AAISM試験関連赤本 & AAISMブロンズ教材

ちなみに、Topexam AAISMの一部をクラウドストレージからダウンロードできます：https://drive.google.com/open?id=1rO4nTEw197szz5-IKrWXKqE3T3-cpkIm

ISACA認証試験に参加する方はTopexamの問題集を買ってください。AAISM試験の成功を祈ります。

AAISMの無料デモでは、世界で発生している最新のポイントを追跡できるように、ISACA1年間で無料で更新できます。 AAISM試験トレントの試験の質問は多かれ少なかれ白熱した問題に関係しており、Topexam試験の準備をするお客様は終日試験のトレースを保持するのに十分な時間がない必要があるため、当社のAAISM模擬試験は役立ちます あなたがあなたが無視したホットポイントを補うための助けになるツールとして。 したがって、ISACA Advanced in AI Security Management (AAISM) Exam試験に合格する自信が増し、確実にAAISM試験に合格する率が上がります。

>> AAISM試験関連赤本 <<

AAISMブロンズ教材、AAISM合格問題

ご存じのように、私たちのAAISM学習教材を利用するユーザーが多いです。AAISM学習教材の質問が表示されない場合は、私たちとご連絡頂きます。私たちのスタッフは毎日多くのことを対処しなければなりませんが、どのユーザーも無視することはありません。 私たちのAAISM学習教材の市場はますます大きくなりました。そして、顧客のサポートがあると、私たちのAAISM学習教材がより良くなると信じています。

ISACA AAISM 認定試験の出題範囲：

トピック	出題範囲
トピック 1	• AIテクノロジーとコントロール：このセクションでは、AIセキュリティアーキテクトの専門知識を測定し、安全なAIアーキテクチャとコントロールの設計に関する知識を評価します。プライバシー、倫理、信頼に関する懸念事項、データ管理コントロール、監視メカニズム、そしてAIシステムに合わせたセキュリティコントロールの実装について扱います。
トピック 2	• AI ガバナンスとプログラム管理: 試験のこのセクションでは、AI セキュリティ ガバナンス プロフェッショナルの能力を測定し、ガバナンス フレームワーク、ポリシー作成、データ ライフサイクル管理、プログラム開発、インシデント対応プロトコルを通じて AI セキュリティを実装する際に関係者にアドバイスすることに重点を置いています。
トピック 3	• AI リスク管理: 試験のこのセクションでは、AI リスク管理者のスキルを測定し、リスク処理計画やベンダー監視など、AI 導入に関連する企業の脅威、脆弱性、サプライ チェーン リスクの評価をカバーします。

ISACA Advanced in AI Security Management (AAISM) Exam 認定 AAISM 試験問題 (Q21-Q26):

質問 # 21
A newly hired programmer suspects that the organization's AI solution is inferring users' sensitive information and using it to advise future decisions. Which of the following is the programmer's BEST course of action?

- A. Inform the governance panel
- B. Suggest fine-tuning the AI solution
- C. Alert the CIO to the risk
- D. Conduct a code review

正解：A

解説：
AAISM directs personnel to use established AI governance channels for suspected privacy, ethics, or compliance risks. The governance panel (risk, privacy, legal/compliance, security, product/data science) is chartered to triage, record, investigate, and direct remediation for potential inference of sensitive attributes and resulting decision impacts. Direct technical action (A or C) bypasses due process and accountability; escalating directly to a single executive (B) lacks the structured, cross-functional oversight required for regulated and ethical AI risk handling.
References:AI Security Management™ (AAISM) Body of Knowledge: AI Governance Operating Model; Roles & Responsibilities; Risk Intake and Triage for Privacy/Inference Risks.AAISM Study Guide: Ethics & Responsible AI Escalation Pathways; Governance Board Procedures; Documentation and Decision Records.

質問 # 22
An organization has discovered that employees have started regularly utilizing open-source generative AI without formal guidance. Which of the following should be the CISO's GREATEST concern?

