EXAMTOPICS
- Expert Verified, Online, **Free**.

CERTIFICATION TEST
- CertificationTest.net - Cheap & Quality Resources With Best Support

Question #1 *Topic 1*

Which of the following key performance indicators (KPIs) are MOST important when evaluating whether an AI model meets business objectives?

A. Cost of resources required for AI model training

B. AI model accuracy in predicting actual outcomes

C. Frequency of AI model retraining

D. Number of users interacting with the AI model

Suggested Answer: *B*

Community vote distribution

B (100%)

Lightfinger 6 months ago

Selected Answer: B

B - aligns closest to business objectives and expectations.

upvoted 3 times

Question #2 *Topic 1*

The BEST way to prevent sensitive information disclosure by large language model (LLM) chatbots is through:

A. manual monitoring.

B. data sanitization.

C. data masking.

D. access controls.

Suggested Answer: *C*

Community vote distribution

C (60%) B (40%)

Apsw2015 1 month ago

Selected Answer: C

Large Language Models (LLMs) have the capacity to memorize and unintentionally reveal sensitive information if not properly managed. As per the AAIA™ Study Guide, data masking is a critical technique that prevents the exposure of personally identifiable information (PII) or confidential content by obscuring or replacing sensitive parts of the data during training or interaction.
"Data masking ensures that training data used for LLMs does not contain real sensitive identifiers.

upvoted 1 times

RAJ56 1 month ago

Selected Answer: B

Data Sanitization involves removing Sensitive Data from Training Data

upvoted 1 times

Swallows 1 month, 1 week ago

Selected Answer: B

Masking is effective in concealing display and partial output, but since the original data itself exists, there are still risks to the model's internal processing, logging, and regeneration.

upvoted 1 times

50a3805 3 months, 3 weeks ago

Selected Answer: C

Data sanitisation refers to the permanent destruction of data

upvoted 1 times

Ssourav 4 months, 2 weeks ago

Selected Answer: B

B. Data sanitization

Reasoning:
The key risk here is that LLMs can unintentionally expose sensitive or personal data during training or responses.

Data sanitization means removing or redacting sensitive information before the data is used for training or prompts, ensuring the LLM never "sees" or stores such data.

This is a preventive control — it addresses the root cause of data leakage.

Other options:

Data masking (C) protects sensitive data in specific fields (e.g., masking credit card digits) but doesn't fully sanitize large unstructured text used for LLM training.

Access controls (D) protect who can use the model but don't stop the model from leaking data internally learned.

Manual monitoring (A) is reactive, not preventive.

upvoted 3 times

Lightfinger 6 months ago

Selected Answer: C

The listed correct answer (B. Data sanitisation) is misleading. Data sanitisation refers to the permanent destruction of data, typically for disposal. In LLM contexts, the best control to prevent sensitive information disclosure is C. Data masking, which obscures sensitive elements while preserving utility.

upvoted 3 times

Question #3 *Topic 1*

An organization is using information gathered from customer accounts to train its AI chatbot. Which of the following is the GREATEST risk associated with this practice?

A. Transparency

B. AI model hallucinations

C. AI bias

D. Disclosure of personal information

Suggested Answer: *D*

Community vote distribution

D (100%)

Ssourav 4 months, 2 weeks ago

Selected Answer: D

D. Disclosure of personal information

Explanation:
When customer-account data are used for AI training, the primary and greatest risk is that personally identifiable or confidential data could be exposed—either because the model retains sensitive details in its parameters or because those details can later surface in responses.

While transparency, bias, and hallucinations are genuine issues, they are secondary compared with the direct legal, regulatory, and ethical risk of personal-data disclosure, which can lead to privacy violations, data-protection breaches (e.g., GDPR non-compliance), and reputational damage.

upvoted 1 times

Lightfinger 6 months ago

Selected Answer: D

D - Privacy is the greatest concern here.

upvoted 1 times

Question #4 *Topic 1*

An IS auditor is evaluating an organization's incident management program to ensure it is sufficiently prepared to manage AI-related incidents. Which of the following is MOST important for the auditor to validate?

A. The program includes processes to respond to AI model drift and data integrity attacks.

B. The program prioritizes incidents based on alignment with industry leading practices.

C. The program uses past AI-related incidents and resolutions to categorize current incidents.

D. The program mandates retraining AI systems after incidents are investigated.

Suggested Answer: *A*

Community vote distribution

A (100%)

Ssourav 4 months, 2 weeks ago

Selected Answer: A

A. The program includes processes to respond to AI model drift and data integrity attacks.

Explanation:
When assessing AI-related incident management, the core objective is ensuring that the organization can detect, contain, and respond to incidents unique to AI systems.
Two of the most critical AI-specific risks are:

Model drift — when the AI model's performance degrades due to data or environment changes.

Data integrity attacks — adversarial manipulation or poisoning of training or input data.

A well-prepared incident management program must have clear response and remediation procedures for these AI-specific events, not just generic IT incidents.

Options B, C, and D are supportive or procedural but don't directly address AI-specific risk preparedness, which is what the question emphasizes.
upvoted 1 times

Lightfinger 6 months ago

Selected Answer: A

A - most important, others are important too, but come secondarily.
upvoted 1 times

Question #5 *Topic 1*

Which of the following is MOST important for an IS auditor to consider when identifying AI risk in a know your customer (KYC) application within a banking organization?

A. Business disruption and financial impact

B. Intellectual property leakage and invalidation

C. Benchmarking against peer organizations

D. Incident response plan

Suggested Answer: *A*

Community vote distribution

A (100%)

Ssourav 4 months, 2 weeks ago

Selected Answer: A

A. Business disruption and financial impact

Reasoning:
In a banking KYC environment, AI is used for identity verification, fraud detection, and compliance screening. The highest-priority risk for an IS auditor is the one that affects regulatory compliance and financial operations if the AI fails or behaves incorrectly.

If the AI system misidentifies or incorrectly blocks legitimate customers, it can directly cause business disruption, regulatory penalties, and loss of customer trust—a major financial impact.

Risks like IP leakage or benchmarking are secondary; they don't threaten immediate operational or compliance continuity.

An incident-response plan (D) is reactive, while the question asks about identifying risk, not response.

upvoted 1 times

Lightfinger 5 months, 3 weeks ago

Selected Answer: A

A is the most important.

upvoted 1 times

Question #6 *Topic 1*

A digital bank utilizes an AI system to generate credit scores. Which of the following would BEST mitigate the risk of sudden and unexplained changes in a borrower's credit score?

A. Using only data from the last six months to one year to avoid outdated information affecting the credit score

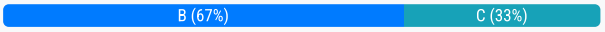
B. Ensuring the system is periodically reviewed and calibrated by human experts to maintain stability in predictions

C. Obtaining and validating the credit scores from third-party agencies to cross-check AI-generated results

D. Allowing the AI to operate fully autonomously to prevent processing delays

Suggested Answer: *B*

Community vote distribution



zxccvbnm 4 months, 3 weeks ago

Selected Answer: B

B. Having third party result to compare the result trained by own banks data will have big discrepency.

upvoted 1 times

Lightfinger 5 months, 3 weeks ago

Selected Answer: B

B - hyperparameters of the AI solution have to be periodically reviewed, and it also ticks the HitL aspect.

upvoted 1 times

Lightfinger 6 months, 1 week ago

Selected Answer: C

I think it is C - the questions ask about the BEST mitigation of risk. If we do not consider cost, C would be a better option. It is ot efficient, or cost effective, but would minimise the risk better than B.

upvoted 1 times

Question #7 *Topic 1*

Which of the following is MOST important for an IS auditor to review during an AI system audit in order to determine compliance with intellectual property and data rights?

A. Data performance metrics

B. Use of open-source intellectual property

C. Model runtime efficiency logs

D. Data usage agreements

Suggested Answer: *D*

Community vote distribution

D (100%)

zxccvbnm 4 months, 3 weeks ago

Selected Answer: D

D. Open source software dont have IP concern

upvoted 1 times

Lightfinger 5 months, 3 weeks ago

Selected Answer: D

D - data usage agreements directly addressing IP and copyright concerns.

upvoted 1 times

Lightfinger 6 months, 1 week ago

Selected Answer: D

I think it is D too. Data usage directly impacts what can be done with the data - copyright and IP.

upvoted 1 times

Question #8 *Topic 1*

Which of the following is the PRIMARY objective of AI governance?

