Up-to-date Questions and Answers from authentic resources to improve knowledge and pass the exam at very first attempt. ----- Guaranteed.

CEDS MCQs
CEDS TestPrep
CEDS Study Guide
CEDS Practice Test
CEDS Actual Questions

killexams.com

ACEDS

CEDS

Certified e-Discovery Specialist (CEDS) Canada - 202

ORDER FULL VERSION

https://killexams.com/pass4sure/exam-detail/CEDS

Question: 729

During a regulatory audit, a Canadian bank must produce ESI from a legacy IBM Notes database containing 5 million emails. The regulator requests metadata fields like Sender, Recipient, and SentDate. The bank uses an e-discovery tool to process the data. Which configurations ensure metadata preservation?

A. Configure the tool to extract metadata using Lotus Notes API with parameters for Sender, Recipient, and SentDate
B. Export emails to PST format without metadata to reduce file size
C. Generate MD5 hashes for each exported file and log them in the chain of custody
D. Manually copy emails to a shared drive to preserve metadata

Answer: A,C

Explanation: Configuring the e-discovery tool to use the Lotus Notes API with specific parameters ensures metadata like Sender, Recipient, and SentDate is preserved. Generating MD5 hashes and logging them maintains data integrity and chain of custody. Exporting to PST without metadata risks losing critical information. Manual copying to a shared drive is not forensically sound and risks metadata alteration.

Question: 730

A Vancouver-based law firm is preparing a legal hold implementation plan for a client facing a regulatory investigation involving complex data sets. The client uses a hybrid IT environment with on-premises servers and cloud-based SaaS applications. Which elements must be included in the legal hold implementation plan to ensure compliance?

A. A process for suspending routine data deletion policies
B. A timeline for completing discovery without stakeholder input
C. Identification of key custodians and their data sources
D. Procedures for documenting the legal hold process

Answer: A, C, D

Explanation: A legal hold implementation plan must include suspending routine data deletion policies to prevent spoliation of relevant ESI. Identifying key custodians and their data sources ensures all relevant data is preserved. Documenting the legal hold process is essential for defensibility, demonstrating compliance with preservation obligations. A timeline without stakeholder input is impractical, as custodians and IT personnel provide critical insights into data locations and retention practices, making this option incorrect.

Question: 731

In a remote collection scenario for a Montreal-based class action lawsuit, you need to collect ESI from a custodian's home desktop without physical access. The system runs Windows 11 with BitLocker encryption. Which tools or methods ensure a forensically sound remote collection?

A. Deploy EnCase Endpoint Investigator with remote imaging capabilities over a secure VPN
B. Instruct the custodian to disable BitLocker and copy files to a shared cloud drive
C. Use a remote desktop protocol (RDP) to access the system and run a collection script
D. Verify the collection with SHA-1 and SHA-256 hash values post-transfer

Answer: A,D

Explanation: EnCase Endpoint Investigator supports forensically sound remote imaging over a secure VPN, preserving data integrity and metadata. Verifying the collection with SHA-1 and SHA-256 hashes ensures the data's authenticity and admissibility. Instructing the custodian to disable BitLocker and copy files risks altering data and metadata, violating forensic principles. Using RDP to run a collection script may not ensure forensic integrity, as it could inadvertently modify system artifacts or fail to capture unallocated space.

Question: 732

A multinational corporation is involved in a complex litigation case in Canada, requiring a document review of 2 million electronically stored documents, including emails, cloud-based collaboration data, and legacy system files. The legal team must ensure the review process is defensible and efficient. Which of the following steps are critical to establishing a robust document review process?

A. Conducting a quality control check on a statistically significant sample of reviewed documents
B. Implementing a single-pass review without iterative feedback to expedite the process
C. Using predictive coding to prioritize documents for review
D. Utilizing a manual review process exclusively to ensure accuracy

Answer: A,C

Explanation: A robust document review process in a complex litigation case requires both efficiency and defensibility. Conducting quality control checks on a statistically significant sample ensures the accuracy and consistency of the review, making the process defensible in court. Predictive coding, a form of technology-assisted review (TAR), prioritizes relevant documents, improving efficiency while maintaining accuracy, especially for large datasets. A single-pass review without iterative feedback risks missing critical documents and is not defensible for such a large volume, as it lacks validation. Similarly, relying solely on manual review is inefficient and impractical for 2 million documents, as it increases costs and time without leveraging available technology.

Question: 733

In an Edmonton-based fraud investigation, your team uses CAL with a random forest model (n_estimators=50, max_features=sqrt). The model's precision is 85%, but recall is 60%, missing key documents. Which actions should you take to improve recall?