- A. Model hallucinations
- B. Policy violations
- C. Lack of monitoring
- D. Data leakage

正解：D

解説：
The greatest immediate risk from unsanctioned use of public or open-source generative AI tools is data leakage-employees may paste confidential or regulated information into third-party systems, resulting in loss of confidentiality, regulatory exposure, and loss of intellectual property. AAISM emphasizes that when AI use occurs outside approved channels, the top control priority is

preventing exfiltration of sensitive data via prompts, attachments, and context sharing. Monitoring and policy are necessary enablers, but leakage is the highest-impact failure mode in the short term; hallucinations primarily affect accuracy, not confidentiality.
References:* AI Security Management™ (AAISM) Body of Knowledge: Generative AI governance; human- in-the-loop risks; data loss and exfiltration vectors in prompts; sanctioned vs. unsanctioned AI usage.* AI Security Management™ Study Guide: Immediate risk triage for shadow AI; DLP and input-control safeguards; confidentiality-first posture for generative AI adoption.

質問 # 23
During red-team testing of an AI system used to make lending decisions, which of the following techniques BEST simulates a data poisoning attack?

- A. Corrupting training data sets to manipulate outcomes
- B. Stealing model weights from a deployed API
- C. Inputting encrypted data into the model
- D. Adding noise to output predictions

正解：A

解説：
AAISM defines data poisoning as the intentional manipulation of training data so that the learned model behaves incorrectly (e.g., skewed lending approvals/denials) while appearing valid. The correct simulation in red-team exercises is to corrupt or seed the training set with adversarial examples or mislabeled records to induce biased or erroneous decision boundaries. Encrypting inputs (A) is unrelated; output noise (B) describes perturbation of predictions, not training; model weight theft (C) is model extraction, not poisoning.
References: AI Security Management™ (AAISM) Body of Knowledge - Adversarial ML Threats; Data Poisoning and Training-Time Attacks. AAISM Study Guide - Red-Team Methods for AI; Poisoning vs.
Evasion vs. Model Extraction; Controls and Testing for Safety-Critical Decisions.

質問 # 24
Which of the following should be done FIRST when developing an acceptable use policy for generative AI?

- A. Determine the scope and intended use of AI
- B. Consult with risk management and legal
- C. Review existing company policies
- D. Review AI regulatory requirements

正解：A

解説：
According to the AAISM framework, the first step in drafting an acceptable use policy is defining the scope and intended use of the AI system. This ensures that governance, regulatory considerations, risk assessments, and alignment with organizational policies are all tailored to the specific applications and functions the AI will serve. Once scope and intended use are clearly defined, legal, regulatory, and risk considerations can be systematically applied. Without this step, policies risk being generic and misaligned with business objectives.
References:
AAISM Study Guide - AI Governance and Program Management (Policy Development Lifecycle) ISACA AI Governance Guidance - Defining Scope and Use Priorities

質問 # 25
Which of the following is MOST important for effective AI risk management?

- A. Risk measurement during an early stage of the AI system life cycle
- B. Utilization of best practice AI risk management frameworks
- C. Creation of separate risk management processes for AI-specific risk
- D. Internal stakeholder participation in AI risk management processes

正解：D

解説：

AAISM emphasizes that effective AI risk management is socio-technical and hinges on cross-functional stakeholder participation (business owners, security, privacy, legal, compliance, data science, operations).
Participation ensures risks are identified, prioritized, and treated in alignment with business context and risk appetite. While early measurement (B) and using frameworks (D) are important, and separate processes (A) can create silos, stakeholder participation is the primary success factor ensuring governance is practical, adopted, and continuously improved.
References: AI Security Management (AAISM) Body of Knowledge - Governance Roles & Accountability; Integrated Risk Management for AI; Cross-Functional Risk Committees and RACI for AI Programs.

質問 # 26
.....

弊社TopexamのAAISM試験準備では、学習習慣を身に付けるのに役立ちます。 AAISM学習教材を購入して使用すると、学習の良い習慣を身に付けることができます。さらに重要なことは、良い習慣は科学的な小道具の学習方法を見つけ、学習効率を高めるのに役立ちます。そして、短時間でAAISM試験に合格するのに役立ちます。弊社からAAISMテストガイドを急いで購入すると、多くのメリットが得られます。