A. Implementing compliance and ethics controls for AI initiatives

B. Promoting a positive return on investment (ROI) from AI projects

C. Defining clear roles and responsibilities for AI development, use, and oversight

D. Ensuring controls over AI are designed well and operate effectively

Suggested Answer: *C*

Community vote distribution

C (100%)

Lightfinger 6 months, 1 week ago

Selected Answer: C

C - governance is all about having clear R&R to have clear accountability for all segments for the AI Management System (AIMS)..

upvoted 1 times

Question #9 *Topic 1*

A healthcare organization uses patient data to train an AI model for early disease detection. Which of the following practices provides the BEST assurance that personal data is secure and its integrity is maintained?

A. Implementing strict data access controls and conducting security tests

B. Encrypting stored data to reduce exposure and log access

C. Updating the AI model with new data and tracking changes

D. Anonymizing patient data and performing regular quality checks

Suggested Answer: *D*

Community vote distribution

D (75%) B (25%)

Ssourav 2 months, 1 week ago

Selected Answer: D

D. Anonymizing patient data and performing regular quality checks

Anonymizing (or pseudonymizing) protects patient privacy (security/confidentiality) by removing identifiable information before using data for AI training.
Regular quality checks ensure data remains accurate, consistent, and fit for use over time — directly supports integrity.
This covers both security (via anonymization) and integrity (via quality checks) of the personal data used in training.

upvoted 1 times

zxccvbnm 4 months, 3 weeks ago

Selected Answer: D

D. A cannot prevent inference and cannot address integrity issue.

upvoted 1 times

Lightfinger 5 months, 3 weeks ago

Selected Answer: D

D - the question is about two distinct parts - "personal data is secure and its integrity is maintained". Addressing both by anonymisation and regular data quality checks.

upvoted 1 times

Lightfinger 6 months, 1 week ago

Selected Answer: B

I think it is B - the question is about integrity (data assurance). Encryption techniques would be able to protect data exposure (confidentiality) and hashes can be easily compared to ensure integrity.

upvoted 1 times

Question #10 *Topic 1*

An organization deploys an AI recruitment platform to screen job applicants. The IS auditor identifies that the platform's decisions may be influenced by model bias. Which of the following risk mitigation strategies is BEST for the auditor to recommend?

A. Implement a process to periodically test the AI system for biases and adjust parameters as needed.

B. Suspend the use of the AI system until the training data can be verified for fairness and compliance.

C. Require manual reviews of all AI-generated recruitment decisions before hiring is finalized.

D. Retrain the AI model using an external data set certified for inclusivity and fairness.

Suggested Answer: *A*

Community vote distribution

A (100%)

Lightfinger 6 months, 1 week ago

Selected Answer: A

A is the best answer. All the other would either be inappropriate, like shutting it down, it would only apply in High risk category critical system (medical) or address HitL for the process (EU AI Act) or it would not be financially sound.

upvoted 1 times

Question #11 *Topic 1*

Which of the following is MOST important to consider when deciding whether to implement an AI solution?

A. The space required for AI hardware

B. The cost of AI implementation

C. The speed of AI implementation

D. The ethical implications of AI

Suggested Answer: *D*

Community vote distribution

D (100%)

Lightfinger 6 months, 1 week ago

Selected Answer: D

D - ethic comes first here.

upvoted 1 times

Question #12 *Topic 1*

Which of the following is the PRIMARY purpose of an AI acceptable use policy?

A. Establishing guidance on the ethical use of AI

B. Explaining the distinction between different types of AI

C. Outlining AI usage monitoring procedures

D. Educating employees on where to find and how to use AI tools

Suggested Answer: *A*

Community vote distribution

A (100%)

Lightfinger 6 months, 1 week ago

Selected Answer: A

A - acceptable use documents provide information on the intended purpose of the AI model along with limitations and use cases.

upvoted 1 times

Question #13 *Topic 1*

Which of the following is the MOST important purpose of conducting a risk assessment for AI models within an organization?

A. Determining whether AI model outputs align with established use cases

B. Categorizing data used by the AI model

C. Defining mitigation strategies for AI deployment

D. Monitoring AI model performance on an ongoing basis

Suggested Answer: *C*

Currently there are no comments in this discussion, be the first to comment!

Question #14 *Topic 1*

Which of the following is the MOST important course of action for an organization prior to allowing end users to utilize an AI tool?

A. Develop an AI policy with guidelines on appropriate use.

B. Determine the impact to the disaster recovery plan (DRP).

C. Implement baseline performance metrics.

D. Ensure a cybersecurity insurance clause is in place to include the use of AI.

Suggested Answer: *A*

Currently there are no comments in this discussion, be the first to comment!

Question #15 *Topic 1*

Which of the following controls would MOST effectively mitigate worst-case service disruption scenarios affecting an AI-based application system?

A. Updating key risk indicators (KRIs) regularly

B. Implementing a kill chain process in the event of disruption

C. Performing periodic tabletop exercises

D. Including a range of AI disruption scenarios in the disaster recovery plan (DRP)

Suggested Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

Question #16 *Topic 1*

An organization uses an AI image generation platform to create promotional materials. An IS auditor identifies that the platform includes copyrighted images in its training data. Which of the following is the auditor's BEST recommendation to address this issue?

A. Suspend the use of the platform until the training data is sanitized.

B. Label all AI-generated images to disclaim the possibility of third-party content.

C. Implement a manual review process to ensure no copyrighted images are used in generated outputs.

D. Use a platform that certifies the provenance and licensing of its training data.

Suggested Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

Question #17 *Topic 1*

A bank uses a video-based know your customer (KYC) verification process. Cybercriminals exploit this process by using deepfake technology to impersonate bank customers. Which of the following countermeasures is the BEST way for the bank to mitigate this risk?

A. Discontinuing the use of the video-based verification process

B. Encrypting all customer data and communication

C. Requesting additional identity and address documents for verification

D. Leveraging AI-based liveness detection during video verification

Suggested Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

Question #18 *Topic 1*

Which of the following is an IS auditor's MOST important course of action when determining whether source data should be entered into approved generative AI tools to assist with an audit?

A. Validate that the tool is leveraging the latest model.

B. Validate that the tool provides a privacy notice.

C. Determine whether the information is reliable.

D. Determine whether any AI model hallucinations have occurred.

Suggested Answer: *C*

Currently there are no comments in this discussion, be the first to comment!

Question #19 *Topic 1*

An AI social media platform uses an algorithm to increase user engagement that could unintentionally promote divisive content. Which of the following is the BEST course of action to mitigate this risk?

A. Introduce controls allowing individuals to customize content preferences.

B. Regularly audit and adjust algorithms to reduce biases.

C. Obtain users' consent for the content they wish to view.

D. Suspend the algorithm until concerns are addressed.

Suggested Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

Question #20 *Topic 1*

Which use case for an AI model to be used by a food delivery service would pose ethical risk to the organization?

A. Using customer service metrics for service speed and food quality to predict customer retention and forecast revenue

B. Comparing total food preparation and delivery time to an industry benchmark to set key performance and risk indicators for individual restaurants

C. Basing driver retention and termination decisions on the number of delivered orders per total hours worked as compared to an industry benchmark

D. Correlating time, cost, delivery distance, and customer satisfaction metrics to issue coupons to customers receiving substandard service

Suggested Answer: *C*

Currently there are no comments in this discussion, be the first to comment!

Question #21 *Topic 1*

Which of the following BEST ensures that an AI system complies with user data ownership rights under privacy regulations?

A. Applying data clustering techniques to anonymize data sets

B. Regularly conducting AI system performance testing for accuracy

C. Implementing a transparent data consent management process

D. Enforcing strict data retention policies to limit storage duration

Suggested Answer: *C*

Currently there are no comments in this discussion, be the first to comment!

Question #22 *Topic 1*

An IS auditor is auditing an organization's data governance framework. The primary objective is to provide assurance that data management practices are standardized to support a trustworthy AI system. Which of the following should be the auditor's MOST important consideration?

A. Retention of stored data

B. Accountability for data management

C. Data practices for training models

D. Portability of data

Suggested Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

Question #23 *Topic 1*

An organization's system development process has been enhanced with AI. Which of the following features presents the GREATEST risk?

A. All codes are generated by AI without human oversight.

B. Non-technical users are validating AI results.

C. The AI personalizes applications for the user.

D. The AI allocates resources for new system development projects.

Suggested Answer: *A*

Currently there are no comments in this discussion, be the first to comment!

Question #24 *Topic 1*

A retail organization uses an AI model to analyze customers' purchase history in order to offer personalized discounts. Which of the following practices represents the MOST ethical use of customer data?

