. For example, governance establishes accountability and decision rights, metadata provides shared context and meaning, and data-quality practices help ensure that data is fit for its intended use.

When these processes are aligned with organisational objectives, data can support better decision-making, operational efficiency, risk management, regulatory compliance, innovation, and measurable business outcomes. Strategic data management therefore requires ongoing coordination among people, processes, policies, and technology rather than isolated data-handling tasks. This integrated view is consistent with DAMA International's description of data management as planning, controlling, and delivering data and information assets, as outlined in the DAMA Body of Knowledge. Further context on DAMA's professional data-management framework is available from DAMA International.

QUESTION NO: 36

The term data quality refers to only the characteristics associated with high quality data.

A. TRUE

B. FALSE

ANSWER: B

Explanation:

FALSE is correct because data quality is not limited to describing desirable characteristics of high-quality data. In DAMA-aligned data management, data quality concerns the degree to which data is fit for its intended purpose and meets defined requirements. That degree may be high, acceptable, poor, or unknown; therefore, the concept necessarily supports assessment of both conforming and nonconforming data. Quality dimensions such as accuracy, completeness, consistency, timeliness, validity, and uniqueness provide measurable ways to evaluate data against business rules, specifications, and user needs. A quality assessment can identify strengths as well as defects, quantify the scale of issues, and guide remediation and ongoing control.

Using the term only for high-quality characteristics would exclude the core management activity of measuring and improving data that does not meet requirements. DAMA's body of knowledge treats data quality as a discipline involving planning, monitoring, measurement, remediation, and prevention so that data can support organizational objectives. This is consistent with ISO's data-quality standards, which define quality in terms of characteristics and requirements rather than an assumption that the data is already high quality. See the DAMA Body of Knowledge and the ISO 8000-8 data quality standard.

QUESTION NO: 37

A project scope requires the collection, exchange, and reporting of data from multiple in-house custom systems. Documents gathered include business concepts, existing database schemas, XSDs, and reporting layouts. How many models of each layer of abstraction can be expected?

A. More XSDs than reporting layouts

B. The same number of each of the model types

C. More physical data models than logical data models, and more logical data models than conceptual data models

D. Only 1 conceptual data model, 1 logical data model, and 1 physical data model

E. More conceptual data models than physical data models

ANSWER: C

Explanation:

More physical data models than logical data models, and more logical data models than conceptual data models is correct because the layers of data-model abstraction serve progressively narrower scopes. A conceptual data model represents the broad business view: major subject areas, business concepts, and their essential relationships. For an initiative spanning several in-house systems, a relatively small number of conceptual models can establish a common business vocabulary and enterprise-level perspective. Logical data models add detailed attributes, identifiers, normalization, and business rules, so multiple logical models may be needed for separate domains, integrations, or application boundaries. Physical data models are most numerous because they implement data structures in specific technologies and systems. Existing database schemas, XSDs used for exchanges, and reporting-oriented structures can each embody system- or implementation-specific physical representations. Thus, as the model becomes closer to implementation, the expected number generally increases: conceptual models are fewest, logical models are more numerous, and physical models are most numerous. This hierarchy supports traceability from shared business meaning through logical design to concrete schemas and interfaces. DAMA recognizes conceptual, logical, and physical modeling as distinct abstraction levels within data modeling and design; see the DAMA Data Management Body of Knowledge and the DAMA-DMBOK2 publisher information.

QUESTION NO: 38

Select three correct attributes a data governance programme must be:

A. Embedded

B. Flexible

C. Measures

D. Rigid

E. Independent responsibility

F. Sustainable

ANSWER: A C F

Explanation:

A data governance programme must be **Embedded**, **Measures**, and **Sustainable**. Governance is embedded when its decision rights, accountabilities, policies, and data-management practices are incorporated into ordinary business and delivery processes rather than operating as a disconnected project. Embedding governance makes accountable behaviour part of how data is created, used, shared, and controlled across the organisation.

It must also use measures. Meaningful metrics allow governance leaders and data owners to monitor whether governance activities are operating effectively and whether they are improving outcomes such as data quality, policy compliance, issue resolution, and business value. Measures support transparent oversight and enable informed prioritisation and continuous improvement.

Finally, governance must be sustainable. Data governance is an ongoing organisational capability, not a one-time remediation effort. Sustainable governance has enduring sponsorship, defined roles, repeatable processes, appropriate resources, and mechanisms to adapt as business priorities, data, technology, and regulation evolve. These attributes align with DAMA's view of data governance as the exercise of authority and control over data assets throughout their lifecycle. See DAMA International's Data Management Body of Knowledge resources and DAMA International's Data Governance overview.

QUESTION NO: 39

Which of the following activities is most likely to maintain bias in data analysis?

A. Re-baselining the data set after each period of analysis to remove assumptions

B. Working with external stakeholders to assess data quality

C. Using more data sets containing the same data

D. Remove sources of likely bias from data sets before analysis

E. Using more data sets with diverse data sources

ANSWER: C

Explanation:

Using more data sets containing the same data is most likely to maintain bias because adding duplicate or substantively identical data does not introduce new evidence, perspectives, populations, collection methods, or measurement conditions. If the original data reflects an unrepresentative sample, historical inequity, inconsistent measurement, or a systematic collection bias, replicating that same information preserves the underlying pattern rather than testing or correcting it. It can also make the biased pattern appear more convincing by increasing its apparent volume, even though the additional records do not increase independence or representativeness. Sound data-management and analytical practice requires assessing data quality in the context of intended use, including the data's provenance, completeness, validity, and representativeness. For bias-sensitive analysis, data practitioners should understand how data was collected and whether it adequately represents the relevant real-world population. The DAMA International body of knowledge identifies data quality as a core data-management discipline and emphasizes fitness for purpose; this requires evaluating whether available data supports reliable decisions rather than merely accumulating more of the same data. NIST likewise describes bias as a source of harmful outcomes that must be identified and managed across the AI and data lifecycle. See DAMA International's Body of Knowledge and NIST AI Risk Management Framework.

