Sample Exam

Edition 202511

Content

Introduction

This is the EXIN Artificial Intelligence Compliance Professional (AICP.EN) sample exam. The Rules and Regulations for EXIN's examinations apply to this exam.

This exam consists of 40 multiple-choice questions. Each multiple-choice question has a number of possible answers, of which only one is correct.

The maximum number of points that can be obtained for this exam is 40. Each correct answer is worth 1 point. You need 26 points or more to pass the exam.

The time allowed for this exam is 90 minutes.

You are allowed to use the AI Act for this exam.

Good luck!

Sample exam

1 / 40
The AI Act is a piece of legislation created for the European Union (EU). In Article 1, the AI Act describes its objectives.

What are the **main** objectives of the AI Act?

A) Guidelines focused solely on environmental protection, with no specific rules for high-risk AI, no prohibitions, and innovation measures only for large corporations
B) Harmonized rules for AI systems in the EU, prohibitions on certain AI practices, requirements for high-risk AI, transparency rules, market surveillance, and innovation support
C) Prohibitions on AI practices, rules for general-purpose AI only, transparency rules excluding high-risk AI, and support for innovation restricted to non-European entities
D) Rules for AI systems limited to safety and health, prohibitions on all AI practices, transparency rules only for high-risk AI, and innovation support excluding startups

2 / 40
According to the AI Act, what do accountability and compliance mean?

A) Accountability focuses on maintaining user privacy and data security, while compliance relates to the integration with existing IT infrastructure.
B) Accountability involves holding developers and operators in AI development responsible, and compliance means adhering to legal requirements.
C) Accountability is about ensuring that AI systems are profitable for developers, and compliance involves meeting user demands and preferences.
D) Accountability refers to AI users being accountable for correct use of the system, while compliance means following industry standards for AI innovation.

3 / 40
Under the AI Act, individuals affected by AI systems have specific rights to ensure transparency, fairness, and accountability.

What is a right explicitly granted under the AI Act?

A) The right to be informed of interacting with or being affected by an AI system
B) The right to demand access to the source code of the AI system
C) The right to prohibit the use of AI in any decision-making process that involves them
D) The right to request deletion of personal data used by the AI system

4 / 40
Anna, a compliance officer at a small or medium-sized enterprise (SME), is responsible for overseeing the implementation of a new AI system used for automating customer support. The company did not build this system but is buying the system from another provider. The AI system is classified as a high-risk AI system under the AI Act.

Anna has been asked to ensure the company complies with user obligations when deploying and monitoring this AI system. She must determine which actions must be prioritized and which actions should be avoided.

What should Anna **not** consider, given the obligations for AI users?

A) Developing the AI model's algorithms further to enhance its decision-making capabilities without involving its provider
B) Keeping detailed records of the AI system's performance and ensuring compliance with relevant reporting requirements
C) Monitoring the performance of the AI system to ensure it operates as intended and complies with safety standards
D) Reporting any serious incidents or malfunctions with the AI system to the appropriate authorities as is required by law

5 / 40
An AI system for facial recognition is used for security purposes in public spaces. One organization is most relevant to overseeing compliance with data protection and privacy regulations, such as the General Data Protection Regulation (GDPR), for this AI system.

Which organization is that?

A) The European Consumer Organization (BEUC)
B) The European Artificial Intelligence Board (EAIB)
C) The European Court of Justice (ECJ)
D) The European Data Protection Board (EDPB)

6 / 40
A business develops an AI system for personalized marketing. This system uses machine learning (ML) algorithms to tailor advertisements to individual customers. During a compliance review, the team identifies the following risks:

- There is no documentation that clearly shows how the AI system handles data.
- The process of how the AI system makes personalized recommendations is not fully understood.
- Customers are complaining about these issues.

The company must comply with the AI Act. The business uses the ISO/IEC 42001 standard and the NIST AI Risk Management Framework (RMF) to accomplish that.