A. Increase n_estimators to 100 to enhance model robustness
B. Incorporate reviewer feedback from 8 additional iterations
C. Switch to a logistic regression model for simpler boundaries
D. Use SMOTE to oversample relevant documents

Answer: A,B,D

Explanation: Increasing n_estimators to 100 improves the random forest's robustness, boosting recall. Adding feedback from 8 iterations enhances CAL training data, improving recall. SMOTE oversamples relevant documents, addressing class imbalance and increasing recall. Switching to logistic regression simplifies the model but may not capture complex patterns effectively.

Question: 734

A Canadian law firm is preserving ESI from a client's Dropbox account with 1 TB of data, including shared folders and version histories. The litigation hold requires preserving metadata like VersionID and SharedWith. Which steps ensure compliance?

A. Use Dropbox's Admin Console to export files with metadata in CSV format
B. Instruct users to download files manually to preserve version histories
C. Implement a litigation hold via Dropbox's API to freeze account activity
D. Log all export actions, including API calls and hash values, in the chain of custody

Answer: A,C,D

Explanation: Using Dropbox's Admin Console to export files with metadata in CSV format preserves VersionID and SharedWith fields. Implementing a litigation hold via Dropbox's API prevents data alteration, ensuring compliance. Logging export actions, including API calls and hash values, maintains a defensible chain of custody. Manual downloads by users risk metadata loss and are not forensically sound.

Question: 735

A Canadian corporation issues a legal hold notice to custodians in a trade secrets dispute. One custodian uses a personal email account for work-related communications, which is subject to a 60-day auto-deletion policy. Which actions ensure proper legal hold notification and preservation?

A. Direct the custodian to forward all relevant emails to a company email account
B. Instruct the custodian to disable the auto-deletion policy for their personal email
C. Provide a template for documenting acknowledgment of the legal hold notice

D. Require the custodian to print all relevant emails for physical storage

Answer: B,C

Explanation: The legal hold notice must ensure preservation of ESI in the custodian's personal email account. Instructing the custodian to disable the auto-deletion policy prevents loss of relevant emails. Providing a template for documenting acknowledgment ensures the custodian confirms receipt and understanding of the notice, enhancing defensibility. Forwarding emails to a company account risks altering metadata and is not a standard preservation method. Printing emails is impractical and does not preserve electronic metadata, failing to meet e-discovery standards.

Question: 736

A Canadian law firm is preparing for a U.S.-based case and must comply with preservation obligations under the U.S. Federal Rules of Civil Procedure. Which rules apply?

A. Rule 16(f) for scheduling conferences
B. Rule 26(f) for discovery planning
C. Rule 37(e) for ESI preservation
D. Rule 34 for document requests

Answer: B,C

Explanation: Rule 26(f) governs discovery planning, including preservation discussions. Rule 37(e) addresses ESI preservation and sanctions for failure. Rule 16(f) deals with scheduling violations, not preservation. Rule 34 governs document requests, not preservation obligations.

Question: 737

In Reveal, your team is designing search terms for a Canadian environmental litigation case involving 700,000 documents. Which search strategies ensure high recall?

A. Use a Boolean query: "pollution AND (chemical OR waste) NOT (draft OR internal)"
B. Implement a proximity search: "pollution W/10 regulation"
C. Apply a wildcard search: "pollut*" to capture variations like "pollution" or "polluted"
D. Run a regex search: "\b(regulation|compliance)\b.*\bpollution\b"

Answer: A,B,C,D

Explanation: A Boolean query like "pollution AND (chemical OR waste) NOT (draft OR internal)" targets relevant terms while excluding irrelevant documents, ensuring high recall. A proximity search like "pollution W/10 regulation" captures regulatory discussions, increasing inclusivity. A wildcard search like "pollut*" includes variations, boosting recall. A regex search like "\b(regulation|compliance)\b.*\bpollution\b" targets specific contexts, enhancing coverage.

Question: 738

A PIA for an e-discovery project identifies that ESI includes trade secrets shared with a third-party vendor. Which PIA components ensure compliance with PIPEDA?

A. Assess vendor compliance with SOC 2 Type II standards
B. Document data-sharing agreements
C. Implement homomorphic encryption for trade secrets
D. Evaluate data retention schedules

Answer: A,B,D

Explanation: Assessing SOC 2 Type II compliance ensures the vendor meets security standards. Documenting data-sharing agreements aligns with PIPEDA's accountability principle. Evaluating retention schedules minimizes privacy risks. Homomorphic encryption is not a standard PIA requirement.

Question: 739

During a litigation hold, a Canadian university must preserve ESI from a learning management system (LMS) like Canvas, including student submissions and metadata like SubmissionID and Timestamp. Which steps ensure compliance?

A. Use the Canvas API to export submissions with metadata in JSON format
B. Instruct instructors to download submissions manually
C. Implement a litigation hold by configuring retention policies in Canvas
D. Log the export process, including API calls and hash values, in the chain of custody

Answer: A,C,D

Explanation: Using the Canvas API to export submissions with metadata in JSON format preserves SubmissionID and Timestamp. Configuring retention policies in Canvas implements a litigation hold, preventing data loss. Logging the export process with hash values ensures a defensible chain of custody. Manual downloads by instructors risk metadata loss and are not forensically sound.