QUESTION NO: 40

Data can be assessed based on whether it is required by:

A. Regulatory reporting

B. Capturing policy

C. Ongoing operations

D. Provide the starting point for customizations, integration or even replacement of an application

E. Business policy

F. Make the integration between data management and data analytics possible

ANSWER: A C E

Explanation:

Data requirements should be assessed in relation to the business, legal, and operational purposes that make the data necessary. **Regulatory reporting** is a valid basis because laws, regulations, and supervisory obligations can require an organization to collect, retain, govern, and report particular data elements. Such requirements commonly establish expectations for accuracy, completeness, lineage, retention, and demonstrable control.

Ongoing operations is also a valid basis. Data is required when it enables the organization to execute and manage its day-to-day processes, including delivering products or services, serving customers, administering transactions, monitoring performance, and making operational decisions. Identifying these needs is a core part of defining data requirements and ensuring that data supports business processes.

Business policy provides another valid basis for assessment because internal policies translate organizational strategy, risk appetite, governance decisions, and management rules into requirements for information. A policy may establish what information must be recorded, how long it must be retained, who may use it, and which quality or control standards apply. DAMA's body of knowledge emphasizes aligning data-management practices with business needs, governance, compliance, and operational use. See DAMA International's Body of Knowledge overview and DAMA International's Data Governance resources.

QUESTION NO: 41

The advantage of a decentralised Data Governance model over a centralised model is:

A. An increased level of ownership from local decision making groups

B. The cheaper execution of Data Governance operations

C. Having a common approach to resolving Data Governance issues

D. The common metadata repository configurations

E. The easier implementation of industry data models

ANSWER: A

Explanation:

An increased level of ownership from local decision making groups is the key advantage of a decentralised Data Governance model. In this model, governance authority and accountability are distributed to business domains, divisions, regions, or other local groups that are closest to the data's operational use and subject-matter context. This proximity enables people with direct knowledge of data definitions, quality concerns, regulatory needs, and business priorities to participate actively in decisions and to take responsibility for data within their area. Local ownership can also improve engagement with governance processes because responsibilities are embedded in the work of the teams that create, maintain, and consume the data. DAMA's Data Management Body of Knowledge treats Data Governance as the exercise of authority, control, and shared decision-making over data; a decentralised approach assigns more of that authority to appropriate local stakeholders while retaining the need for enterprise coordination and standards. This model is particularly useful in organisations with diverse business units, products, or geographic operations, where a single central body may lack sufficient domain context for all decisions. See DAMA International's overview of the Data Management Body of Knowledge and its Data Governance resources.

QUESTION NO: 42

Malware types include:

A. Trojan horse

B. Worm

C. Weasel

D. Virus

E. Adware

F. Camware

ANSWER: A B D E

Explanation:

Malware is software intentionally designed to disrupt systems, damage or alter data, obtain unauthorized access, or otherwise compromise the confidentiality, integrity, or availability of information assets. **Trojan horse**, **worm**, **virus**, and **adware** are established malware categories relevant to data-management security controls.

A Trojan horse disguises malicious functionality as legitimate or desirable software, exploiting a user's decision to install or run it. A worm is self-propagating malware that can spread across systems or networks without attaching itself to another file. A virus is malicious code that attaches to a host file or program and replicates when that host executes. Adware delivers or displays unwanted advertising and, particularly when installed without meaningful consent or when it tracks users and changes system settings, is treated as malicious or potentially unwanted software in security guidance.

Recognizing these categories supports data protection practices such as endpoint controls, malware scanning, secure configuration, patching, user awareness, incident response, and monitoring for unauthorized data access or exfiltration. The U.S. Cybersecurity and Infrastructure Security Agency describes malware and common forms in its security guidance, while the National Institute of Standards and Technology provides security-control guidance for malicious-code protection in NIST SP 800-53.

QUESTION NO: 43

Which of the following are must-do for any successful Data Governance programme?

A. Create a communications plan to inform to all stakeholders what you are doing.

B. Ensure there is a Data Governance Policy with which everyone in the organization is required to comply.

C. Create a training programme for all for data owners and data stewards.

D. Set up a wiki for incorrect data definitions.

E. Allocate Data Ownership responsibilities according to their role in the organization.

ANSWER: B

Explanation:

Ensure there is a Data Governance Policy with which everyone in the organization is required to comply. is the essential foundational action. A Data Governance Policy establishes the organization-wide mandate for governing data: it states the purpose, scope, principles, accountabilities, decision rights, and expected behaviors that make governance enforceable rather than merely aspirational. Requiring compliance makes the policy applicable across business functions, technology teams, and data domains, so that data-related decisions and controls are performed consistently. It also provides the authority needed to define supporting standards, assign stewardship activities, resolve data issues, measure conformance, and escalate noncompliance through appropriate management channels. In DAMA's Data Governance guidance, policy is a core governance mechanism because it translates organizational objectives and regulatory or risk obligations into direction that people must follow. A documented, approved policy therefore creates the common authority on which the programme's operating model and controls can be built. See the DAMA International Body of Knowledge overview and the DAMA-DMBOK resource site for Data Governance context and principles.

QUESTION NO: 44

What result(s) is/are Data Handling Ethics trying to avoid?

A. Loss of reputation for the organization and loss of customers

B. Unethical use of information by staff to achieve business outcomes; customers trust so they are willing to pay more

C. Increased Risk for people whose data is exposed and criminal proceedings

D. Ensure that Data Governance is in line with Corporate Governance and ethic business statements

E. Ensure that organizations are adhering to ethical standards set by industry and bodies such as the World Economic Forum

ANSWER: A

Explanation:

Loss of reputation for the organization and loss of customers is correct because data handling ethics is intended to ensure that data is collected, accessed, used, shared, retained, and disposed of in ways that deserve stakeholder trust. Ethical handling extends beyond technical compliance: it requires an organization to consider whether its data practices are fair, transparent, proportionate, and respectful of the people represented by the data. When an organization uses data in a manner that stakeholders regard as unethical, trust can be damaged even where the organization believes it has met a minimum legal or contractual requirement. Loss of trust has a direct organizational consequence: customers, partners, employees, and the public may disengage, resulting in reputational harm and loss of customers. DAMA's professional ethics guidance emphasizes responsible conduct, integrity, and protecting the interests of stakeholders; these principles support trustworthy data-management practices and help preserve organizational confidence. The DAMA-DMBOK framework also positions data ethics as an important consideration across data-management activities, particularly where decisions and uses of data can affect people. See the DAMA International Code of Ethics and the DAMA-DMBOK reference information.