According to this standard and framework, what should the business do to resolve the issues?

A) Conduct a series of user experience (UX) tests to get feedback on usability, learnability, and customer preferences
B) Focus on improving the system's prediction accuracy to improve cost efficiency, customer satisfaction, and engagement
C) Implement a documentation process that details data sources, processing methods, and algorithmic decision-making
D) Upgrade the system's hardware to ensure faster processing, greater efficiency, and higher customer satisfaction

7 / 40
A business develops an AI system to monitor patients who are hospitalized. The system uses high-definition cameras inside the patients' rooms to monitor the status of the patients in real time. If the system detects a patient is in distress, it automatically calls a nurse to the patient's bed.

To improve the performance of the AI system, the business wants to start building a database of videos of the patients with a note from a professional at critical points in the video, to build more training data for the system.

The business is considering doing a data protection impact assessment (DPIA). The team responsible is unsure if a DPIA should be done at all. If a DPIA is mandatory, the team wants to know when the assessment should be done: now or only after deployment of the update.

The business must comply with the AI Act and the General Data Protection Regulation (GDPR).

Should the business do a DPIA now?

A) Yes, because a DPIA is required for AI projects that could pose a high risk to the rights of natural persons.
B) Yes, because a DPIA is required for any project that collects personal data, even if the project is low risk.
C) No, because a DPIA is not required for using data for training purposes, education, or scientific research.
D) No, because a DPIA is only required after the AI system has been fully developed, tested, and deployed.

8 / 40
A business develops an AI system for real-time facial recognition. A private security firm deploys the AI system to monitor a public shopping mall. The system scans all visitors, cross-checks them with databases of past offenders and political activists, and flags visitors that are listed in one of those databases. Visitors that are flagged are covertly tracked throughout their visit to assess whether they engage in what the security firm finds suspicious behavior.

According to the AI Act, in which category should the use of this AI system be classified?

A) Unacceptable risk
B) High risk
C) Limited risk
D) Minimal or no risk

9 / 40
A travel agency uses an AI system to develop dynamic, targeted marketing campaigns for their vacation packages. These campaigns include real-time advertisement placements on social media and travel platforms, using the individuals' browsing history. The travel agency uses AI to infer the user's emotional state and then suggests customized destinations and activities.

The travel agency must comply with the AI Act.

What risk must the travel agency address?

A) The risk of including potential biases. They should update the training data regularly to avoid suggesting irrelevant destinations or infer wrong emotional states.
B) The risk of ineffective advertising activities. They should focus on updating the algorithm, because the AI Act does not cover personalized advertisements.
C) The risk of lack of transparency. They should guarantee openness about the AI, reduce bias in suggestions, and evaluate if the advertising activities are ethical.
D) The risk of misusing personal data. They should stop using AI-driven personalization because the AI Act forbids using personal data for targeted advertising.

10 / 40
A company developed an AI model that can be used in various industries, including healthcare and finance. Due to its wide application, the AI model carries potential risks to public health.

What did the company develop, and which practices should the company implement according to the AI Act?

A) The company developed a general-purpose AI (GPAI) that carries systemic risks. It should conduct additional tests to mitigate the risks.
B) The company developed a high-risk AI system. It should implement all the requirements for high-risk AI systems as outlined in the AI Act.
C) The company developed a narrow AI model. It should ensure the model operates only within predefined parameters to prevent risks.
D) The company developed an experimental AI model. It should focus on research and development without immediate risk management.

11 / 40
An organization develops a high-risk AI system. During testing, the development team identifies various risks, including inconsistencies in data completeness and the presence of outdated records. These risks could negatively impact the model's performance.

The organization must comply with the AI Act. They use the CEN/CLC/TR 18115 framework to do so.

According to this framework, what should the organization do to address these risks?