A. Retaining and analyzing all available customer data to ensure unbiased recommendations

B. Providing the public with access to review and audit the data set of collected customer information

C. Sharing customer purchase data with third-party vendors to improve advertising and communication

D. Utilizing customer purchase data only after obtaining explicit consent and allowing customers to opt out

Suggested Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

Question #25 *Topic 1*

In the context of an AI implementation, which of the following actions is MOST critical for an organization's change management program?

A. Conducting a comprehensive risk assessment specific to AI-related changes

B. Reviewing documentation for AI system changes, updates, and patches

C. Verifying that all employees have completed mandatory AI ethics training

D. Ensuring the organization has a dedicated AI governance committee

Suggested Answer: *A*

Community vote distribution

A (100%)

AliakseiB 4 months ago

Selected Answer: A

The correct answer is: ✅ A. Conducting a comprehensive risk assessment specific to AI-related changes

Explanation:

In an AI implementation, change management must go beyond traditional IT controls.
Because AI systems are dynamic, data-driven, and can evolve with retraining or tuning, changes can introduce new ethical, operational, or regulatory risks — even if the code itself doesn't change.

Therefore, the most critical action in change management is to perform a comprehensive, AI-specific risk assessment before deployment or modification.

This ensures the organization:

Understands the impact of model updates (e.g., retraining, new data sources),

Evaluates bias, accuracy, explainability, and compliance risks,

Maintains traceability and accountability for every AI-related change

upvoted 1 times

Question #26 *Topic 1*

During a pre-implementation risk assessment, an AI model is determined to present a significant risk of bias and potential harm in excess of the organization's risk tolerance. Which of the following is the MOST appropriate response?

A. Obtain board approval for an exception.

B. Enhance the data that the model is trained on.

C. Revisit the risk tolerance to ensure it is appropriate.

D. Postpone deployment until the risk can be safely managed.

Suggested Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

Question #27 *Topic 1*

An organization is adopting AI for its procurement and inventory teams, raising concern from stakeholders that they will lose their jobs due to AI. Which of the following is the BEST way for the IS auditor to assess whether the potential negative impacts were minimized?

A. Review human-centered design practices to determine how they were considered.

B. Review how the project management team collected feedback in engagement activities.

C. Review the current state assessment of how AI may impact the organization.

D. Review the AI roadmap for short-term and long-term milestones.

Suggested Answer: *A*

Swallows 4 weeks ago

Selected Answer: C

Specifically, this means:
Workforce Impact Analysis
Employment Risk Assessment
Relocation Plan
Skills Transition Plan
Quantitative Risk Analysis
Confirm the following.
The most important thing in an audit is:
Is there an empirical impact assessment?
Therefore, C.

upvoted 1 times

Question #28 *Topic 1*

A healthcare organization uses data clustering to group patients by medical history for personalized treatment recommendations. Which of the following is the GREATEST privacy risk associated with this practice?

A. Clustering increases the complexity of the model, making data harder to anonymize.

B. The clustering requires more data, increasing the risk of a privacy breach.

C. Irrelevant features in the data may result in inaccurate or biased treatments.

D. Clusters can reveal sensitive personal information depending on how the information is presented.

Suggested Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

Question #29 *Topic 1*

Which of the following is the GREATEST risk associated with using AI in audit planning?

A. Scope creep

B. Limited knowledge

C. Increased planning costs

D. Incomplete data

Suggested Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

Question #30 *Topic 1*

When using off-the-shelf AI models, which of the following is the MOST appropriate way for organizations to approach vendor management?

A. Establish responsibility and clear terms for model updates and support.

B. Only use models from vendors with globally recognized accreditation.

C. Use the vendor only if the contract has been reviewed by the information security department.

D. Ensure a minimum of three quotes have been obtained for market research and comparison.

Suggested Answer: *A*

Currently there are no comments in this discussion, be the first to comment!

Question #31 *Topic 1*

Which of the following metrics are the BEST indication of a mature and effective approach to an organization's data governance program for its AI systems?

A. Total budget allocated to AI initiatives across all departments

B. Number of AI projects completed within the last fiscal year

C. Percentage of AI models with documented data lineage

D. Frequency of data quality audits on the organization's data sets

Suggested Answer: *C*

Currently there are no comments in this discussion, be the first to comment!

Question #32 *Topic 1*

Which of the following is the BEST way to support the development and design of high-risk AI systems?

A. Conduct regular training sessions for users on data privacy.

B. Ensure the availability of trustworthy data sets.

C. Regularly back up the AI system's data to a secure, offsite location.

D. Implement multi-factor authentication (MFA) for all users accessing the AI system.

Suggested Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

Question #33 *Topic 1*

An organization shares an AI model with external partners. One partner reports that sensitive data has been inadvertently exposed through the model's outputs. Which of the following is the IS auditor's BEST recommendation?

A. Retrain the model immediately and implement privacy-preserving techniques.

B. Disable the shared model and notify partners of the potential breach.

C. Limit the model's outputs to anonymized results while investigating further.

D. Audit the data pipelines of all partners to identify the source of the leak.

Suggested Answer: *A*

Community vote distribution

B (100%)

Swallows 1 month, 1 week ago

Selected Answer: C

While option B is highly appropriate from an incident response standpoint, it does not reflect an auditor's perspective.

upvoted 1 times

KAP2HURUF 3 months, 2 weeks ago

Selected Answer: B

Containtment first

upvoted 2 times

Question #34 *Topic 1*

Which of the following controls helps mitigate the risk of competitors poisoning data utilized by a machine learning (ML) model performing sentiment analysis of product reviews?

A. Peer reviewing code that acquires product reviews from social media posts

B. Hiring a marketing firm to text links to customers requesting product reviews for monetary compensation

C. Requiring customers to authenticate access to their accounts prior to writing product reviews

D. Augmenting the unbalanced product review data set with the use of oversampling by the model developer

Suggested Answer: *C*

Currently there are no comments in this discussion, be the first to comment!

Question #35 *Topic 1*

The PRIMARY purpose of maintaining an audit trail in AI systems is to:

A. facilitate transparency and traceability of decisions.

B. analyze model accuracy and fairness.

C. ensure compliance with regulatory standards for AI.

D. measure computational efficiency.

Suggested Answer: *A*

Currently there are no comments in this discussion, be the first to comment!

Question #36 *Topic 1*

Which of the following is MOST important to review in order to gain assurance that an AI model is performing without biases?

A. AI model temperature

B. AI development environment

C. AI training data

D. AI model adaptability

Suggested Answer: *C*

Currently there are no comments in this discussion, be the first to comment!

Question #37 *Topic 1*

Which of the following is the MOST important risk for an IS auditor to consider when reviewing the adoption of an AI system?

A. Immaturity of AI systems in the industry

B. Resistance to the use of AI technology

C. Costs associated with AI system maintenance

D. Bias in AI system decision making

Suggested Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

Question #38 *Topic 1*

During an audit of an investment organization's AI-powered software, an IS auditor identifies a potential security risk. What is the GREATEST risk associated with staff exfiltrating organizational data to a generative AI tool?

A. Excessive reliance on AI-generated insights

B. Unauthorized data disclosure

C. Potential business disruptions

D. Data contamination due to biased AI model outputs

Suggested Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

Question #39 *Topic 1*

Which of the following will provide the BEST evidence to support the alignment of an AI model with an organization's business objectives?

A. AI change management requests

B. AI model vulnerability assessment

C. AI acceptable use policy

D. AI model inventory

Suggested Answer: *D*

Community vote distribution

A (100%)

Swallows 1 month, 1 week ago

Selected Answer: C

Evidence of alignment means an official document that clearly states the purpose.
Therefore, the best evidence supporting alignment between AI models and the organization's business objectives is option C."

upvoted 1 times

lingtianx1127 1 month, 2 weeks ago

Selected Answer: D

I belive the answer D is correct. you need to know what "AI" models or technology you are currently using before you can start planning for the audit of AI.

upvoted 1 times

JanBas 2 months, 1 week ago

Selected Answer: A

Can it b A, as change requests would record the business justification for the change?

upvoted 1 times

Question #40 *Topic 1*

An organization uses third-party licensed data for training its AI models. During an audit, it is discovered that data usage restrictions were violated. Which of the following is the IS auditor's MOST appropriate recommendation?

A. Review all organizational data agreements.

B. Discontinue use of the AI model training data.

C. Strengthen system development life cycle (SDLC) controls.

D. Implement stronger data clustering techniques.

Suggested Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

Question #41 *Topic 1*

Which of the following is the MOST significant risk associated with a deep learning system algorithm being updated as it learns?

