Free Questions for CDFOM

Shared by Everett on 06-01-2026

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

Which process is not part of the 6-step document management life cycle?

Options:

A- Creation
B- Publication
C- Provisioning
D- Destruction

Answer:

C

Explanation:

EPI's document management methodology follows a 6-step structured life cycle for all controlled documentation used in a data center (e.g., SOPs, MOPs, EOPs, safety documents, policies, maintenance procedures).

The life cycle ensures all documents remain current, controlled, traceable, and properly retired.

The six recognized stages in the EPI-aligned document management life cycle are typically:

Creation -- The document is drafted and developed.

Review -- Subject matter experts verify technical correctness.

Approval -- Authorized managers approve it for release.

Publication / Release -- Document is issued for operational use under control.

Maintenance / Updates -- Regular updates and version control.

Archival / Destruction -- Retired versions are archived or securely destroyed.

Within this structure, ''Provisioning'' is not a recognized document life-cycle step in EPI's DCFOM framework.

Provisioning is a term used in IT or service management (e.g., server or user provisioning) but not in document control life cycles.

Therefore, Option C (Provisioning) is the correct answer.

EPI DCFOM-Aligned Reference Concepts (Paraphrased, Not Verbatim)

Document management requires strict version control procedures.

The document life cycle includes creation, review, approval, publication, maintenance, and destruction/archival.

''Provisioning'' is not part of the document lifecycle in the EPI framework.

Question 2

Question Type: MultipleChoice

During lock-out/tag-out, which of the below is the most recommended procedure?

Options:

A- Operator locking out the equipment and another operator removing the lock-out
B- Operator locking out the equipment and the safety manager removing the lock-out
C- Operator locking out the equipment and the facilities manager removing the lock-out
D- Operator locking out the equipment and the same operator removing the lock-out

Answer:

D

Explanation:

In the EPI Facilities Operations Manager body of knowledge, the Lock-Out/Tag-Out (LOTO) procedure is a mandatory safety control to ensure that electrical or mechanical equipment cannot be energized while work is being performed. A core principle emphasized in EPI safety training is:

''The person who applies the lock must be the same person who removes it.''

This aligns with international best practices for occupational health and safety, where LOTO ensures that the individual performing maintenance or repair has full control of the energy isolation device.

Why this is required:

Personal Safety Responsibility

The lock identifies the technician directly working on the equipment. Only they can confirm whether work is complete and the area is safe for re-energizing.

Risk Prevention

If someone else removes the lock (another operator, safety manager, or facilities manager), they may incorrectly assume that the equipment is ready to be restored, which can lead to severe injury or fatality.

Compliance With EPI Safety Guidelines

EPI emphasizes the principle of ''single-person control'' over hazardous energy. No supervisor or colleague may remove another technician's lock unless a formal, documented emergency override procedure is followed --- which is not considered standard practice.

Clear Accountability Chain

LOTO prevents ambiguity or miscommunication. The technician who placed the lock is the only one with full knowledge of the work status and hazards involved.

Why other options are incorrect:

A, B, and C violate the fundamental LOTO rule because they involve someone other than the applying operator removing the lock.

Oversight personnel (safety manager, facilities manager) monitor and audit the process, but they should not remove another person's lock except under rare, emergency, escalation-approved situations.

EPI DCFOM-Aligned Reference Concepts (Paraphrased, Not Verbatim)

LOTO must ensure the isolation device is locked and tagged by the person performing the work.

Only the same individual may remove their own lock.

Removal by another party is only permitted under controlled, documented emergency protocols.

The process prevents accidental energization and protects worker safety.

Question 3

Question Type: MultipleChoice

What is the main reason for (senior) management to be scheduled into the 'on-duty' roster?

Options:

A- It provides management hands-on experience solving incidents.
B- It provides management better insights with the number of incidents occurring
C- It involves management when incidents are escalating
D- It assists management in optimally reviewing monitoring thresholds

Answer:

C

Explanation:

Senior management is included in the duty roster to support escalation procedures.

In EPI's operational model:

Managers are not part of routine monitoring or incident handling.

Their role is to intervene only when an incident escalates beyond operational authority, such as major outages, SLA-impacting events, or high-risk situations.

Management provides decision-making, authorization, and resource allocation during escalations.

Why other options are incorrect:

A: Managers should not gain ''hands-on'' experience during incidents.

B: Incident reporting already provides insights; no roster needed.

D: Monitoring thresholds are reviewed separately, not via duty rosters.

Thus, C is correct.

EPI DCFOM-Aligned Reference Concepts (Paraphrased)

Management is involved in the escalation layer, not daily operations.

Duty rosters ensure proper escalation handling and governance.

Question 4

Question Type: MultipleChoice

The organization plans for implementing an information security management system (ISMS).

By doing so, what is the main objective?

Options:

A- Preservation of an organizations' financial and organizational records
B- Preservation of confidentiality and format of organizational assets
C- Preservation of confidentiality, integrity and availability of organizational assets
D- Preservation of customer agreements and records

Answer:

C

Explanation:

An Information Security Management System (ISMS) is designed to protect information assets through structured controls, policies, and risk management practices.

EPI aligns with globally accepted security frameworks (e.g., ISO/IEC 27001), where the foundation of an ISMS is the CIA triad:

C --- Confidentiality

Ensures information is accessible only to authorized persons.