A) Conduct a data protection impact assessment (DPIA) to address the fairness of AI decision-making
B) Encrypt all training and testing datasets using protocols to prevent unauthorized access to personal data
C) Implement general-purpose risk controls to reduce the mentioned operational and reputational risks
D) Improve the data quality by applying structured quality metrics and statistical evaluation methods

12 / 40
The AI Act describes several roles connected to an AI system.

What is the definition of the role 'importer of an AI system'?

A) A person or organization that designs, develops, and markets an AI system under their own name or trademark.
B) A person or organization that places an AI system on the market but is not responsible for its original development.
C) A person or organization that uses an AI system in their operations and ensures local compliance with user obligations.
D) A regulatory authority tasked with monitoring if the AI system is imported in compliance with the AI Act regulations.

13 / 40
A business develops an AI system for fraud detection in financial transactions. This system analyzes transaction patterns to identify suspicious activities and prevent fraudulent behavior. Given the potential for false positives that could impact legitimate transactions and the evolving nature of fraud tactics, the business recognizes the need for effective safeguards.

The business must comply with the AI Act. To help prevent issues concerning false positives, the business uses the ISO/IEC 23894 standard.

According to this standard, what should the business do to prevent these issues?

A) Embed risk management into all activities to ensure comprehensive oversight and proactive risk mitigation
B) Enhance data privacy measures to protect sensitive information and comply with privacy regulations
C) Focus on improving model accuracy to ensure reliable performance and minimize false positives
D) Implement cybersecurity measures to protect the system from external threats and unauthorized access

14 / 40
A manufacturing company uses robotic devices driven by AI for quality control on its assembly lines. The investigative team notes that an anonymous whistleblower claims the AI system lately shows an unusually low number of faulty products. The reason for the underreporting of faulty products is a software update of the AI system. Upon manual inspection, the products are faulty and unsafe to use.

The report states that the new defect detection algorithm produces a crucial error that causes the false negatives. According to the whistleblower, managers knew about the issue but did not address the issue, to avoid damaging the company's reputation.

What should the next actions be?

A) - Adjust the internal algorithm to address the problem
- Notify the relevant competent authority if the issue still exists after 30 days

B) - Investigate the problem internally and start solving it
- Notify the relevant competent authority of the occurrence immediately

C) - Research the whistleblower's reasons for reporting
- Notify the relevant competent authority if consumers start complaining

D) - Stop using the AI system and switch to an older method
- This makes it unnecessary to inform the relevant competent authority

15 / 40
MedTech Diagnostics uses a high-risk AI system for diagnosing medical conditions from X-ray images. They have the following in place:

- The company has passed an external audit to ensure the AI system adheres to the AI Act's standards.
- A robust risk management framework identifies and mitigates potential issues, with contingency plans in place.
- Detailed records of the AI system's operations are securely stored for accountability and audits.
- Clear documentation and training are provided to users, explaining AI decision-making and limitations.
- All AI-generated diagnoses are reviewed by medical professionals before being finalized, integrating human judgment.

What else should the company implement?

A) They should add robust data governance procedures to maintain the reliability and fairness of their AI system.

B) They should ensure that the AI system can operate independently without any human intervention for efficiency.

C) They should implement a system to automatically override human decisions to speed up the diagnosis process.

D) They should include a feature that allows patients to directly modify their medical records based on AI suggestions.

16 / 40
An insurance company implements a new AI-based credit scoring system with access to both internal databases and public databases. The following risks are identified:

- **A lack of proper training data**. If the model is not trained well, it will be difficult to accurately determine a fair score for people.
- **Integration with other applications**. It will be difficult to integrate the AI-based engine into the rather complex and at some points outdated application environment.
- **Non-compliance with the GDPR**. The General Data Protection Regulation (GDPR) has specific requirements for the autonomous processing of personal data by automated systems.
- **Transparency and quality of the model**. Both the employees and the customers must be able to understand the results and decisions of the AI model.

The insurance company must comply with the AI Act.

Which risk is **not** important for compliance with the AI Act?