QUESTION NO: 45

The most important reason to implement operational data quality measurements is to inform data consumers about levels of data effectiveness.

A. FALSE

B. TRUE

ANSWER: B

Explanation:

TRUE is correct. Operational data quality measurements provide ongoing, objective evidence of whether data is effective for its intended business use. Data consumers need this visibility because their decisions, processes, reporting, analytics, and customer interactions depend on knowing whether the data they receive is sufficiently accurate, complete, timely, consistent, and otherwise fit for purpose. Measurements translate data-quality expectations into observable results, such as the percentage of required values populated, the frequency of invalid records, or whether data is delivered within an agreed time window.

In DAMA-aligned practice, data quality is not an abstract technical characteristic; it is evaluated in relation to the needs of data consumers and the business processes they support. Publishing and monitoring operational measures enables consumers and data owners to understand the current level of confidence they can place in a data set, identify material risks, and make informed decisions about use, remediation, and prioritization. This consumer-facing insight is therefore a primary purpose of operational measurement, alongside supporting governance and continuous improvement. The DAMA-DMBOK framework treats data quality as a core data-management discipline; see the DAMA-DMBOK reference information and DAMA International's professional data-management resources.

QUESTION NO: 46

If data is a governed resource, like other resources (e.g., human resources, finance, property), how is Data Governance different from other types of Governance?

A. Oversight of a particular resource

B. Agreed models for risk management over the particular resource

C. Oversight of a resource that represents other resources, therefore supporting other resource governance

D. Ensuring compliance with regulation for the particular resource

E. Agreed models for decision making and decision rights, defined authority, and escalation paths for the resource

ANSWER: C

Explanation:

Oversight of a resource that represents other resources, therefore supporting other resource governance is correct because data has a distinctive role among organizational assets: it records, describes, measures, and provides evidence about people, finances, property, operations, customers, products, and other resources. Consequently, well-governed data is necessary for an organization to govern those represented resources reliably. For example, financial governance depends on accurate, controlled financial data; human-resources governance depends on trustworthy employee and workforce data; and property governance depends on complete asset and ownership records. Data Governance establishes the authority, accountability, policies, standards, and oversight needed to ensure data is fit for these purposes across its lifecycle. DAMA's Data Management Body of Knowledge identifies this representational characteristic as the key distinction: data is both an organizational resource in its own right and an enabler of governance for other resources. This makes Data Governance foundational and cross-cutting rather than limited to a single business asset domain. See DAMA International's overview of the Data Management Body of Knowledge and the DAMA Dictionary definition of Data Governance.

QUESTION NO: 47

Data governance requires control mechanisms and procedures for, but not limited to, escalating issues to higher level of authority.

A. FALSE

B. TRUE

ANSWER: B

Explanation:

TRUE is correct. Data governance establishes decision rights, accountabilities, oversight structures, and repeatable processes for managing data-related decisions and problems. An escalation procedure is a core governance control because it ensures that an issue which cannot be resolved at its operational level is brought to the appropriate data owner, steward, governance council, or executive authority. This makes decision-making transparent, timely, and aligned with organizational policy, risk tolerance, regulatory obligations, and business priorities.

Effective escalation mechanisms define such matters as issue-severity criteria, responsible roles, required evidence, resolution timeframes, decision authority, and documentation of outcomes. They also provide a path for resolving conflicts across business areas, such as disputes about data definitions, quality requirements, access, ownership, or acceptable use. In this way, escalation is not merely an administrative activity; it is an essential control that enables governance bodies to exercise their assigned authority and maintain accountability for data assets. DAMA identifies governance as the exercise of authority and control over data management, a concept reflected in the DAMA Data Management Body of Knowledge overview. The importance of defined accountability and decision processes is also consistent with the EDM Council Cloud Data Management Capabilities framework.

QUESTION NO: 48

The loading of country codes into a CRM is a classic:

A. Reference data integration

B. Fact data integration

C. Master data integration

D. Analytics data integration

E. Transaction data integration

ANSWER: A

Explanation:

Reference data integration is correct because country codes are standardized, relatively stable code values used to classify and consistently interpret business data across systems. In a CRM, a country-code list commonly supplies permitted values and associated definitions—such as an ISO country identifier, country name, and possibly region or currency—to support consistent customer and address records. Loading this controlled set into the CRM is therefore an integration of reference data: reusable classification data that provides common context for operational records rather than describing an individual customer, event, or transaction. DAMA's data-management guidance distinguishes reference data as codes and descriptions used to categorize other data, and recognizes its governance as essential for interoperability and consistent reporting. ISO's country-code standard is a common real-world example of such a controlled reference dataset. See the ISO 3166 country-code overview and DAMA International's Data Management Body of Knowledge resources.

QUESTION NO: 49

Business glossaries have the following objectives:

A. Improve the alignment between technology assets and the business organization.

B. Capture cultural factors that might impact the concepts and terminology.

C. Maximise search capability and enable access to documented institutional knowledge.

D. Enable common understanding of the core business concepts and terminology.

E. Reduce the risk that data will be misused due to inconsistent understanding of the business concepts.

ANSWER: A B C D E

Explanation:

A business glossary is a governed collection of agreed business terms, definitions, relationships, and related context. Its objectives include creating a shared understanding of core concepts and terminology, which gives business users, data professionals, and technology teams a consistent semantic foundation for communicating about data. It also improves alignment between business needs and technology assets by connecting business language to data assets, models, reports, and systems.

Glossaries make documented institutional knowledge easier to find and reuse, strengthening search and discovery capabilities. By establishing approved meanings and ownership for terms, they reduce the likelihood that data will be interpreted or used inconsistently. A mature glossary also captures cultural, organizational, regional, or domain-specific context that can affect how a concept or term is understood. That context is essential when standardizing terminology across teams while retaining necessary business nuance. These objectives support the DAMA view of business glossaries as foundational semantic and governance assets that enable reliable data use across the organization. See DAMA International's Data Management Body of Knowledge overview and Technics Publications' DAMA-DMBOK resource page.

QUESTION NO: 50

In defining a Data Security Policy, what role should Data Governance play?