A. System algorithms can easily be modified by attackers because the algorithms reside in system memory.

B. Project stakeholders may not endorse the system because its behavior may be contrary to their expectations.

C. Operational risk may increase because the system is continuously running.

D. The system may generate discriminatory output because of biases in training data.

Suggested Answer: *D*

Swallows 1 month ago

Selected Answer: B

The biggest risk is not the technology itself, but the breakdown of acceptance and governance

upvoted 1 times

Question #42 *Topic 1*

When assessing the potential risk of implementing an AI system, it is MOST important to validate the model's:

A. processing speed and computational efficiency,

B. decision-making explanations and interpretability of its outputs,

C. number of parameters and its overall complexity,

D. compatibility with existing legacy software used by the organization.

Suggested Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

Question #43 *Topic 1*

An organization uses an AI video generation platform to create videos for public audiences. An IS auditor notes that there are no clear governance policies defining how viewers should be informed that content is generated by AI. Which of the following recommendations would BEST ensure the ethical use of AI within this platform?

A. Establish a policy requiring all AI-generated content to be labeled as such for transparency.

B. Improve the production quality of AI-generated content to match industry standards.

C. Conduct regular content accuracy checks to ensure AI-generated videos meet quality expectations.

D. Limit access to the video generation platform to approved users within the organization.

Suggested Answer: *A*

Currently there are no comments in this discussion, be the first to comment!

Question #44 *Topic 1*

Which of the following would be of GREATEST concern to an IS auditor reviewing an organization's AI policies and procedures?

A. The documentation of AI models does not address business resiliency and disaster recovery.

B. The AI model does not have an approval process for production changes.

C. External validation is not required for AI systems before deployment.

D. The data privacy policy has not been reviewed in the past three years.

Suggested Answer: *C*

Community vote distribution

B (100%)

lingtianx1127 1 month, 2 weeks ago

Selected Answer: B

B should be the answer becasue unauthorized change to AI model would post greatest ethical and financial risk to the company

upvoted 1 times

Ssourav 2 months, 1 week ago

Selected Answer: B

Why B is the GREATEST concern:

Without an approval process for production changes, there's no control over how models are updated, retrained, or deployed. This can lead to:

Unauthorized or untested changes going live

Loss of model integrity and performance

Inability to trace or rollback problematic updates

Violation of regulatory requirements for change management

This is a foundational IT governance failure (akin to lack of change control in traditional IT systems) and would be a top audit finding.

upvoted 1 times

Question #45 *Topic 1*

An IS auditor is participating in a task force to select an AI solution vendor. The vendor states that their product is only functional with web integration activated. Which of the following is the GREATEST concern?

A. AI training model environment

B. Inappropriate algorithms used by the vendor

C. Data hallucinations and biases

D. Impacts on employee and contractor workforces

Suggested Answer: *A*

Community vote distribution

A (100%)

AliakseiB 4 months ago

Selected Answer: A

The correct answer is: ✅ A. AI training model environment

Explanation:

If the vendor's AI solution requires web integration to function, this means the system may:

Connect to external data sources or cloud-based APIs, and

Potentially transmit internal or sensitive data outside the organization's controlled environment.

This introduces the greatest risk to the AI training and operational environment, as it could expose proprietary or confidential data to:

Unauthorized access,

Data leakage, or

Unintended use in external AI model training.

Thus, the IS auditor's primary concern should be around data protection, privacy, and environment isolation — not the algorithms or workforce impacts.

upvoted 1 times

Question #46 *Topic 1*

In order to ensure effective alignment with organizational priorities, which of the following is MOST important for an IS auditor to address when developing an audit plan for an AI-based tool?

A. Cost-benefit strategy for AI adoption

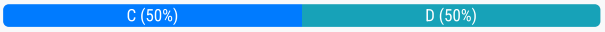
B. AI users' understanding of ethical standards

C. The AI tool's security alignment with governance policies

D. Management practices for AI oversight

Suggested Answer: *D*

Community vote distribution



Swallows 1 month ago

Selected Answer: D

The first thing IS auditors should consider when formulating a plan is how to continuously monitor and control the AI.

upvoted 1 times

Ssourav 2 months, 1 week ago

Selected Answer: D

Why D is MOST important:

Without proper management oversight, even a well-designed AI tool can drift from organizational priorities, introduce unmanaged risks, or fail to deliver expected value. Oversight ties the AI system into the organization's governance framework — a key audit focus.

upvoted 1 times

KAP2HURUF 3 months, 1 week ago

Selected Answer: C

D. Management practices for AI oversight

Oversight is important, but without security alignment, even strong management practices cannot mitigate fundamental risks.

upvoted 2 times

Question #47 *Topic 1*

An IS auditor is evaluating an organization's AI-based hiring tool. The tool excludes candidates from postal codes correlating with specific demographic groups, despite not explicitly using race or ethnicity as input variables. Which of the following is the auditor's BEST course of action?

A. Assess proxy variables within the AI model that may correlate with sensitive attributes.

B. Advise the company to collect explicit demographic data to directly control for bias.

C. Recommend removing all geographic data from the AI model training to ensure fairness.

D. Suggest deploying a different AI model that does not consider any personal data.

Suggested Answer: *A*

Currently there are no comments in this discussion, be the first to comment!

Question #48 *Topic 1*

An IS auditor is utilizing an AI chat tool to assist with grammar and improve the overall readability of a report they are writing. Which of the following is the MOST significant risk the auditor should consider when using this AI tool?

A. The AI tool may alter the intended meaning of the content, leading to misinterpretation of the report.

B. The auditor may become overly reliant on the AI tool, compromising their own writing skills.

C. The AI tool may introduce new grammatical errors that were not present in the original text.

D. The use of the AI tool may increase the risk of intellectual property violations.

Suggested Answer: *A*

Currently there are no comments in this discussion, be the first to comment!

Question #49 *Topic 1*

Which of the following is MOST important to have in place before implementing a system that utilizes AI?

A. Training on the use of the system's AI capabilities

B. An AI acceptable use policy

C. Model evaluation and validation methodology

D. A project plan for deploying the AI system

Suggested Answer: *C*

Currently there are no comments in this discussion, be the first to comment!

Question #50 *Topic 1*

A car insurance company uses an AI model to determine customer premiums. To ensure the ethical use of this model, which of the following testing practices should the company consider to be MOST important?

A. Running model performance tests on randomized data to improve the model's accuracy

B. Ensuring demographic data is not used to train models outside of the defined use case

C. Testing to ensure the model's predictions do not discriminate based on age or gender

D. Deploying the model only for a small randomly selected group of existing customers

Suggested Answer: *C*

Community vote distribution

C (100%)

Swallows 4 weeks, 1 day ago

Selected Answer: C

In practice, this would look like this:
Using Age and Sex is legal → OK
However, testing to ensure that their impact is in line with laws, regulations, and internal policies → required
For example:
Are the insurance premiums for 20-year-olds and 21-year-olds not too different?
Are there any unintended biases in the data structure?
Even if gender is not used directly, are proxy variables (such as car type or place of employment) acting as a substitute for gender?
Fairness testing is necessary to identify these issues.
upvoted 1 times

AliakseiB 4 months ago

Selected Answer: C

The correct answer is: ✅ C. Testing to ensure the model's predictions do not discriminate based on age or gender

Explanation:

In an AI-based insurance pricing model, the most critical ethical concern is algorithmic fairness — ensuring that the model's predictions do not discriminate against protected groups (e.g., by age, gender, race, or location).

Testing for bias and discrimination ensures that:

The model complies with ethical AI principles and anti-discrimination regulations.

Premiums are determined based on legitimate risk factors rather than demographic proxies.

The organization maintains transparency, accountability, and public trust in its AI systems.

This type of testing is a key part of AI fairness and ethics auditing.
upvoted 2 times

Question #51 *Topic 1*

A financial services company is developing AI models to predict customer credit risk. To reduce privacy concerns, the company decides to train the models primarily using synthetic data. Which of the following is an IS auditor's BEST recommendation to evaluate synthetic data risk?

A. Discontinue the use of synthetic data for model training.

B. Conduct cluster analysis using synthetic data.

C. Require validation of synthetic data quality.

D. Perform regression testing using synthetic data.

Suggested Answer: *C*

Currently there are no comments in this discussion, be the first to comment!