A) A lack of proper training data
B) Integration with other applications
C) Non-compliance with the GDPR
D) Transparency and quality of the model

17 / 40
A government agency proposes an AI system to help with predicting crime hotspots around the downtown area of a larger town. The system will be used for automated surveillance. It is programmed to automatically identify persons that display suspicious behavior and report them to the local police. This is a great opportunity for preventing crime, increasing feelings of safety, and ensuring justice after crime.

Are there any risks related to implementing this AI system?

A) Yes, because an AI system that is used for automated decisions carries the inherent risk of bias, which may unfairly disadvantage individuals.
B) Yes, because the AI Act foresees so many privacy risks with surveillance systems that it outright forbids its employment in public spaces.
C) No, because in crime prosecution and prevention, AI systems carry no particular risks since they are used to enhance public safety.
D) No, because public domain AI systems boost efficiency and carry no risk, since the decisions are objective and free from human error.

18 / 40
An organization develops an AI system for recruitment purposes. During internal testing, the team identified a risk: the system sometimes unintentionally favored candidates from certain backgrounds, leading to potentially discriminatory outcomes. The team is now unsure how to structure their response to these concerns.

The organization must comply with the AI Act. To help mitigate the risk, the organization uses the ISO/IEC TR 24368 standard.

According to this standard, what should the organization do to mitigate this risk?

A) Adjust the algorithm to prioritize demographic quotas based on employment statistics
B) Adopt a zero-data approach by removing all demographic data from the training set
C) Apply cybersecurity measures to protect candidate data and enhance system integrity
D) Implement a stakeholder engagement process to identify and mitigate potential biases

19 / 40
An organization develops an AI system for loan approval. During internal testing, the compliance team finds a risk: they find a lack of transparency in how the model makes decisions, as well as limited documentation for risk evaluation.

The organization must comply with the AI Act. The organization uses the ISO/IEC 42001 standard and the NIST AI Risk Management Framework (RMF) to accomplish that.

According to this standard and framework, what should the business do to address this risk?

A) Conduct a safety compliance assessment based on recommended cybersecurity guidelines
B) Decommission the AI system immediately and transition to a manual loan approval process
C) Define a measurement plan with transparency metrics and record decision logic for oversight
D) Rebuild the system using synthetic data to eliminate as many sources of bias as possible

20 / 40
A leading automotive manufacturer has developed a highly automated vehicle (level 4) equipped with an AI-based object recognition technology for road safety. During testing, the following risks are discovered:

- The system's ability to detect speed bumps is compromised under low-light conditions.
- It might be hard to sell the model, because it does not know dimensions of other vehicles.
- The developers are not quite sure how to explain how the model makes decisions.
- Not all stakeholders were asked for input during the development phase of the AI system.

When **only** looking at AI Act compliance, what must be addressed?

A) The risk of insufficient testing under real-world conditions
B) The risk of lack of transparency in AI decision-making
C) The risk of limited scalability of the AI system to other vehicle models
D) The risk of limited stakeholder involvement during AI development

21 / 40
A logistics company is building an AI system to optimize its delivery paths and lower fuel usage. The organization is weighing two choices:

- A closed-source AI model from a vendor who guarantees speedier installation and verified compliance certifications.
- An open-source AI model that allows for great customizing and transparency.

The company must comply with the AI Act but also wants to balance innovation and cost.

Which model suits this company **best**?

A) A closed-source AI model, because it is intrinsically more secure and trusted by authorities. This reduces the possibility of non-compliance.
B) A closed-source AI model, because it provides pre-certified compliance. This lessens the company's burden of proving AI Act compliance.
C) An open-source AI model, because it guarantees complete transparency. This helps with documentation and auditability requirements.
D) An open-source AI model, because it is excepted from AI Act compliance. This is due to the source code being publicly available.

22 / 40
The AI Act defines ethical principles for AI development.

What is **not** one of those principles?