A. Write the Data Security Policy

B. Send all Data Security questions to the legal department

C. Have no role in the Data Security Policy

D. Review and approve the Data Security Policy

E. Own and maintain the Data Security Policy

ANSWER: D

Explanation:

Review and approve the Data Security Policy is correct because Data Governance provides the decision-making, oversight, and accountability structure that ensures security policy is aligned with organizational data strategy, risk tolerance, regulatory obligations, and business requirements. In a DAMA-oriented operating model, the governance function establishes policy direction and resolves cross-functional issues through an appropriate governance council or similar authority. It should ensure that accountable business, legal, privacy, risk, and technology stakeholders have reviewed the policy and that its requirements can be applied consistently across data domains.

Approval is an important governance control: it makes the policy an authorized organizational standard rather than merely a technical document. Governance should also require periodic review when regulations, business use of data, classifications, or risks change, and should monitor whether policy-related controls and exceptions are managed appropriately. The operational security function normally develops, implements, and administers the detailed controls, while governance supplies the oversight and formal authorization needed for sustainable accountability. This separation supports clear decision rights and effective stewardship of data as an enterprise asset. See DAMA International's overview of the Data Management Body of Knowledge and NIST guidance on information-security program policy and governance in NIST SP 800-12 Rev. 1.

QUESTION NO: 51

Please select the two classifications of database types:

A. Centralized

B. Generic

C. Distributed

D. MapReduce

ANSWER: A C

Explanation:

Centralized and Distributed are the two applicable classifications because they describe the fundamental architectural placement of database data and processing resources. A centralized database stores and manages data at one central location or system, with users and applications accessing that authoritative repository. This arrangement supports consistent administration, governance, security controls, backup procedures, and management of shared data. IBM describes centralized databases as databases located at a single site and accessed by users from multiple locations.

A distributed database stores logically related data across multiple networked locations while presenting or managing it as a coordinated database environment. Distribution may support local access, availability, scalability, and geographic or organizational requirements; it also requires coordinated management of data, metadata, synchronization, and integrity. These classifications are important to data management because database architecture affects ownership, data quality controls, security, integration, recovery, and operational responsibilities. See IBM's overview of centralized and distributed databases and Oracle's discussion of distributed database concepts.

QUESTION NO: 52

The categories of the Data Model Scorecard with the highest weightings include:

A. How well does the model capture the requirements?

B. None of the above

C. How good are the definitions?

D. How complete is the model?

E. How structurally sound is the model?

F. All of the above

ANSWER: A D E

Explanation:

The highest-weighted Data Model Scorecard categories are **How well does the model capture the requirements?**, **How complete is the model?**, and **How structurally sound is the model?**. These dimensions focus on whether a model represents the business need faithfully, includes the necessary entities, attributes, relationships, and rules, and applies sound modeling structures that can be understood and maintained. Together, they assess the model's practical fitness for use: a model must first address the stated requirements, contain sufficient scope and detail, and be structurally robust enough to support consistent implementation and future change.

In DAMA's data modeling and design discipline, data models are treated as essential artifacts for communicating data requirements and establishing a reliable foundation for data integration, database design, and governance. Giving the greatest emphasis to requirements coverage, completeness, and structural soundness prioritizes the characteristics that most directly determine whether the model can support the intended business and technical outcomes. Definitions remain important metadata and governance assets, but the scorecard's highest-weighted areas emphasize the model's substantive representation and design quality. See DAMA International's Data Management Body of Knowledge information and the publisher's DAMA-DMBOK reference page.

QUESTION NO: 53

Data modelling tools and model repositories are necessary for managing the enterprise data model in all levels.

A. TRUE

B. FALSE

ANSWER: A

Explanation:

TRUE is correct because an enterprise data model must be managed as a durable, shared information asset across conceptual, logical, and physical levels of detail. Data modelling tools provide the controlled environment for creating, visualizing, validating, comparing, and maintaining models. A model repository preserves the models and their associated metadata, including definitions, relationships, standards, ownership, version history, and links between levels of abstraction.

This repository-based approach supports traceability: a business concept represented at the conceptual level can be connected to its logical data structures and, where applicable, to implemented physical structures. It also enables collaboration among data architects, modelers, data stewards, business stakeholders, and technical teams while reducing duplication and inconsistent definitions. Governance depends on being able to locate the approved model, understand its status, control changes, and reuse established data structures and naming standards. DAMA's body of knowledge treats data modeling and metadata management as essential, interrelated data-management disciplines, making managed modeling tools and repositories foundational capabilities for enterprise data architecture. See DAMA International's Data Management Body of Knowledge and its CDMP certification overview.

QUESTION NO: 54

One of the deliverables in the Data Integration and Interoperability context diagram is:

A. Data Integration and Interoperability Strategy

B. Data hogging

C. Data access agreements

D. Data security plan

ANSWER: C

Explanation:

Data access agreements is a valid deliverable of Data Integration and Interoperability because integration work enables data to move, be shared, or be made available across applications, organizational units, and external parties. Such sharing requires a documented agreement that defines who may access data, for what approved purpose, under which conditions, and with what responsibilities. These agreements provide an operational control point between the technical mechanisms that exchange data and the governance expectations governing its appropriate use.

Within the DAMA-DMBOK view, Data Integration and Interoperability is concerned with the planning, implementation, and control of data movement and data sharing across boundaries. A data access agreement supports those outcomes by documenting access arrangements and helping ensure that exchanged data is available to authorized consumers in a managed, accountable manner. It also gives integration teams a clear basis for configuring interfaces, provisioning access, and applying relevant handling requirements. DAMA's Data Management Body of Knowledge identifies Data Integration and Interoperability as a core data-management knowledge area; the published DMBOK reference is available from Technics Publications, and DAMA International's overview of the body of knowledge is available at DAMA International.

QUESTION NO: 55

The process of identifying how different records may relate to a single entity is called:

A. Meshing

B. Munging

C. Mirroring

D. Matching

E. Mangling

ANSWER: D

Explanation:

Matching is the correct term for identifying records that represent, or may represent, the same real-world entity—for example, customer records held in separate systems or duplicate records within one dataset. The activity evaluates identifying attributes such as name, address, email address, date of birth, or business identifiers to determine the likelihood that records relate to one entity. Matching can use exact comparisons, standardized values, fuzzy or probabilistic techniques, and match rules with confidence thresholds. Its results support linking records, detecting duplicates, constructing a consolidated entity view, and deciding whether records should be merged or managed through survivorship rules. In DAMA data-management practice, matching is an important capability in data quality, data integration, and master data management because reliable entity identification is required before data from multiple sources can be integrated into trusted master records. The DAMA Dictionary defines data matching in terms of identifying records that correspond to the same entity. See the DAMA-DMBOK reference page and DAMA International's Data Management Body of Knowledge overview.