Question #52 *Topic 1*

It was determined that an AI system used for medical diagnoses shows decreased accuracy for minority populations. Which of the following is the BEST way to address this issue?

A. Retrain the model with more representative data.

B. Transition to exclusively using synthetic data generation.

C. Optimize model hyperparameters for better performance.

D. Apply anonymization techniques to the training data.

Suggested Answer: *A*

Currently there are no comments in this discussion, be the first to comment!

Question #53 *Topic 1*

An IS auditor has identified that the configuration of a proprietary AI model has been leaked. Which of the following is the MOST significant risk?

A. Attackers can disable security systems by analyzing the model's source code.

B. Attackers can use the data to degrade the model's performance.

C. Attackers can train their own improved model for legitimate use.

D. Attackers can exploit vulnerabilities in the model.

Suggested Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

Question #54 *Topic 1*

An AI generated photo showing a catastrophe circulated on social media, impacting the supply chain. This is an example of which type of risk?

A. Compliance risk

B. Societal risk

C. Economic risk

D. Data privacy risk

Suggested Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

Question #55 *Topic 1*

Which of the following processes is MOST important for an organization to have in place to ensure the credibility of AI outputs?

A. User consent

B. Model alignment

C. Data governance

D. Data analytics

Suggested Answer: *C*

Swallows 4 weeks ago

Selected Answer: B

The answer is not D, but B for the following reasons. Please delete my original answer, as it has not yet been approved.

The process by which a model is adjusted to produce output that is consistent with the organization's objectives and rules.

→ This directly ensures reliability.

upvoted 1 times

Swallows 4 weeks, 1 day ago

Selected Answer: D

Data analysis verifies the following aspects of AI output:

Accuracy

Consistency

Outlier detection

Model performance evaluation

Bias detection

Output validity testing

In other words, this is the process of directly verifying whether AI output is trustworthy.

To ensure the reliability of output,

data analysis is the most practically necessary process.

upvoted 1 times

Question #56 *Topic 1*

When reviewing an organization's AI data governance program, which of the following is MOST important to validate to ensure compliance with privacy regulations?

A. Implementation of privacy techniques in AI models

B. Security of private cloud deployment of AI models

C. Feasibility of AI model retraining to incorporate new privacy data

D. Avoidance of AI models that are based on open-source algorithms

Suggested Answer: *A*

Currently there are no comments in this discussion, be the first to comment!

Question #57 *Topic 1*

An organization passes transaction data to an AI system so it can produce recommendations for customers. Which of the following is MOST important for management to do to keep this reliable?

A. Be aware of the social influences of the AI-based services they provide.

B. Obtain independent certification on strategies for business resilience.

C. Have insurance coverage to compensate for AI-related litigations.

D. Ensure risk mitigation scenarios reduce exposures to a tolerable range.

Suggested Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

Question #58 *Topic 1*

A banking organization uses AI to support the credit scoring process. Which of the following is the GREATEST benefit of providing interpretations of AI model outputs?

A. It ensures the outputs align with the organization's internal ethical standards.

B. It helps auditors identify areas where the AI model may require retraining.

C. It allows stakeholders to understand the reasons behind the outputs.

D. It reduces the need for human oversight in the loan approval process.

Suggested Answer: *C*

Currently there are no comments in this discussion, be the first to comment!

Question #59 *Topic 1*

When evaluating an AI system used to approve loan applications, an IS auditor notes decisions are made by the AI tool without oversight. Which of the following is the auditor's BEST recommendation?

A. Establish early human review checkpoints to detect errors or biases in AI decisions.

B. Allow human review only when customers appeal decisions.

C. Perform cross-validation before model deployment to production.

D. Accept the outputs of the AI tool as valid if technical validation was previously conducted.

Suggested Answer: *A*

Currently there are no comments in this discussion, be the first to comment!

Question #60 *Topic 1*

When evaluating whether an AI algorithm deployed by an organization aligns with its business objectives, it is MOST important to:

A. review algorithm documentation for completeness.

B. confirm the outcomes from using the algorithm support strategic goals.

C. validate that data sources are identified in the business strategy.

D. verify the algorithm's ability to process transactions accurately.

Suggested Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

Question #61 *Topic 1*

An organization uses an AI-based chatbot that collects customer data during interactions. Which of the following is MOST important to ensure compliance with data consent requirements?

A. Obtaining consent each time queries are processed by the chatbot

B. Deleting data immediately following customer interactions with the chatbot

C. Anonymizing user interaction data after three months

D. Embedding a consent mechanism that provides clear options before data collection begins

Suggested Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

Question #62 *Topic 1*

A large organization is implementing a new AI system that uses customer data. Which of the following is the BEST approach for risk mitigation to protect customer privacy?

A. Implement a mechanism for customers to opt out of the use of their data.

B. Assign sole responsibility for risk mitigation to the development team.

C. Implement data anonymization and impact assessments.

D. Conduct periodic risk and vulnerability assessments.

Suggested Answer: *C*

Swallows 4 weeks, 1 day ago

Selected Answer: C

Opt-outs are only effective if customers take action.
However, many customers are unaware of the opt-out feature, don't understand how it works, or find it inconvenient.
This leaves them open to potential risks.

upvoted 1 times

Question #63 *Topic 1*

An IS auditor learns that the organization's AI solution is configured with web integration enabled. Which of the following is the MOST important control for the auditor to validate?

A. Data augmentation activities prior to model building

B. Key performance indicator (KPI) metrics for model inference time

C. Activity logging with integration to the organization's SIEM system

D. Separation of duties between the model creator and the model tester

Suggested Answer: *C*

Swallows 4 weeks, 1 day ago

Selected Answer: A

Data imported from the web poses a higher risk of contamination than internal data, making it more susceptible to serious AI security risks such as data poisoning attacks, bias injection, and the inclusion of fraudulent data.

For this reason, data augmentation activities (data security checks and cleansing) before model building can be considered the most important control.

upvoted 1 times

Question #64 *Topic 1*

Which of the following is the GREATEST risk resulting from excessive agency in AI systems?

A. Inefficient prioritization of tasks

B. Uncontrolled access and unauthorized actions

C. Slower AI system responses and performance

D. Increased need for oversight of model actions

Suggested Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

Question #65 *Topic 1*

During an audit of an organization that has adopted AI, it was discovered that data ownership responsibilities were not clearly defined. Which of the following is the MOST likely consequence of this gap?

A. Higher operational costs for managing data storage solutions

B. Reduced organizational reliance on AI solutions

C. Decreased performance of AI models due to redundant data ownership

D. Increased risk of data breaches due to lack of accountability

Suggested Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

Question #66 *Topic 1*

Which of the following should be the PRIMARY consideration when establishing an accountability structure for AI governance?

A. Ensuring AI systems are used ethically and responsibly

B. Minimizing financial risk associated with AI implementation

C. Maximizing the efficiency and productivity gains from AI technologies

D. Protecting the intellectual property rights of AI developers

Suggested Answer: *A*

Currently there are no comments in this discussion, be the first to comment!

Question #67 *Topic 1*

Which of the following is the GREATEST risk associated with using facial recognition authentication for opening bank accounts?

A. Inconsistent image quality across devices can reduce the accuracy of identity verification algorithms.

B. AI-generated deepfake or synthetic images can fool the authentication system.

C. Authentication may fail if the user is wearing sunglasses or a mask.

D. The system may incorrectly reject valid facial images due to strict thresholds.

Suggested Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

Question #68 *Topic 1*

Which of the following is MOST important for an IS auditor to assess when reviewing logs of prompts and corresponding AI responses?

A. Employee use of the AI model outside of business hours

B. Disclosure of confidential information in response to queries

C. Volume of storage utilized and length of retention periods

D. Inadequate AI model training prior to being migrated to production

Suggested Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

Question #69 *Topic 1*

Which of the following is the MOST important to ensure an organization's management is fulfilling ethical responsibilities related to AI?

A. Ensure human rights are protected from the potential negative impacts of AI.

B. Ensure risk assessments are performed to identify regulatory risks.

C. Model future changes in personal and social behavior where AI may play a pivotal role.

D. Design international ethics standards to be observed by the organization.

Suggested Answer: *A*

Currently there are no comments in this discussion, be the first to comment!

Question #70 *Topic 1*

A company is developing an AI system to generate videos and images. Which of the following would BEST enable the company to mitigate harm caused by deepfakes?

A. Differential privacy

B. Watermarking

C. Sanitization

D. Model encryption

Suggested Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

Question #71 *Topic 1*

An audit reveals inconsistencies in the retention period of data used for AI training. What is the BEST recommendation to mitigate this risk?