A) Explicability
B) Fairness
C) Loss prevention
D) Respect for AI autonomy

23 / 40
A startup develops an AI system to assist with personalized learning in schools by tailoring lesson plans to individual students' needs. The system collects data on students' performance and learning behaviors.

According to the AI Act, what should the startup consider here, to balance innovation with regulation?

A) Avoid labeling the system as high-risk to circumvent additional regulatory burdens and streamline innovation
B) Ensure the AI system undergoes a conformity assessment and complies with high-risk system regulations
C) Implement robust data protection features but take out user notifications to avoid delays in deployment
D) Market the system to private schools exclusively to limit the impact of high-risk compliance requirements

24 / 40
A financial institution, Fintegra, is implementing an AI system to detect fraud in transactions. The system requires access to customers' transaction information and demographic data for its analysis. Fintegra must comply with the AI Act's data minimization requirement.

What is the **best** way for Fintegra to comply with the data minimization requirement?

A) They should anonymize all transaction data and remove any data that identifies a natural person to comply with the requirement, even if that data is critical for fraud detection purposes.
B) They should collect all personal details, including full name and precise address, to ensure precise analysis and improvement over time, and securely store the data as long as needed.
C) They should limit data collection to transaction data that is relevant to detecting fraud, and avoid processing personal details, such as the customers' full name or precise address.
D) They should share the collected data only with recognized vendors compliant with the AI Act, which minimizes internal handling of personal details, like the customer's full name.

25 / 40
EduTech is implementing an adaptive learning platform that uses AI to personalize learning paths for students. The platform adjusts the difficulty of tasks based on individual performance.

What risk should EduTech mitigate to ensure the ethical use of this AI system?

A) The risk of bias and discrimination, because these would lead to unfair advantages or disadvantages for certain students. This risk is mitigated by regularly reviewing and updating the AI system's data sets and algorithms.
B) The risk of over-reliance on technology, which could result in students not developing critical thinking skills. This risk is mitigated by keeping the AI system's decision-making process confidential to stimulate students to think more.
C) The risk of privacy breaches, because sensitive student data, including their performance could be mishandled or exposed. This risk is mitigated by focusing more on improving the technical performance of the AI system.
D) The risk of transparency issues, because students and educators may not understand how decisions are made. This risk is mitigated by ensuring that the AI system operates without human oversight, which ensures fairness.

26 / 40
A hospital department specializes in the diagnosis and treatment diseases. They develop an AI diagnostic system to assist in identifying rare diagnoses. The system analyses patient data, medical history, and imaging scans.

The system is successfully adopted in the United States (US). Some medical specialists in the European Union (EU) want to adopt the system, but they do not have clear understanding of how the AI system works. They also do not have special knowledge and experience in monitoring AI or recognizing malfunctions or misdiagnoses.

What is **not** a risk associated with the adoption of this AI system?

A) The risk of lack of effective human supervision
B) The risk of misdiagnosis due to automation bias
C) The risk of mistrust caused by lack of transparency
D) The risk of unauthorized access to patient records

27 / 40
A business makes an AI system for smart home assistants. During testing, the team finds that voice recognition errors, such as confusing similar-sounding words, lead to unintended actions, like turning on the wrong appliance. These mistakes can cause privacy breaches, such as recording conversations without consent or misidentifying users, potentially sharing sensitive information with unauthorized parties.

The organization must comply with the AI Act. They use the CEN/CLC/TR 18115 framework to do so.

According to this framework, what should the AI provider do to address the issue?

A) Create a stakeholder engagement plan to get different views on how the AI system works
B) Do an ethical impact assessment to understand privacy risks of smart home assistants
C) Improve the training data quality by using systematic validation and error-checking methods
D) Increase data security with encryption to protect voice data and prevent data breaches

28 / 40
A technology company was found to be using an AI system for real-time remote biometric identification, which is explicitly prohibited by the AI Act.

What is the appropriate penalty for this violation?