QUESTION NO: 56

According to the DMBoK2, by creating Data Management Services, IT involves the Data Governance Council:

A. To estimate the enterprise needs for these services and provide the justification for staffing and funding to provide these services

B. To provide a funnel for data and information issues to take the administration load off IT

C. To ensure that data and information is still managed by IT and business only plays an advisory role

D. To enable the business to maintain oversight on data and information projects

E. To provide data stewards as and when needs to perform services where IT resources are either not available or do not exist

ANSWER: D

Explanation:

The correct answer is *"To enable the business to maintain oversight on data and information projects"*. In the DAMA-DMBOK view, Data Governance establishes the decision rights, accountability, direction, and oversight needed to manage data as an enterprise asset. Data Management Services provide an operational means for IT to deliver data-related capabilities in a manner that is visible, coordinated, and aligned with business priorities. This service-oriented approach gives the Data Governance Council a practical mechanism through which to oversee the data and information initiatives that affect the organization. The Council can use that oversight to ensure that projects reflect enterprise policies, business requirements, data-quality expectations, risk obligations, and strategic objectives. It also supports communication and accountability between business stakeholders and technology teams, rather than treating data initiatives as isolated IT work. The emphasis is therefore on enabling sustained business oversight of the data and information project portfolio through formalized services and governance engagement. DAMA describes its Body of Knowledge as the framework for data-management principles, practices, and disciplines: DAMA Body of Knowledge. Further background on data governance as organizational decision-making and accountability is available from the EDM Council DCAM framework.

QUESTION NO: 57

Data science merges data mining, statistical analysis, and machine learning with the integration and data modelling capabilities, to build predictive models that explore data content patterns.

A. FALSE

B. TRUE

ANSWER: B

Explanation:

TRUE is correct. Data science is an interdisciplinary practice that applies statistical analysis, data mining, machine learning, and programming techniques to data in order to discover meaningful patterns and develop models. Its work depends on more than the analytical algorithm itself: data must be acquired, integrated from relevant sources, assessed for quality, transformed into usable analytical data sets, and represented through appropriate data structures or models. These information-management capabilities enable analysts to understand the available content and prepare reliable inputs for exploratory, descriptive, and predictive analysis.

Predictive models use observed data and identified relationships to estimate likely future outcomes or unknown values. Data mining contributes pattern-discovery methods, statistical analysis provides rigorous methods for inference and evaluation, and machine learning supplies techniques for training models that generalize from examples. Together, these disciplines support the stated goal of exploring data-content patterns and building predictive models. DAMA recognizes data science as closely related to, and dependent on, core data-management disciplines, including data integration, data quality, metadata, and data modeling. See DAMA International's Data Management Body of Knowledge information and the publisher description of DAMA-DMBOK2.

QUESTION NO: 58

Defining quality content requires understanding the context of its production and use, including:

A. Producers

B. Timing

C. None of the above

D. Delivery

E. Consumers

F. Format

ANSWER: A B D E F

Explanation:

Quality content cannot be defined solely by whether information is accurate or well written; it must be fit for its intended purpose within the business context. **Producers** matter because their authority, expertise, responsibilities, and the processes used to create content affect its reliability and governance. **Consumers** define the needs the content must satisfy, such as the decisions, tasks, accessibility requirements, and level of detail required for effective use.

Timing is essential because content has to be current, available at the required point in a process, and retained or refreshed according to its business value. **Delivery** concerns the channel, workflow, access method, and distribution controls that make content available to intended users. **Format** determines whether content can be understood, exchanged, searched, processed, preserved, and reused in its intended environment. Together, these contextual factors support the DAMA principle that data and content quality are assessed relative to purpose and use, rather than as isolated intrinsic characteristics. DAMA's body of knowledge recognizes content and document management as a data-management discipline, while ISO's information-quality guidance emphasizes suitability for user needs and context. See DAMA International's Data Management Body of Knowledge information and ISO 8000-8 information-quality standard.

QUESTION NO: 59

An organization will create an uncover valuable Metadata during the process of developing

Data Integration and Interoperability solutions.

A. TRUE

B. FALSE

ANSWER: A

Explanation:

TRUE is correct. Developing Data Integration and Interoperability solutions inherently creates and reveals metadata that is valuable for managing data as an organizational asset. Integration work requires teams to identify source and target systems, define data structures, document attributes, map source fields to target fields, specify transformations, establish business rules, and record data movement. These activities produce both technical metadata, such as schemas, interface definitions, mappings, and lineage, and business metadata, such as definitions, ownership, and usage context.

This metadata is especially valuable because it makes data flows understandable, traceable, and repeatable. It supports impact analysis when a source system or field changes, enables troubleshooting and reconciliation, assists with data-quality monitoring, and improves reuse of integration assets. Capturing it as part of delivery rather than treating it as a separate afterthought also helps establish consistent governance across interoperating systems. DAMA's Data Management Body of Knowledge identifies metadata management as a foundational capability that supports other data-management knowledge areas, including data integration and interoperability. DAMA describes the DMBOK framework at DAMA International—Body of Knowledge. The importance of lineage and metadata for understanding transformations is also reflected in IBM's overview of data lineage.

QUESTION NO: 60

Two risks with the Matching process are:

A. False positives

B. False Certainties

C. False Negatives

D. False Uncertainties

ANSWER: A C

Explanation:

False positives and false negatives are the two fundamental risks in a data matching process. Matching compares records to decide whether they refer to the same real-world entity, such as a customer, supplier, product, or location. A false positive occurs when the process identifies records as a match even though they represent different entities. This can incorrectly merge or link records and can distort a trusted view of the entity. A false negative occurs when records that represent the same entity are not identified as a match. This leaves duplicate or fragmented records unlinked, reducing the completeness of an entity view and potentially causing inconsistent reporting or operations.