Question: 740

During ESI production in a Manitoba case, counsel inadvertently produces privileged communications. What remedies can counsel pursue to mitigate this error?

A. Assert privilege post-production under a clawback agreement
B. Destroy the inadvertently produced documents
C. Request a court order to return or destroy the documents
D. Waive privilege to avoid further disputes

Answer: A,C

Explanation: Under Canadian law, a clawback agreement (often part of a discovery plan) allows counsel to assert privilege after inadvertent production, as per Sedona Canada principles. A court order may also be sought to mandate return or destruction of privileged documents. Destroying documents unilaterally is not permissible, and waiving privilege is unnecessary if remedies exist.

Question: 741

A law firm's e-discovery platform is targeted by a brute-force attack on user accounts, risking ESI exposure. Which cybersecurity protocols should be implemented to secure the platform?

A. Deploy account lockout after 5 failed login attempts
B. Enable AES-256 encryption for ESI at rest
C. Implement CAPTCHA for login authentication
D. Conduct a Privacy Impact Assessment (PIA)

Answer: A,B,C

Explanation: Account lockout after failed attempts prevents brute-force success. AES-256 encryption secures ESI at rest. CAPTCHA adds an authentication layer to block automated attacks. A PIA assesses privacy risks but is not a direct cybersecurity protocol for immediate attack mitigation.

Question: 742

In a breach of contract case, a Canadian retailer must preserve ESI from a customer relationship management (CRM) system like HubSpot, including contact records with metadata like ContactID and LastActivityDate. Which steps ensure defensible preservation?

A. Use HubSpot's API to export records with metadata in CSV format
B. Allow sales staff to export records manually to a shared drive
C. Implement a litigation hold by configuring retention policies in HubSpot
D. Log the export process, including hash values, in the chain of custody

Answer: A,C,D

Explanation: Using HubSpot's API to export records with metadata in CSV format preserves ContactID and LastActivityDate. Configuring retention policies in HubSpot implements a litigation hold, preventing data loss. Logging the export process with hash values ensures a defensible chain of custody. Manual exports by sales staff risk metadata loss and are not forensically sound.

Question: 743

In a complex commercial litigation case in Ontario, a party requests production of all emails from a key custodian's cloud-based email account spanning 10 years, including metadata. The opposing party argues the request is overly broad under the Sedona Canada Principles. Which actions align with Principle 2 (Proportionality) to address this request?

A. Conduct a full forensic analysis of the cloud account without filtering
B. Limit the search to a 2-year period relevant to the case's key events
C. Negotiate a discovery plan specifying keyword searches and custodians
D. Produce all emails without metadata to reduce costs

Answer: B,C

Explanation: Principle 2 of the Sedona Canada Principles emphasizes proportionality, requiring discovery efforts to be reasonable relative to the case's value, complexity, and importance. Limiting the search to a relevant 2-year period aligns with proportionality by focusing on pertinent evidence. Negotiating a discovery plan with keyword searches and specific custodians ensures a tailored, cost-effective approach. A full forensic analysis without filtering is likely disproportionate due to excessive costs and irrelevance of older data. Producing emails without metadata may compromise evidentiary value, as metadata is often critical in e-discovery.

Question: 744

During a complex litigation, the e-discovery team must collaborate with external counsel using Microsoft Teams. Which security measures should be implemented?

A. Enable conditional access policies in Azure AD
B. Allow anonymous guest access to Teams channels
C. Use sensitivity labels to classify sensitive documents
D. Configure data loss prevention (DLP) policies

Answer: A,C,D

Explanation: Conditional access policies in Azure AD restrict access based on user identity and location, enhancing security. Sensitivity labels classify and protect sensitive documents, aligning with PIPEDA. DLP policies prevent unauthorized sharing of sensitive data. Anonymous guest access increases security risks and is not suitable for sensitive e-discovery collaboration.

Question: 745

Under the Hague Convention, a Canadian court seeks evidence from a French company for a civil case. Which steps are required to issue a valid Letter of Request under the Convention?

A. Include a detailed description of the evidence sought and its relevance to the case
B. Obtain pre-approval from the French Ministry of Justice
C. Translate the request into French as per Article 4 of the Convention
D. Submit the request through the Canadian Central Authority

Answer: A,C,D

Explanation: The Hague Convention (Article 3) requires a Letter of Request to specify the evidence

sought and its relevance. Translation into the language of the requested state (French, in this case) is mandatory under Article 4 unless otherwise agreed. The request must be transmitted through the Central Authority of the requesting state (Canada). Pre-approval from the French Ministry of Justice is not required, though the Central Authority in France processes the request.