A) A formal warning without financial penalties
B) An administrative fine of up to €7.5 million or 1% of the total global annual turnover in the previous financial year
C) An administrative fine of up to €15 million or 3% of the total global annual turnover in the previous financial year
D) An administrative fine of up to €35 million or 7% of the total global annual turnover in the previous financial year

29 / 40
The AI Act particularly emphasizes the importance of two aspects of AI systems: transparency and traceability.

Why are transparency and traceability important?

A) Because they are crucial for ensuring accountability and fostering trust in AI systems.
B) Because they are mandatory requirements for all products, including AI systems.
C) Because they are particularly essential for the reliability and automation of AI systems.
D) Because they are shared between European, Chinese, and American legislation.

30 / 40
An AI system, used by a retail organization, automatically changes the way elements of the website are displayed based on user preferences and device used. The system recommends products and enhances user experience using click history and time spent on a page.

According to the AI Act, in which category should the use of this AI system be classified?

A) Unacceptable risk
B) High risk
C) Limited risk
D) Minimal or no risk

31 / 40
A company creates an AI system for automated decision-making in its hiring process. The AI system will screen resumes, rank candidates, and make recommendations for interviews.

The company is worried that the AI system may have biases that could affect the hiring process.

What is the **best** approach for the company to mitigate biases in the AI system?

A) Allow the AI system to learn and adapt without further human intervention
B) Ignore biases in the training data and focus on the AI system's performance
C) Implement a diverse development team to create and monitor the AI system
D) Use a single source of data for training the AI system to ensure consistency

32 / 40
Feline Finesse is a webshop that sells cat accessories and cat pillows, including personalized cat plushies based on customer pictures. The webshop uses an AI system that can do the following things:

- It dynamically changes prices depending on consumer activity.
- It ranks search results, based on customer preferences.
- It gives personal recommendations for other products it thinks the customer likes.

Currently, the webshop makes customers aware of what the AI system does and is very transparent about how the algorithm works. However, the CEO questions this practice and wants to know what degree of transparency is required and how it affects sales.

With reference to the AI Act, what should the CEO know about transparency?

A) Transparency can prove to consumers that the system is objective. Consumers have a right under the AI Act to understand how their data is used and this understanding fosters trust.
B) Transparency can show the limits or constraints of the AI system. Consumers may lose trust in the company after understanding this, which damages the company's reputation.
C) Transparency is not mandated for e-commerce. Consumers are helped by the convenience of personalization and do not need knowledge or understanding of how the AI system operates.
D) Transparency is restricted to making the source code of the AI system available. Consumers' confidence in the system may decrease from understanding how the algorithm works exactly.

33 / 40
A high-risk AI system is used in the recruitment process, automatically filtering candidates based on their qualifications. However, the deployer has not implemented any mechanism for human intervention or oversight in cases of questionable decisions.

According to the AI Act, does this system require human oversight?

A) Yes, because human oversight is necessary for intervention in decision-making processes.
B) Yes, because human oversight ensures compliance with fairness and transparency obligations.
C) No, because automated systems are designed to function without human intervention.
D) No, because recruitment processes do not involve critical safety risks to natural persons.

34 / 40
A company prepares to launch a general-purpose AI (GPAI) model. The model can be adapted for tasks such as customer service automation, content creation, and data analysis. The company is based outside the European Union (EU) but plans to distribute the model across several EU member states.

According to the AI Act, what is **not** required before distributing the GPAI model in the EU?

A) Appoint an authorized representative in the EU to handle compliance matters
B) Comply with EU copyright regulations for model training with copyrighted data
C) Conduct a thorough audit to verify full conformity with all EU laws and regulations
D) Publish a detailed summary of the content used for training the GPAI model

35 / 40
An organization deploys an AI system for predictive maintenance for industrial equipment. After several months of operation, the system generates a very high number of false alerts, disrupting workflows. An investigation shows the following:

- The organization did not consider the dynamic environmental changes on the work floor.
- The organization lacks a formal process for reassessing risks after deployment.