A. Enhance licensing agreements to include retention clauses.

B. Establish a dedicated data clustering team for ongoing oversight.

C. Implement automated data cleansing tools to enforce retention policies.

D. Assign data ownership roles to the AI model development team.

Suggested Answer: *C*

Currently there are no comments in this discussion, be the first to comment!

Question #72 *Topic 1*

An IS auditor reviewing an AI-based data governance program discovers that there is no formal data classification policy in place. Which of the following is the MOST likely consequence of this gap?

A. Inappropriate handling of sensitive data during AI model training

B. Delayed AI model deployment due to data inefficiencies

C. Reduced data cleansing accuracy due to lack of categorization

D. Unauthorized data sharing with contractors

Suggested Answer: *A*

Currently there are no comments in this discussion, be the first to comment!

Question #73 *Topic 1*

To ensure stakeholders are adequately prepared to address workforce impacts, which of the following is an IS auditor's BEST recommendation for an organization's AI incident response plan?

A. Review the frequency of AI security incidents and updates to the response plan.

B. Verify that the organization has an AI ethics committee to discuss potential workforce impacts.

C. Validate that regular cross-functional AI incident drills and skill gap assessments are performed.

D. Confirm that all employees have completed a standardized online AI awareness course within the last year.

Suggested Answer: *C*

Currently there are no comments in this discussion, be the first to comment!

Question #74 *Topic 1*

An organization seeks to sustain effective AI governance and risk management amid rapidly evolving AI technologies.

Which of the following represents the MOST effective course of action?

A. Provide role-specific AI training to technical staff.

B. Outsource AI training to external vendors.

C. Conduct comprehensive AI training for senior management.

D. Integrate continuous AI training into security awareness programs

Suggested Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

Question #75 *Topic 1*

An AI tool is being implemented for a regional healthcare organization. Which of the following training methods BEST ensures the AI output does not reveal whether someone's personal data was used?

A. Supervised learning with labeled patient records

B. Data augmentation during training to improve privacy

C. Differential privacy applied during model training

D. Transfer learning using public health data sets

Suggested Answer: *C*

Community vote distribution

C (100%)

Swallows 4 weeks ago

Selected Answer: C

Even if an external attacker were to query the model...
"Was this patient's data used?"
"Can we generate this individual's information?"
"Perform a membership inference attack."
To prevent such attacks,
Differential Privacy add noise to the training process to disperse information and prevent them from determining whether personal data was used.

upvoted 1 times

Question #76 *Topic 1*

An organization has deployed a generative AI system for customer support that includes frequent updates to the AI model after deployment. Which of the following represents the GREATEST risk?

A. Lack of a change management policy specific to AI

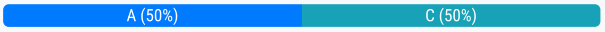
B. Overreliance on manual review of AI model outputs

C. Lack of continuous monitoring for model changes

D. Lack of a dedicated AI governance committee

Suggested Answer: *C*

Community vote distribution



Swallows 4 weeks ago

Selected Answer: A

From the perspective of prioritizing root cause risks, A is the correct answer.
C should be considered a secondary risk.

upvoted 1 times

RAJ56 1 month ago

Selected Answer: C

The greatest risk is that frequent AI model updates occur without robust governance, resulting in unvalidated behavior changes that impact accuracy, compliance, and customer outcomes.

upvoted 1 times

Question #77 *Topic 1*

An organization is developing an AI system that integrates data from multiple external sources without clearly defined data ownership policies. Which of the following is the GREATEST concern in this situation?

A. Deficiencies in policies and procedures validating AI model accuracy

B. Limited documentation of user access permissions

C. Excessive dependence on automated data collection and cleansing

D. Gaps in AI privacy compliance and accountability

Suggested Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

Question #78 *Topic 1*

An organization is using a large language model (LLM) to assist in evaluating loan applications, but the training data used is known to be incomplete. Which of the following is the GREATEST associated risk?

A. Unfair loan decisions

B. Delays in loan approval

C. Reduced customer satisfaction

D. Increased manual processing of applications

Suggested Answer: *A*

Currently there are no comments in this discussion, be the first to comment!

Question #79 *Topic 1*

Which of the following is the MOST important reason to establish AI governance structures that extend beyond regulatory compliance?

A. To align with global AI data privacy standards

B. To mitigate reputational risk associated with public scrutiny of AI systems

C. To ensure ethical integrity throughout the AI life cycle

D. To establish guardrails limiting AI system functionality to approved use cases

Suggested Answer: *C*

Currently there are no comments in this discussion, be the first to comment!

Question #80 *Topic 1*

Which of the following should be an IS auditor's GREATEST concern when reviewing an anomaly detection process implemented for a high-risk AI system?

A. Failure to identify anomalies that can bias training data

B. Lack of regular quality reviews for training data

C. Infrequent updates to anomaly detection algorithms

D. Inadequate staff training on the use of the system

Suggested Answer: *A*

Currently there are no comments in this discussion, be the first to comment!

Question #81 *Topic 1*

An IS auditor is evaluating an organization's data governance controls for its AI system. Which of the following represents the GREATEST risk in this context?

A. Inconsistent data management practices

B. Lack of procedures for automated data backup

C. Limited frequency of AI system performance and data accuracy reviews

D. Inadequate controls over data accuracy and privacy compliance

Suggested Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

Question #82 *Topic 1*

Which of the following is the GREATEST risk of using AI to generate audit reports?

A. The AI system uses inconsistent formatting across audit reports.

B. The AI system misrepresents control effectiveness.

C. The AI system cannot integrate with management dashboard tools.

D. The AI system is not able to include historical audit findings.

Suggested Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

Question #83 *Topic 1*

Which of the following should be an IS auditor's GREATEST concern if class imbalance is identified in training data for an AI model?

A. Data drift

B. Data quality

C. Model bias

D. Model overfitting

Suggested Answer: *C*

Community vote distribution

C (100%)

Swallows 4 weeks ago

Selected Answer: C

The model is strongly optimized for the majority class and cannot accurately judge the minority class.

This leads to model bias.

Misclassification occurs frequently for certain users and cases.

High-risk AI directly affects safety and fairness.

upvoted 1 times

Question #84 *Topic 1*

A healthcare AI tool used by a hospital recommends treatments based on patient data. The tool sometimes suggests treatments that have high success rates but significant risk. The hospital's risk management approach prioritizes patient safety over innovative solutions. Which of the following is the hospital's BEST course of action?

A. Adjust the AI's parameters to align with the hospital's risk tolerance.

B. Discontinue using the AI tool and rely solely on doctor expertise.

C. Obtain patients' consent for the use of their data by the AI tool.

D. Use the AI tool only for low-risk situations.

Suggested Answer: *A*

Currently there are no comments in this discussion, be the first to comment!

Question #85 *Topic 1*

An AI audit reveals that a loan approval model has a significantly higher rejection rate for applicants from a specific demographic group. Which of the following should be management's PRIMARY response?

A. Accept the audit findings as within risk tolerance.

B. Determine if audit sampling is sufficient.

C. Conduct comprehensive bias analysis.

D. Synthesize more data of the affected demographic group.

Suggested Answer: *C*

Currently there are no comments in this discussion, be the first to comment!

Question #86 *Topic 1*

Which of the following provides the BEST evidence that an organization's AI integration is aligned with its overall technology strategy?

A. Key performance indicators (KPIs) have been defined for AI systems.

B. The organization has developed and socialized AI use policies.

C. Management promotes a culture of innovation.

D. The IT department includes many individual contributors with AI expertise.

Suggested Answer: *A*

Currently there are no comments in this discussion, be the first to comment!

Question #87 *Topic 1*

An organization has deployed an AI-powered customer service chatbot trained using customer chat logs. When reviewing AI risk assessment documentation, which of the following should be the IS auditor's GREATEST concern?

A. Limited AI model capability to incorporate and adapt to new data

B. Obsolete procedures leading to inadequate data integrity validation

C. Reputational impacts resulting from inaccurate chatbot responses

D. Insufficient access controls leading to unauthorized customer data exposure

Suggested Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

Question #88 *Topic 1*

Which of the following is the GREATEST risk associated with deploying an AI system with ineffective anomaly detection?

A. Inconsistent AI system configuration management

B. Undetected data poisoning that impacts AI decision quality

C. Delayed incident response to AI model drift

D. Failure to comply with AI reporting standards

Suggested Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

Question #89 *Topic 1*

An IS auditor is considering using a web-based AI tool to update an audit report. What should be the MOST important consideration before inputting the report?