I --- Integrity

Ensures information is accurate, complete, protected from unauthorized modification.

A --- Availability

Ensures information and systems are accessible when required.

Implementing an ISMS aims to safeguard these three fundamental information security objectives.

Why the other options are incorrect:

A --- This focuses only on records retention, not information security as a whole.

B --- Omits integrity and availability, which are essential ISMS elements.

D --- Too narrow; ISMS covers all information assets, not just customer records.

Thus, the correct answer is C, which fully represents the CIA triad.

EPI DCFOM-Aligned Reference Concepts (Paraphrased)

ISMS is responsible for protecting confidentiality, integrity, and availability of all information assets.

The CIA triad forms the basis of information security objectives.

Question 5

Question Type: MultipleChoice

Several data center services in the service catalog charge the customer on the actual usage of those services.

What chargeback model is applied?

Options:

A- Service Based Pricing (SBP)
B- Negotiated Flat Rate (NFR)
C- Tiered Flat Rate (TFR)
D- Measured Resource Usage (MRU)

Answer:

D

Explanation:

When customers are billed based on the actual consumption of services, this model is known as Measured Resource Usage (MRU).

MRU charges customers according to:

Actual power consumption

Actual cooling usage

Actual rack utilization

Actual bandwidth or cross-connect usage

Actual resource usage metrics

This model aligns with transparency, fairness, and resource accountability.

Why other options are incorrect:

A -- SBP: Charges based on predefined service definitions, not usage.

B -- NFR: A single negotiated flat fee, regardless of usage.

C -- TFR: Flat fee bands or tiers, independent of precise usage.

Thus, D -- MRU is correct.

EPI DCFOM-Aligned Reference Concepts (Paraphrased)

MRU charges customers based on actual measured resource consumption.

Common in modern colocations to align costs with usage.

Question 6

Question Type: MultipleChoice

The organization is implementing an information security management system (ISMS).

What is the common process model to follow?

Options:

A- SMART
B- PCI-DSS
C- ROI
D- PDCA

Answer:

D

Explanation:

The ISMS framework (aligned with ISO 27001) follows the PDCA cycle:

P -- Plan

D -- Do

C -- Check

A -- Act

This model ensures:

Continuous improvement

Systematic risk management

Documented policies and controls

Regular audits and corrective actions

Why other options are incorrect:

A -- SMART: For objective setting, not ISMS.

B -- PCI-DSS: A security compliance standard, not a process model.

C -- ROI: A financial metric, unrelated.

Thus, D is correct.

EPI DCFOM-Aligned Reference Concepts (Paraphrased)

ISMS implementation is based on PDCA methodology.

Ensures continuous improvement of security controls.

Question 7

Question Type: MultipleChoice

According to the World Economic Forum, which of the below is the largest global risk of the next decade?

Options:

A- Global climate change
B- Air quality in large cities
C- Earthquakes
D- Water scarcity

Answer:

A

Explanation:

While not strictly internal to EPI's core domain (which deals with data centre operations), this question refers to the external risk landscape, as identified by the World Economic Forum (WEF). The WEF's Global Risks Report 2025 shows that environmental risks dominate the 10-year horizon, with extreme weather, ecosystem collapse, and climate-related disruption ranking highest.

Specifically, global climate change (or extreme weather/climate-related events) is rated as the most severe risk over the next decade. While water scarcity and air quality are significant, the WEF ranks climate change / extreme weather as the top long-term threat. Therefore, option A is the most correct.

EPI DCFOM-Aligned Reference Concepts (Paraphrased)

Environmental sustainability forms a major component of data centre operations risk and resilience planning.

External macro-risks such as climate change must be integrated into facility resilience, power planning, cooling design, and business continuity strategies.

Question 8

Question Type: MultipleChoice

Customers of the data center want to know how much of the data center's power comes from renewable sources.

What should the data center service provider do to respond to these requests?

Options:

A- Request the power company to provide an estimate
B- Inform the customer that it is not possible to exactly determine how the power is generated
C- Ignore the request since the source of power generation is not part of the SLA
D- Implement the Renewable Energy Factor (REF) and report accordingly

Answer:

D

Explanation:

Within EPI's Environmental Sustainability framework, the Renewable Energy Factor (REF) is the recommended metric for determining and reporting how much of a data center's consumed power originates from renewable energy sources. REF provides a standardized, transparent, and repeatable method for calculating the renewable component of the total energy supply. This is essential because power grids draw energy from mixed sources, and data centers must demonstrate sustainability performance accurately and consistently, especially when customers demand visibility into carbon-related metrics.

Implementing REF allows the data center to quantify renewable contributions from sources such as solar, wind, hydro, geothermal, or certified renewable energy certificates. It also enables customers to compare sustainability performance across providers, improving trust and supporting corporate environmental objectives. REF becomes part of the data center's transparency strategy, demonstrating commitment to responsible energy usage and aligning with global sustainability expectations.

Options A and B are insufficient and unprofessional; energy providers may give general data, but these are not standardized for reporting purposes. Option C is inappropriate because sustainability transparency is increasingly demanded even if not in the SLA. Therefore, implementing REF is the correct and industry-aligned response.