These risks arise because matching commonly relies on imperfect identifiers and comparison rules, including names, addresses, dates, codes, similarity scores, and confidence thresholds. Data-management practice therefore involves defining match rules appropriate to the business purpose, measuring matching quality, reviewing uncertain cases where appropriate, and tuning thresholds to balance the relative business impact of false positives and false negatives. This is consistent with data-quality work on duplicate detection and record linkage. See DAMA International's Data Management Body of Knowledge resources and NIST's discussion of false-positive and false-negative matching errors.

QUESTION NO: 61

Time-based patterns are used when data values must be associated in chronological order and with specific time values.

A. TRUE

B. FALSE

ANSWER: A

Explanation:

TRUE is correct. Time-based, or temporal, data-modeling patterns represent facts whose meaning depends on when they occurred, were observed, or were valid. They enable data values to be connected to explicit time points or periods and then ordered chronologically for analysis, reporting, auditing, and historical interpretation. For example, a model may need to record a customer's address during a particular validity period, a product's price at a stated effective date, or measurements captured at successive timestamps. In each case, the time attribute is not merely descriptive metadata: it establishes the temporal context needed to interpret the value accurately and sequence related values correctly.

Temporal modeling commonly distinguishes the time an event occurred from the period during which a fact is considered valid, because both perspectives may be relevant to business rules and data-quality requirements. Associating values with defined dates, times, or intervals also supports trend analysis and reliable reconstruction of past states. These principles align with established temporal-data concepts described by the ISO 8601 date and time standard and with the SQL standard's treatment of temporal data types, summarized by ISO/IEC 9075-2:2023.

QUESTION NO: 62

An authoritative system where data is created/captured, and/or maintained through

a defined set of rules and expectations is called:

A. A System of Systems

B. A System of Retirement

C. A System of Record

D. A System of Reference

E. A System of Referential Integrity

ANSWER: C

Explanation:

A System of Record is correct because it is the authoritative source responsible for creating, capturing, and/or maintaining a defined set of data according to established business rules, controls, and accountability expectations. It is the system that an organization recognizes as the trusted operational source for a particular data domain or record type, such as customer, employee, product, or financial-transaction data. Data governance identifies the accountable owners and stewards for the information managed there, while data-quality rules and lifecycle processes help ensure the data remains accurate, complete, timely, and controlled. A system of record need not be the only place where data is viewed or used: downstream analytical, reporting, integration, and reference systems may consume copies. However, when a data value must be created, corrected, or formally maintained, the governed authoritative process is associated with the system of record. This distinction supports consistent master and reference data management, traceability, and reliable enterprise reporting. DAMA's body of knowledge treats authoritative sources and controlled data lifecycle management as central concepts in data governance and data architecture. See DAMA-DMBOK resources from Technics Publications and the DAMA CDMP certification overview.

QUESTION NO: 63

Small reference data value sets in the logical data model can be implemented in a physical model in three common ways:

A. Create a matching separate code table

B. Create a master shared code table

C. None of the above

D. Program integration by joining tables

E. Embed rules or valid codes into the appropriate object's definition.

F. Roadmap Development

ANSWER: A B E

Explanation:

Small, stable reference-value sets represented in a logical model need a physical implementation that both constrains permitted values and makes their meanings consistently available to systems and users. "Create a matching separate code table" is a standard relational implementation: each logical value set becomes its own lookup table, and dependent tables use a foreign key to the applicable code. This preserves value definitions, supports descriptions and effective metadata, and makes governance of the set explicit.

"Create a master shared code table" is also appropriate where multiple value sets can be administered through a common structure. Such a table typically identifies the value-set or domain along with the code and its descriptive attributes, allowing centrally governed reuse of reference data across physical tables.

"Embed rules or valid codes into the appropriate object's definition." is suitable for a small set that is unlikely to change frequently. A database constraint, domain definition, or equivalent rule can enforce the permitted values directly at the column level. DAMA's data-management guidance emphasizes modeling and governing reference data as controlled, reusable business values, while relational constraints are a core mechanism for protecting data integrity. See DAMA International: Data Management Body of Knowledge and PostgreSQL documentation: Constraints.

QUESTION NO: 64

Functionality-focused requirements associated with a comprehensive metadata solution, include:

A. Synchronization

B. Structure

C. None of the above

D. History

E. Volatility

F. Access rights

ANSWER: A B D E F

Explanation:

A comprehensive metadata solution must support the operational characteristics needed to capture, govern, maintain, and use metadata throughout its lifecycle. *Synchronization* is required so that metadata remains aligned across integrated repositories, tools, and source systems. *Structure* provides the defined models, relationships, classifications, and standards that make metadata consistent and understandable. *History* preserves prior metadata states and changes, supporting lineage, traceability, auditability, and impact analysis. *Volatility* addresses the fact that metadata changes at different rates; a solution must be able to manage both relatively stable business definitions and frequently changing technical or operational metadata. *Access rights* enable appropriate stewardship and control by defining who may view, create, update, approve, or administer metadata. Together, these capabilities support metadata as governed, reusable organizational knowledge rather than a static collection of descriptions. DAMA's Data Management Body of Knowledge identifies metadata management as a core data-management discipline and emphasizes governance, integration, quality, and controlled access as essential considerations. See DAMA International's Body of Knowledge overview and the DAMA-DMBOK information page.

QUESTION NO: 65

What position is responsible for the quality and use of their organization's data assets?

A. Chief Information Officer

B. Data Scientist

C. Data Steward

D. Data Modeler

E. Data Architect

ANSWER: C

Explanation:

Data Steward is correct because data stewardship assigns accountable business-facing responsibility for the day-to-day management of data within a defined domain. A steward helps ensure that data is understood, fit for its intended purposes, and used consistently with organizational policies, standards, and governance decisions. This includes defining or maintaining business terms and metadata, identifying data-quality expectations, monitoring and escalating quality issues, supporting issue resolution, and guiding appropriate data use by people across the organization. The role therefore connects governance policy with practical management of data assets and promotes trustworthy, usable data. DAMA's Data Management Body of Knowledge identifies stewardship as a fundamental Data Governance responsibility and describes data stewards as responsible for the management and fitness of data assets in their assigned areas. The DAMA International overview of the *DAMA-DMBOK* also places Data Governance at the center of defining decision rights, accountabilities, and controls for data management. See DAMA International: Body of Knowledge and Technics Publications: DAMA-DMBOK.