The organization must comply with the AI Act. To help solve these issues, the organization uses the ISO/IEC 23894 standard.

According to this standard, what should the organization do to address these issues?

A) Conduct a human-centered design workshop to improve system usability
B) Design a risk management process with ongoing evaluation and monitoring
C) Perform a cybersecurity audit to identify and address possible vulnerabilities
D) Replace the AI system with a simpler, rule-based model for easier control

36 / 40
An AI system is used by a car fleet management company to track driver behavior and forecast maintenance requirements. Large volumes of data, such as GPS locations, driving patterns, and vehicle performance indicators, are gathered and processed by the system. A recent audit found that the business had not put in place sufficient data protection procedures.

According to the AI Act, data management and privacy protection are essential for this business.

Why is this essential?

A) Because it enables the business to prioritize business objectives and operational efficiency
B) Because it enhances user trust, safeguards personal data, and prevents unauthorized access
C) Because it is mandatory and complying with the AI Act avoids legal trouble and potential fines
D) Because it streamlines data gathering procedures by removing the need for user consent

37 / 40
According to the AI Act, which use of an AI system fits the classification of limited risk?

A) A chatbot designed to assist customers with general inquiries, which is programmed to disclose it is an AI.
B) A facial recognition system used for real-time identification of customers in public spaces, such as a mall.
C) A medical diagnostic tool that assists doctors by giving treatment recommendations based on patient data.
D) An AI system that operates an autonomous vehicle, which drives on public roads without human supervision.

38 / 40
A business develops an AI system for education. The AI system will determine if a student gets access to materials, is admitted to a school, or gets assigned to a class. The AI system will be provided via cloud services.

According to the AI Act, in which category should the use of this AI system be classified?

A) Unacceptable risk
B) High risk
C) Limited risk
D) Minimal or no risk

39 / 40
An organization has developed an AI system for automated hiring. During testing, the team finds the following:

- The system consistently scores candidates from certain ethnic backgrounds lower, because there is demographic bias in the training data.
- Currently, there is no internal review process or feedback mechanism from relevant parties that could have pointed the risk of this specific bias out.

The organization must comply with the AI Act. To help solve these issues, the organization uses the ISO/IEC TR 24368 standard.

According to this standard, what should the organization do to solve these issues?

A) Create a synthetic dataset to address demographic imbalances and improve fairness
B) Implement transparency to increase the system's explainability and accountability
C) Strengthen data encryption practices and use access control to prevent breaches
D) Use an ethical framework with stakeholder input to evaluate human rights issues

40 / 40
An AI startup develops a general-purpose AI (GPAI) model, trained on publicly available online content, including news articles, research papers, and social media posts. After launching, the company receives a legal notice from a group of authors claiming their intellectual property (IP) was used for training the model without authorization.

What should be done to protect IP rights in this case?

A) Argue that the GPAI model qualifies as open-source, and is exempt from copyright compliance obligations
B) Claim fair use under the AI Act, since the content was publicly available, and continue using the dataset
C) Delete the AI-generated outputs containing similarities to the disputed works to avoid infringement claims
D) Document and share details of the GPAI training dataset, including provenance, to ensure compliance

Answer key

1 / 40
The AI Act is a piece of legislation created for the European Union (EU). In Article 1, the AI Act describes its objectives.

What are the **main** objectives of the AI Act?