Question: 746

In a PMI-based e-discovery project, the project manager must manage a budget overrun due to unexpected data volume (3TB instead of 1TB). Which actions should be taken?

A. Conduct a change control process to revise the budget
B. Negotiate with the vendor to reduce processing fees
C. Proceed without adjusting the budget or scope
D. Update the risk register to reflect data volume risks

Answer: A,B,D

Explanation: A change control process formally revises the budget to account for the increased data volume, ensuring PMI compliance. Negotiating with the vendor to reduce fees mitigates cost overruns while maintaining quality. Updating the risk register documents data volume risks, improving future planning. Proceeding without adjustments risks project failure and non-compliance with proportionality principles.

Question: 747

In a data extraction task for a Vancouver-based regulatory audit, you need to extract data from a PostgreSQL database. Which commands or tools ensure forensically sound extraction?

A. Use pg_dump with --no-owner to export the database with metadata
B. Run TRUNCATE on irrelevant tables before export
C. Use Magnet AXIOM to process the database with hash verification
D. Export tables to CSV using a GUI tool without metadata

Answer: A,C

Explanation: The pg_dump command with --no-owner exports the database with metadata, ensuring forensic soundness. Magnet AXIOM processes databases with hash verification, maintaining integrity. The TRUNCATE command risks spoliation by deleting data. Exporting to CSV without metadata fails to meet e-discovery standards for admissibility.

Question: 748

A Canadian corporation receives a subpoena from a U.S. court requesting ESI, including employee emails and financial records stored on a server in British Columbia. The data includes personal information subject to the Personal Information Protection and Electronic Documents Act (PIPEDA).

Which actions should counsel take to respond appropriately?

A. Challenge the subpoena based on Canadian data protection laws
B. Comply fully with the subpoena without reviewing for privacy compliance
C. Negotiate with the requesting party to narrow the scope of the subpoena
D. Transfer the data to a U.S. server to simplify compliance

Answer: A,C

Explanation: Under PIPEDA, personal information cannot be disclosed without consent or legal authority, and a foreign subpoena does not automatically override Canadian privacy laws. Counsel should challenge the subpoena if it conflicts with PIPEDA and negotiate to narrow its scope to minimize privacy violations while meeting legal obligations. Full compliance without review risks violating Canadian law, and transferring data to a U.S. server does not address privacy obligations and may complicate jurisdiction issues.

Question: 749

A litigation hold is issued for a Canadian company involved in a trade secrets dispute. The company's ESI includes data stored on an obsolete tape backup system deemed not reasonably accessible due to high restoration costs. Which factors should the e-discovery team consider to justify excluding this ESI from collection?

A. Availability of similar ESI from more accessible sources
B. Estimated cost and time required to restore the tape backups
C. Potential relevance of the data to the litigation
D. The company's budget constraints for e-discovery

Answer: A,B,C

Explanation: To justify excluding not reasonably accessible ESI, the team must demonstrate that the burden of restoration outweighs the data's relevance. Assessing the availability of similar ESI from more accessible sources supports proportionality under Canadian e-discovery rules. Estimating restoration costs and time provides evidence of undue burden. Evaluating potential relevance ensures compliance with disclosure obligations, as irrelevant data may be excluded. The company's budget constraints alone are not a legally valid justification for exclusion.

KILLEXAMS.COM

Killexams.com is a leading online platform specializing in high-quality certification exam preparation. Offering a robust suite of tools, including MCQs, practice tests, and advanced test engines, Killexams.com empowers candidates to excel in their certification exams. Discover the key features that make Killexams.com the go-to choice for exam success.

Exam Questions:

Killexams.com provides exam questions that are experienced in test centers. These questions are updated regularly to ensure they are up-to-date and relevant to the latest exam syllabus. By studying these questions, candidates can familiarize themselves with the content and format of the real exam.

Exam MCQs:

Killexams.com offers exam MCQs in PDF format. These questions contain a comprehensive collection of questions and answers that cover the exam topics. By using these MCQs, candidate can enhance their knowledge and improve their chances of success in the certification exam.

Practice Test:

Killexams.com provides practice test through their desktop test engine and online test engine. These practice tests simulate the real exam environment and help candidates assess their readiness for the actual exam. The practice test cover a wide range of questions and enable candidates to identify their strengths and weaknesses.

Guaranteed Success:

Killexams.com offers a success guarantee with the exam MCQs. Killexams claim that by using this materials, candidates will pass their exams on the first attempt or they will get refund for the purchase price. This guarantee provides assurance and confidence to individuals preparing for certification exam.

Updated Contents:

Killexams.com regularly updates its question bank of MCQs to ensure that they are current and reflect the latest changes in the exam syllabus. This helps candidates stay up-to-date with the exam content and increases their chances of success.