QUESTION NO: 66

Considerations for whether to integrate two data stores should include all except

the:

A. Maintaining of master data trust across the two data stores

B. Privacy and access consideration for the data

C. Complexity of data operations

D. Ability to govern the data across both systems

E. Capability of the systems to support the data natively

ANSWER: C

Explanation:

Complexity of data operations is the exception. The decision to integrate data stores is principally an architectural and governance decision: it must establish whether data can be consistently understood, trusted, protected, controlled, and used across the participating environments. DAMA's data-management approach emphasizes accountable stewardship, data quality, metadata, security, and governance as essential controls wherever data is shared or integrated. The key question is therefore whether the organization can preserve appropriate authority, trust, privacy, access control, and native system support for the data after integration. Operational complexity may be affected by an integration design and should be managed during implementation, but it is not itself a fundamental criterion for deciding whether two stores should be integrated. It is a consequence or delivery concern rather than a core suitability consideration. This distinction helps prevent teams from treating an integration purely as a technical pipeline exercise instead of assessing whether the resulting data environment can be responsibly governed and relied upon for business use. See the DAMA International overview of the DMBoK framework at DAMA International: Body of Knowledge and the DMBoK publisher's description at Technics Publications: DAMA-DMBOK.

QUESTION NO: 67

Typically, DW/BI projects have three concurrent development tracks, including:

A. Technology

B. Trickle Feeds

C. Data

D. BI Tools

E. Messaging

F. Streaming

ANSWER: A C D

Explanation:

DW/BI delivery commonly proceeds through concurrent technology, data, and BI-tool tracks because a usable analytical solution depends on all three being ready together. **Technology** covers the technical platform and operational capabilities needed to run the warehouse and BI environment, such as infrastructure, database services, integration tooling, security, deployment, and performance capacity. **Data** covers the acquisition, integration, transformation, quality management, modeling, and loading of trusted information into the warehouse or other analytical data stores. This track establishes the governed, consistent data foundation on which reporting and analysis rely. **BI Tools** covers the user-facing analytical layer: semantic access, reports, dashboards, visualizations, self-service analysis, and related delivery capabilities. Treating these as concurrent tracks supports iterative development: the platform can be provisioned as data pipelines are built, while BI content is developed and validated against progressively available data. This aligns with DAMA's view that data management comprises coordinated disciplines, including data architecture, data integration, data quality, data warehousing/business intelligence, and data security. Kimball's lifecycle guidance likewise emphasizes coordinated work across technology, data, and BI application delivery. See DAMA International's Body of Knowledge overview and Kimball Group's DW/BI techniques.

QUESTION NO: 68

The information governance maturity model describes the characteristics of the information governance and recordkeeping environment at five levels of maturity for each of the eight

GARP principles. Please select the correct level descriptions:

A. Level 2 In Development

B. Level 4 Proactive

C. Level 2 Sub-standard

D. Level 4 Proactive

E. Level 3 Transformational

F. Level 3 Essential

ANSWER: A B D F

Explanation:

The correctly stated maturity levels are **Level 2 In Development**, **Level 3 Essential**, and **Level 4 Proactive**. These names are part of the Generally Accepted Recordkeeping Principles maturity model, which provides a structured way to assess the maturity of an organization's information governance and recordkeeping practices across each GARP principle. At the In Development level, an organization has begun establishing and implementing relevant policies, procedures, and controls. At the Essential level, recordkeeping capabilities are established sufficiently to support routine business and legal requirements.

At the Proactive level, governance is managed strategically and systematically, with practices designed to anticipate needs and reduce information-related risk.

The model's five ordered maturity descriptions are Sub-standard, In Development, Essential, Proactive, and Transformational. Therefore, each occurrence of the text **Level 4 Proactive** is a valid level description, even though it appears twice in the supplied choices. This maturity framework helps organizations identify their current state and define practical improvement targets for accountable information governance. ARMA International describes the GARP framework and its recordkeeping principles at ARMA's Generally Accepted Recordkeeping Principles. Additional information on managing federal records and accountability is available from the U.S. National Archives Records Management.

QUESTION NO: 69

Examples of interaction models include:

A. Hub-and-spoke

B. Publish - subscribe

C. Point-to-point

D. Wheel-and-spike

ANSWER: A B C

Explanation:

Hub-and-spoke, Publish - subscribe, and Point-to-point are established interaction models used to describe how systems, applications, or data consumers exchange messages and data. Hub-and-spoke centralizes exchanges through an integration hub, enabling participating systems to connect through a common intermediary rather than maintaining a separate direct connection with every other system. This pattern supports managed routing, transformation, governance, and reuse of integration services.

Publish - subscribe supports event-driven interaction: publishers emit messages or events without needing to identify individual recipients, while subscribers receive messages for the topics to which they have subscribed. This decoupling is particularly useful where one data event must be distributed to multiple downstream consumers. Point-to-point describes direct communication in which a sender delivers a message to one intended receiving endpoint or queue, supporting a clear producer-to-consumer exchange. These models are important integration design concepts because they determine coupling, distribution behavior, routing responsibilities, and operational management of data flows. See Enterprise Integration Patterns: Messaging Patterns and AWS Prescriptive Guidance on messaging patterns.

QUESTION NO: 70

Please select the answer that best fits the following description: Contains only real-time data.

A. Batch layer

B. Speed layer

C. Serving layer

D. Real-time layer

ANSWER: B

Explanation:

In the Lambda Architecture model, **Speed layer** is the component that contains and processes the most recently arrived, real-time data. Its purpose is to make fresh events available for analysis before those events have been incorporated into the comprehensive batch computation. Because batch processing has an inherent processing delay, the speed layer provides low-latency handling of incoming data streams and produces real-time views or updates that can be queried promptly.

This layer is intentionally limited to the current, not-yet-batch-processed portion of the data stream. As data becomes part of the durable batch dataset and is recomputed by the batch process, the corresponding speed-layer results can be replaced or reconciled with the more complete batch results. This division allows an architecture to combine timely responses for newly arriving data with accurate, historical recomputation over the full dataset. The description “Contains only real-time data” therefore identifies the Speed layer. An overview of Lambda Architecture and its batch and speed paths is available from Martin Fowler’s Lambda Architecture article; the original architectural framing is also described in Big Data: Principles and Best Practices of Scalable Realtime Data Systems.