A. The AI tool alignment with organizational report formatting

B. Safeguard measures of the AI tool

C. Impact on the audit budget

D. Compliance with organizational data protection requirements

Suggested Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

Question #90 *Topic 1*

When an IS auditor uses generative AI with external retrieval-augmented generation (RAG) to gather evidence during an audit, which of the following poses the GREATEST data security risk?

A. Sensitive internal context may be included in queries sent to external services.

B. Personal information may be shared based on model training data.

C. External search engines only respond to public data.

D. The model might fail to retrieve data from the vector.

Suggested Answer: *A*

Currently there are no comments in this discussion, be the first to comment!

Question #91 *Topic 1*

Which of the following insider threats involving the use of AI would present the GREATEST risk?

A. Leaking of system hyperparameters

B. Launching social engineering attacks

C. Destroying system backups

D. Exfiltrating sensitive data

Suggested Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

Question #92 *Topic 1*

Which of the following is the BEST recommendation to mitigate excessive agency when implementing an AI system as a browser extension?

A. Minimize browser extension functionality.

B. Remove user access to browser extensions.

C. Maximize browser extension functionality.

D. Use open source browser extensions.

Suggested Answer: *A*

Currently there are no comments in this discussion, be the first to comment!

Question #93 *Topic 1*

An organization is reviewing its existing data governance framework after implementing an AI-based document repository solution. Which of the following should be the PRIMARY consideration for the organization?

A. Data retention policy

B. Data classification

C. Data enrichment

D. Qualitative data collection

Suggested Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

Question #94 *Topic 1*

An IS auditor is reviewing change documentation of an AI model. Which of the following would pose the GREATEST risk?

A. Management has not tested the model.

B. Test results are not in a standardized format.

C. There is a low number of test scenarios.

D. The seed used for testing is not documented.

Suggested Answer: *C*

Community vote distribution

A (100%)

Swallows 3 weeks, 5 days ago

Selected Answer: C

When auditing changes to AI models,
it's most important to ensure that the modified model is thoroughly tested and free of unintended behavior or errors.
With fewer test scenarios:
Critical defects may go undetected.
Increased likelihood of malfunction under specific conditions.
Overlooking bias or edge cases.
Significantly increased risk to production.
Since AI models have a high degree of input diversity,
a lack of scenarios poses a critical quality risk.

upvoted 1 times

RAJ56 1 month, 2 weeks ago

Selected Answer: A

Greatest Risk is lack of testing for a change in Model (AI or otherwise).

upvoted 1 times

Question #95 *Topic 1*

What is the MOST important reason government organizations should provide regular AI training programs for all staff?

A. To minimize the cost of AI deployment

B. To ensure staff are up to date on ethical considerations

C. To allow staff to understand the tools available

D. To reduce learning using outdated information

Suggested Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

Question #96 *Topic 1*

Which of the following should be of GREATEST concern to an IS auditor when reviewing ethical considerations for an AI solution?

A. The decision-making process is unexplainable.

B. The solution is hosted on a shared cloud environment.

C. The model has not been retrained recently.

D. The solution documentation is still in draft.

Suggested Answer: *A*

Currently there are no comments in this discussion, be the first to comment!

Question #97 *Topic 1*

Which of the following would pose the GREATEST risk when reviewing AI acceptable use training content?

A. The content does not cover the use of effective prompting.

B. The content does not cover the non-deterministic nature of AI.

C. The content does not cover AI model architectures.

D. The content does not cover required performance metrics.

Suggested Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

Question #98 *Topic 1*

An IS auditor is reviewing an AI application that uses customer data to refine the organization's marketing outreach strategies. Which of the following should be the auditor's PRIMARY focus during this review?

A. Alignment with organizational AI strategies

B. Access control design and effectiveness

C. Compliance with applicable privacy regulations

D. Escalation protocols for sensitive data breaches

Suggested Answer: *C*

Currently there are no comments in this discussion, be the first to comment!

Question #99 *Topic 1*

An organization is training a skin cancer recognition model. Photographs collected from which of the following sources would present the GREATEST risk associated with data integrity?

A. Research facility receiving grants for cancer research

B. Open-source data augmentation file

C. Social media platform with images from all over the world

D. Cohort of dermatologists with signed patient consent forms

Suggested Answer: *C*

Currently there are no comments in this discussion, be the first to comment!

Question #100 *Topic 1*

An IS auditor examining change management procedures for an AI system observes inconsistent training data validation and verification protocols prior to model retraining. Which of the following is the MOST significant risk in this context?

A. Addition of AI model complexity due to inconsistent data inputs

B. Noncompliance due to inadequate model training documentation

C. Degradation of system reliability due to compromised or substandard data

D. Delays in AI model retraining due to procedural inefficiencies

Suggested Answer: *C*

Currently there are no comments in this discussion, be the first to comment!

Question #101 *Topic 1*

An AI healthcare diagnostic tool requires large volumes of patient data, raising concerns about privacy and data breaches. Which of the following is the MOST effective strategy to mitigate this risk?

A. Encrypt the data and transmit it through a secure channel.

B. Limit the tool's access to only publicly available data sets.

C. Collect data from all patients to use for data analysis.

D. Use synthetic data or anonymized data sets for model training.

Suggested Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

Question #102 *Topic 1*

Which of the following is MOST important to consider when evaluating ethical risk related to data used for training an AI model?

A. Ability to generate diverse outputs

B. Sensitivity and origin of training data

C. Frequency of model updates

D. Cleaning and validation methods for training data

Suggested Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

Question #103 *Topic 1*

Which of the following is the GREATEST concern when an audit team relies on generative AI to create audit reports?

A. The reports may be more likely to reflect outdated information.

B. The reports may contain misstatements resulting from hallucinations.

C. The reports may use inconsistent formatting from prior audit findings.

D. The reports may tend to use generic language for audit issues.

Suggested Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

Question #104 *Topic 1*

Which of the following is the MOST important reason to conduct regular threat modeling exercises for AI systems and data?

A. To proactively identify potential vulnerabilities in AI systems

B. To assess the performance of AI algorithms

C. To comply with AI regulatory requirements

D. To prevent instances of AI model drift

Suggested Answer: *A*

Currently there are no comments in this discussion, be the first to comment!

Question #105 *Topic 1*

Which of the following is the MOST important reason for applying regular software updates to AI systems operating in high-risk environments?

A. To safeguard the systems against AI-powered zero-day exploits

B. To accelerate model training cycles and enhance processing speed

C. To reduce the need for human oversight of model outputs

D. To address vulnerabilities and reduce the risk of output integrity attacks

Suggested Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

Question #106 *Topic 1*

Which of the following is the MOST important AI data governance method to protect privacy and data security?

A. Using external data sources for AI training

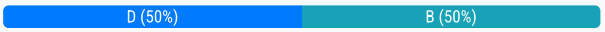
B. Developing AI acceptable use policies

C. Optimizing AI model performance metrics

D. Implementing periodic monitoring

Suggested Answer: *D*

Community vote distribution



Swallows 3 weeks, 5 days ago

Selected Answer: D

In AI data governance, monitoring is paramount to continuously protect privacy and data security.
Why?
In AI systems,
unauthorized access,
data leaks,
model changes,
signals of privacy violations,
policy violations,
and more can occur over time, making continuous monitoring a core governance activity.

upvoted 1 times

RAJ56 1 month ago

Selected Answer: B

AI acceptable use policies are the foundational data governance control that define:
What data may or may not be used for AI training and inference
Restrictions on using PII, confidential, or regulated data User responsibilities, prohibited behaviors, and enforcement mechanisms Without this governance layer, technical controls (monitoring, metrics, performance tuning) lack direction and consistency, increasing privacy and data security risk.

upvoted 1 times

Question #107 *Topic 1*

A car rental company is developing an AI system to dynamically adjust rental pricing based on demand, location, and customer profiles. Which of the following is the MOST important reason to conduct specific testing during development?

A. To ensure the model's pricing logic aligns with business strategy

B. To ensure the system integrates seamlessly with legacy booking platforms

C. To confirm that the AI system can handle high volumes of customer queries

D. To verify that pricing decisions do not result in discriminatory outcomes

Suggested Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

Question #108 *Topic 1*

Which of the following should be done FIRST when developing an incident management process for AI threats?

A. Establish incident classification procedures.

B. Define clear roles and responsibilities.

C. Configure SIEM for security alerts.

D. Develop incident escalation procedures.

Suggested Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

Question #109 *Topic 1*

Which of the following roles is BEST suited to define the implementation roadmaps for adopting AI solutions?

