

Boost up Your Certification Score

Isaca AAIR

ISACA Advanced in AI Risk



For More Information – Visit link below:

<https://www.examsboost.com/>

Product Version

- ✓ Up to Date products, reliable and verified.
- ✓ Questions and Answers in PDF Format.

Visit us at: <https://www.examsboost.com/test/aaair>

Latest Version: 6.0

Question: 1

A risk practitioner is developing risk scenarios related to successful data poisoning attacks on an AI model used across the organization. Which of the following is the BEST approach to help ensure the scenarios are relevant?

- A. Perform adversarial testing in a sandbox environment.
- B. Gather information on similar attacks impacting industry peers
- C. Create comprehensive data flow diagrams.
- D. Engage key stakeholders in risk scenario development.

Answer: D

Explanation:

Risk scenario development in AI requires that scenarios be grounded in organizational context, business processes, and actual threat landscapes. Risk scenarios must reflect the specific systems, data flows, and stakeholder concerns relevant to the organization.

Why D is Correct: According to the ISACA AAIR Study Guide, engaging key stakeholders is the cornerstone of effective risk scenario development. Stakeholders bring domain knowledge, business context, and awareness of operational dependencies that technical practitioners may lack. This collaborative approach ensures scenarios address real-world consequences, organizational risk appetite, and business-critical functions—making them actionable and relevant.

Why A is Wrong: Adversarial testing in a sandbox validates controls but does not by itself produce contextually relevant risk scenarios. It is a technical activity, not a scenario development process.

Why B is Wrong: Peer benchmarking provides useful threat intelligence but cannot replace stakeholder engagement. Industry peer data may not reflect the organization's specific AI architecture or risk tolerance.

Why C is Wrong: Data flow diagrams are useful supporting artifacts but describe technical pathways rather than capturing the organizational and business context required for relevant risk scenarios.

Question: 2

Which of the following is a risk practitioner's BEST recommendation to establish accountability for AI system outputs and decisions?

- A. Centralized governance task force for model decision authority

- B. Continuous monitoring and key performance indicators (KPIs)
- C. Regular reviews of resource allocation for AI projects
- D. Formal documented role assignments with named owners

Answer: D

Explanation:

Accountability in AI governance requires that specific individuals or roles be clearly designated as responsible for AI system outputs, decisions, and associated risks. Without formal documentation of ownership, accountability gaps emerge.

Why D is Correct: The ISACA AAIR framework emphasizes that accountability must be explicit and documented, with named individuals assigned to own AI outcomes. Formal role assignments create a traceable chain of responsibility that supports auditability, regulatory compliance, and effective escalation when issues arise. Named ownership prevents diffusion of responsibility.

Why A is Wrong: A centralized task force creates collective responsibility, which can dilute individual accountability. Governance bodies support oversight but do not replace individual role ownership for specific outputs.

Why B is Wrong: Continuous monitoring and KPIs are valuable operational controls but represent monitoring mechanisms, not accountability structures. Monitoring detects issues but does not assign responsibility for them.

Why C is Wrong: Resource allocation reviews address investment efficiency rather than accountability for AI decisions and outputs. This is a management activity, not an accountability framework.

Question: 3

Which of the following is the PRIMARY purpose of maintaining comprehensive model cards and documentation?

- A. Justifying model use cases
- B. Preserving audit trails
- C. Listing technical specifications
- D. Providing model transparency

Answer: D

Explanation:

Model cards are standardized documents that communicate key information about AI models, including their intended use, training data, performance characteristics, limitations, and ethical considerations. They serve as a primary transparency instrument in AI governance.

Why D is Correct: According to the ISACA AAIR curriculum, the primary purpose of model cards is to provide transparency to stakeholders—including developers, users, auditors, and

regulators. Transparency enables informed decision-making about model deployment, helps identify potential misuse, and supports responsible AI governance across the life cycle.

Why A is Wrong: Justifying use cases is a secondary benefit. Model cards are not primarily advocacy documents; their core function is objective disclosure of model characteristics and limitations.

Why B is Wrong: Preserving audit trails is a governance function served by version control and change management systems. While model cards contribute to audit readiness, it is not their primary purpose.

Why C is Wrong: Technical specifications represent only a subset of model card content. Model cards go beyond technical detail to address fairness, bias, intended use boundaries, and societal impact considerations.

Question: 4

Which of the following BEST enables an organization adopting AI solutions to foster an ethical and risk-aware culture?

- A. All business units use checklists to ensure AI risk and ethical concerns are addressed.
- B. Senior management representatives actively participate in industry conferences related to AI ethics.
- C. AI policies include clear disciplinary actions for violations of risk and ethical standards.
- D. Leadership consistently models ethical behavior and values for AI development and use.

Answer: D

Explanation:

Organizational culture is primarily shaped by leadership behavior and tone at the top. In AI governance, an ethical culture cannot be mandated through documentation alone—it must be demonstrated through the actions and values of organizational leaders.

Why D is Correct: The ISACA AAIR Study Guide emphasizes that tone at the top is the most powerful driver of ethical culture. When leaders consistently model ethical behavior in AI development and usage, they create a normative environment where employees internalize values rather than merely complying with rules. This authentic leadership approach produces sustainable cultural change.

Why A is Wrong: Checklists are compliance tools that address process adherence, not cultural transformation. A checklist culture can produce box-ticking behavior without genuine ethical commitment.

Why B is Wrong: Conference participation raises awareness but has minimal impact on day-to-day organizational behavior. External networking does not directly shape internal culture.

Why C is Wrong: Disciplinary actions represent reactive compliance enforcement. While necessary, punitive measures create a compliance-driven rather than values-driven culture, which is less robust and sustainable.

Question: 5

To reinforce organization-wide ethical norms and risk recognition, which of the following is MOST important to integrate into AI user training?

- A. Acceptable use policy and acknowledgment
- B. Ethical risk indicators and reporting
- C. Cyber threat identification and AI incident handling
- D. External regulations and compliance checklists

Answer: B

Explanation:

Effective AI user training must go beyond policy acknowledgment and compliance instruction to equip employees with the practical skills needed to identify ethical risks and report them appropriately. This builds an active risk-aware workforce.

Why B is Correct: The ISACA AAIR framework identifies that training on ethical risk indicators and reporting mechanisms directly reinforces ethical norms by enabling employees to recognize real-world signs of AI misuse, bias, or harmful outputs. When staff can identify specific risk signals and know how to escalate them, the organization builds a proactive risk culture grounded in practical ethical literacy.

Why A is Wrong: Acceptable use policy acknowledgment is a compliance activity, not a culture-building measure. Acknowledging a document does not ensure employees understand how to apply ethical principles in practice.

Why C is Wrong: Cyber threat identification addresses security risk, which is narrower than the full scope of ethical AI risk. Security training does not develop ethical judgment regarding fairness, bias, or societal impact.

Why D is Wrong: Regulatory compliance checklists address legal obligations but do not develop the ethical reasoning and risk recognition skills needed to reinforce organizational norms.

Thank You for Trying Our Product

For More Information – **Visit link below:**

<https://www.examsboost.com/>

15 USD Discount Coupon Code:

G74JA8UF

FEATURES

- ✓ **90 Days Free Updates**
- ✓ **Money Back Pass Guarantee**
- ✓ **Instant Download or Email Attachment**
- ✓ **24/7 Live Chat Support**
- ✓ **PDF file could be used at any Platform**
- ✓ **50,000 Happy Customer**



Visit us at: <https://www.examsboost.com/test/aair>