QUESTION NO: 71

Inputs in the reference and master data context diagram include:

A. None of the above

B. Business Drivers

C. Business model

D. Data Glossary

E. Cultural Drivers

F. All of the above

ANSWER: B D

Explanation:

Business Drivers and Data Glossary are inputs to reference and master data management because they establish both the purpose for the work and the shared meaning needed to perform it consistently. Business Drivers express the organizational needs that justify and prioritize master and reference data capabilities, such as improving reporting consistency, supporting regulatory obligations, integrating systems, or improving customer and product operations. They guide which domains should be addressed, the expected business outcomes, and the level of investment and governance required.

A Data Glossary provides agreed business terms, definitions, and usage rules. This is essential when identifying authoritative master-data entities and reference-data values, since shared definitions allow business and technical stakeholders to distinguish concepts consistently across processes and systems. The glossary helps ensure that managed data represents business concepts in a clear, reusable manner and supports semantic consistency in downstream integration, analytics, and governance activities.

These inputs align with DAMA’s treatment of reference and master data management as a business-driven discipline that relies on common definitions and governance. See the DAMA Body of Knowledge and the DAMA-DMBOK2 overview.

QUESTION NO: 72

Issues caused by data entry processes include:

A. Data entry interface issues

B. List entry placement

C. Field overloading

D. None of the above

E. Training issues

F. Changes to business processes

ANSWER: A B C E F

Explanation:

Data entry quality depends on both the design of the capture process and the people and business context in which it operates. Data entry interface issues are a direct source of defects when screens, labels, validation prompts, defaults, or navigation do not make the intended value clear. List entry placement also affects accuracy: lists that are poorly ordered, difficult to find, or separated from the relevant field increase selection mistakes. Field overloading causes ambiguity when one field is used to store multiple meanings or values, making consistent entry and subsequent interpretation difficult.

Training issues are equally important because users need to understand data definitions, allowable values, entry conventions, and the operational consequences of inaccurate or incomplete capture. Changes to business processes can introduce new data requirements, alter ownership, or invalidate established entry procedures; unless supporting forms, interfaces, definitions, and training are updated, data quality problems can result. These are recognized practical sources of data-quality defects at the point of capture and should be addressed through clear standards, usable controls, stewardship, and ongoing process management. See the DAMA Body of Knowledge overview and the ISO 8000 data quality standard information.

QUESTION NO: 73

Why is it so important to conduct a Data Governance Readiness Assessment?

A. Because it will show that the Data Governance team is working hard

B. It will give the Business some metrics

C. It is important because the organization will have an opportunity for business people to be identified as data stewards

D. It is important because it will prove that the IT department is best qualified to define, develop, and manage the organizationâ€™s data assets

E. It will identify the readiness and level of maturity that an organization will need to effectively govern and sustain its data, processes, and policies

ANSWER: E

Explanation:

It will identify the readiness and level of maturity that an organization will need to effectively govern and sustain its data, processes, and policies. A Data Governance Readiness Assessment establishes a practical baseline before an organization launches or expands a governance program. It evaluates whether essential foundations are sufficiently in place, including executive sponsorship, defined decision rights, accountability, organizational roles, policy and standards capabilities, data-management processes, and the capacity to sustain change. Understanding this starting point allows leaders to identify gaps, prioritize realistic improvements, sequence implementation activities, and tailor the governance operating model to the organization's actual capabilities and needs. The assessment therefore supports an achievable roadmap rather than treating governance as a one-time project or a purely technical initiative. It also provides a maturity benchmark that can be used to measure progress as governance capabilities become more formalized and embedded in business operations. This purpose aligns with DAMA's treatment of Data Governance as the exercise of authority, control, and shared decision-making over data assets, supported by ongoing planning, oversight, and monitoring. See the DAMA Body of Knowledge and DAMA International's overview of Data Governance.

QUESTION NO: 74

Data science involves the iterative inclusion of data sources into models that develop insights. Dat science depends on:

A. Consistency

B. Rich data sources

C. Information alignment and analysis

D. Information delivery

E. Presentation of findings and data insights

F. All of the above

ANSWER: B C D E

Explanation:

Data science depends on *rich data sources*, because iterative modeling requires sufficiently broad, relevant, and usable data from which to identify patterns, test hypotheses, and refine models. It also depends on *information alignment and analysis*: data from different sources must be understood in context, related appropriately, assessed for fitness, and analyzed using suitable statistical, analytical, or machine-learning methods. Without this alignment, adding sources can create misleading rather than useful results.

Information delivery is essential because analytical outputs must reach the people, processes, applications, or decision points where they can be used. Data science creates value when insights are operationalized or made available for informed action, not merely when a model is built. Finally, *presentation of findings and data insights* is a core dependency because results need to be communicated clearly, with appropriate context, interpretation, and visualization, so that stakeholders can understand the findings and make decisions responsibly. These elements reflect the broader DAMA view that data management enables the availability, integration, analysis, communication, and effective use of data and information. See DAMA International's Data Management Body of Knowledge overview and the publisher's information for The DAMA Guide to the Data Management Body of Knowledge.

QUESTION NO: 75

Device security standards include:

A. Access policies regarding connections using mobile devices

B. Awareness of security vulnerabilities

C. Installation of malware software

D. Storage of data on fixed devices

ANSWER: A B D

Explanation:

Device security standards establish required safeguards for endpoints that create, access, process, or retain organizational data. **Access policies regarding connections using mobile devices** are essential because mobile endpoints may connect through less controlled networks and can introduce data-access risks; standards should specify authorization, secure connection requirements, device-management controls, and acceptable use. **Awareness of security vulnerabilities** is also a core requirement because users and administrators need to recognize weaknesses such as unpatched software, insecure configurations, phishing, loss or theft, and compromised applications so that they can apply required controls and report incidents promptly. **Storage of data on fixed devices** belongs in device-security standards because organizations must define whether data may reside on managed desktops, workstations, or other fixed endpoints and require appropriate safeguards such as access control, encryption where applicable, retention controls, secure disposal, and managed backup practices. Together, these measures support the DAMA data-security objective of protecting data confidentiality, integrity, and availability through policies and operational controls. NIST's endpoint and mobile-device guidance likewise emphasizes managed devices, secure configuration, access restrictions, and protection of data stored on endpoints. See DAMA International Body of Knowledge and NIST SP 800-124 Rev. 2, Guidelines for Managing the Security of Mobile Devices.