A. Risk management committee

B. Steering committee

C. Product management

D. Internal audit

Suggested Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

Question #110 *Topic 1*

After AI training data has been tested for biases, which of the following is MOST important to check in order to validate the effectiveness of the testing?

A. Feedback on data validation is obtained from key stakeholders.

B. Possible impacts from AI outputs remain within the acceptable risk level.

C. AI processes will meet expected service turnaround time.

D. Sensitive information from users is securely masked before input.

Suggested Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

Question #111 *Topic 1*

Which of the following is the GREATEST risk associated with the use of AI coding tools by software developers?

A. Excessive reliance on AI tools to accomplish routine development tasks

B. Increased likelihood of human biases in code

C. Introduction of security vulnerabilities by AI tools

D. Difficulty in training developers due to the complexity of AI tools

Suggested Answer: *C*

Currently there are no comments in this discussion, be the first to comment!

Question #112 *Topic 1*

An insurance company uses an AI model to set premium rates. To align with AI-related policies on fairness, which of the following is the FIRST course of action?

A. Training alternate AI models and comparing biases with the primary model

B. Reviewing AI model training data to identify potential biases

C. Modifying the AI model's training data set to address potential biases

D. Allowing customers to contest premium rates provided by the AI model

Suggested Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

Question #113 *Topic 1*

During a walk-through, an IS auditor observes an AI engineer entering a prompt that manipulates the AI model's behavior. Which of the following is the BEST control to prevent this?

A. Enforce an input/output template.

B. Deploy adversarial training.

C. Encrypt the underlying data.

D. Retrain the model immediately.

Suggested Answer: *A*

Currently there are no comments in this discussion, be the first to comment!

Question #114 *Topic 1*

Which of the following is the MOST effective control to safeguard a model's architecture, weights, and hyperparameters?

A. Provide training to employees on best practices for AI technical security.

B. Require users to sign a confidentiality agreement before making services and data available.

C. Maintain detailed data audit logs of identified deviations within model training data.

D. Implement strict access controls and encryption for model components.

Suggested Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

Question #115 *Topic 1*

Which of the following presents the MOST significant barrier to generative AI model explainability?

A. Bias within data sets used for model training

B. Rapid evolution of algorithm capabilities

C. Lack of alignment between stakeholder groups

D. Insufficient staff experience with using generative AI tools

Suggested Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

Question #116 *Topic 1*

Which of the following is the MOST important step in an AI incident management process to ensure continuous improvement?

A. Define ownership

B. Root cause analysis

C. Archive logs

D. Assess severity

Suggested Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

Question #1 *Topic 2*

Which of the following should be done FIRST when an attacker exfiltrates sensitive information from an AI model?

A. Inform regulators and affected stakeholders of a potential data breach.

B. Implement rate limiting and query restrictions to reduce exploitation attempts.

C. Isolate impacted systems until the attack vector is identified.

D. Rebuild the AI model using a more secure architecture.

Suggested Answer: *C*

Currently there are no comments in this discussion, be the first to comment!

Question #2 *Topic 2*

Which of the following do supervised AI learning models PRIMARILY use to tram algorithms?

A. Unlabeled data sets

B. Randomized data sets

C. Labeled data sets

D. Clustered data sets

Suggested Answer: *C*

Currently there are no comments in this discussion, be the first to comment!

Question #3 *Topic 2*

A generative AI system has a validation control in place to reject inappropriate questions by checking them against built-in ethical standards. Which of the following enables malicious actors to circumvent this control through prompt engineering?

A. Presenting theoretical situations to justify the reason for asking the questions

B. Submitting the same questions in a foreign language translated by another AI-based system

C. Randomly placing keywords unrelated to the main topic

D. Asking the same questions later when the algorithm has changed after further learning

Suggested Answer: *A*

Currently there are no comments in this discussion, be the first to comment!

Question #4 *Topic 2*

When converting data categories before training an AI model, which of the following scenarios represents the GREATEST risk?

A. One-hot encoding the data attribute car colors for the options red, blue, green black, white

B. Creating dummy variables for the data attribute product flavor for the options vanilla, chocolate, strawberry, banana

C. One-hot encoding the data attribute customer rewards category for the options economy, business, first class

D. Creating dummy variables for the data attribute dog breed for the options labrador, terrier, beagle

Suggested Answer: *C*

Currently there are no comments in this discussion, be the first to comment!

Question #5 *Topic 2*

When utilizing a machine learning (ML) model to predict whether a wind turbine electricity generator will fail, which model evaluation metric should be the PRIMARY focus?

A. Recall

B. Specificity

C. Precision

D. Accuracy

Suggested Answer: *A*

Currently there are no comments in this discussion, be the first to comment!

Question #6 *Topic 2*

An IS auditor notes that an AI model achieved significantly better results on training data than on test data. Which of the following problems with the model has the IS auditor identified?

A. Underfitting

B. Bias

C. Overfitting

D. Generalization

Suggested Answer: *C*

Swallows 1 month ago

Selected Answer: C

A typical symptom of overfitting is a model that fits very well to the training data but performs poorly on unseen test data.

upvoted 1 times

Question #7 *Topic 2*

Which of the following is MOST important to have in place when initially populating data into a data frame for an AI model?

A. An approved risk assessment for including, excluding, or subsequently dropping data attributes from the model

B. The code for separating data into training and testing data sets

C. An analysis of exploratory data that checks for incorrect data types, null values, and duplicate entries

D. The box charts histograms, scatterplots, and Venn diagrams that identify correlations and outliers

Suggested Answer: *C*

Currently there are no comments in this discussion, be the first to comment!

Question #8 *Topic 2*

In order to streamline operations, a bank has deployed an AI application to automatically detect and prevent further fraud on accounts. However, customers have voiced concerns that their usual transactions are being rejected. Which of the following is the MOST likely cause of the false positives?

A. Consent is not properly managed.

B. Compute scale training was not performed.

C. The hyperparameters are not optimized.

D. Data versioning controls were not developed.

Suggested Answer: *C*

Currently there are no comments in this discussion, be the first to comment!

Question #9 *Topic 2*

Which of the following is the PRIMARY reason IS auditors must be aware that generative AI may return different investment recommendations from the same set of data?

A. Neural node access varies each time the process is executed.

B. Servers are reconfigured periodically.

C. Limitations can arise in the quantification of risk profiles.

D. Computational logic is based on probabilities.

Suggested Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

Question #10 *Topic 2*

Which of the following strategies used by modelers to enhance data accuracy has the GREATEST risk of bias and information loss?

A. Filling blank attributes in records with the mean, median, or mode within a grouping

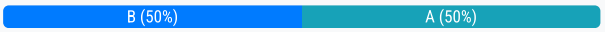
B. Placing numerical data into bins or buckets for a manageable quantity of correlations and result analyses

C. Separating multiple data attributes within one field into individual attribute columns

D. Identifying and deleting duplicate entries in the data set

Suggested Answer: *A*

Community vote distribution



Swallows 1 month, 1 week ago

Selected Answer: B

The model depends on interval boundaries, so arbitrary classifications can have a significant impact.

upvoted 1 times

Ssourav 2 months, 1 week ago

Selected Answer: A

Filling missing values with averages appears harmless but creates biased, less truthful data, posing the greatest risk of bias and information loss.

upvoted 1 times

50a3805 3 months, 3 weeks ago

Selected Answer: B

Preprocessing choices can introduce model bias and affect fairness, especially when continuous data is discretized or transformed in ways that change the underlying relationships.

Because binning fundamentally alters original numerical values, it creates the highest combined risk of bias + information loss.

upvoted 1 times

Question #11 *Topic 2*

An IS auditor reviewing documentation for an AI model notes that the modeler utilized a K-means clustering algorithm, which clusters data into categories for correlations and analysis. Which of the following is the MOST important risk for the auditor to consider?

A. K-means clustering is not a common data clustering method due to its complexity and difficulty categorizing data correctly.

B. K-means clustering algorithms are significantly sensitive to outliers and dependent on the similarity of units of measure.

C. K-means clustering determines the number of clusters for the modeler without supervision.

D. K-means clustering requires the modeler to supervise the learning analysis, which can introduce bias.

Suggested Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

Question #12 *Topic 2*

The PRIMARY purpose of utilizing neural networks in AI is to:

A. mimic human decision making

B. improve the user interface

C. minimize maintenance costs

D. increase computational power

Suggested Answer: *A*

Currently there are no comments in this discussion, be the first to comment!