A) Guidelines focused solely on environmental protection, with no specific rules for high-risk AI, no prohibitions, and innovation measures only for large corporations
B) Harmonized rules for AI systems in the EU, prohibitions on certain AI practices, requirements for high-risk AI, transparency rules, market surveillance, and innovation support
C) Prohibitions on AI practices, rules for general-purpose AI only, transparency rules excluding high-risk AI, and support for innovation restricted to non-European entities
D) Rules for AI systems limited to safety and health, prohibitions on all AI practices, transparency rules only for high-risk AI, and innovation support excluding startups

A) Incorrect. This option focuses only on environmental protection and excludes specific rules for high-risk AI, prohibitions, and innovation measures for large corporations, which misrepresents the AI Act's comprehensive approach.
B) Correct. This option accurately reflects the AI Act's main points, including harmonized rules for AI systems, prohibitions on certain AI practices, specific requirements for high-risk systems, transparency rules, market surveillance, and innovation support focused on small and medium enterprises (SMEs). (Literature: A, Chapter 3.1, 3.2; AI Act, Article 1)
C) Incorrect. This option suggests that the AI Act only addresses general-purpose AI and excludes high-risk AI from transparency rules, while restricting innovation support to non-European entities, which is not supported by the AI Act's objectives.
D) Incorrect. The AI Act’s objectives are broader than just safety and health. This option inaccurately claims that rules are limited to safety and health, excludes startups from innovation support, and states prohibitions on all AI practices, which does not align with the AI Act's provisions.

2 / 40
According to the AI Act, what do accountability and compliance mean?

A) Accountability focuses on maintaining user privacy and data security, while compliance relates to the integration with existing IT infrastructure.
B) Accountability involves holding developers and operators in AI development responsible, and compliance means adhering to legal requirements.
C) Accountability is about ensuring that AI systems are profitable for developers, and compliance involves meeting user demands and preferences.
D) Accountability refers to AI users being accountable for correct use of the system, while compliance means following industry standards for AI innovation.

A) Incorrect. While user privacy and data security are important, accountability and compliance in the AI Act are broader concepts focused on responsibility and adherence to legal and regulatory requirements, rather than solely on privacy or integration concerns. Compliance is about following legal and ethical regulations, not IT integration.
B) Correct. Accountability means that developers and operators of AI systems can be held responsible for their actions and outcomes. Compliance refers to following the legal and regulatory requirements outlined in the AI Act to ensure systems are safe, transparent, and fair. (Literature: A, Chapter 3.10)
C) Incorrect. Accountability is not related to profitability or user preferences, and compliance is not about meeting user demands. Instead, they focus on responsibility and adherence to legal standards for AI systems.
D) Incorrect. Accountability involves holding developers and operators responsible for the AI systems' actions, not shifting blame. Compliance is more about meeting specific legal and regulatory standards rather than general industry standards.

3 / 40
Under the AI Act, individuals affected by AI systems have specific rights to ensure transparency, fairness, and accountability.

What is a right explicitly granted under the AI Act?

A) The right to be informed of interacting with or being affected by an AI system
B) The right to demand access to the source code of the AI system
C) The right to prohibit the use of AI in any decision-making process that involves them
D) The right to request deletion of personal data used by the AI system

A) Correct. Individuals must be informed when they are interacting with an AI system, unless it is obvious to a reasonably well-informed person. This ensures transparency and helps individuals understand when AI is influencing decisions that may affect them. (Literature: A, Chapter 3.6; AI Act, Article 50)
B) Incorrect. The AI Act does not grant individuals the right to access the source code of an AI system. Transparency obligations focus on providing explanations and disclosures rather than full access to proprietary code.
C) Incorrect. The AI Act does not give individuals the right to prohibit AI from being used in decision-making, but it does ensure oversight and transparency.
D) Incorrect. While data protection laws provide individuals with certain rights over their data, the AI Act does not grant a blanket right to request deletion of all data used by an AI system.

4 / 40
Anna, a compliance officer at a small or medium-sized enterprise (SME), is responsible for overseeing the implementation of a new AI system used for automating customer support. The company did not build this system but is buying the system from another provider. The AI system is classified as a high-risk AI system under the AI Act.

Anna has been asked to ensure the company complies with user obligations when deploying and monitoring this AI system. She must determine which actions must be prioritized and which actions should be avoided.

What should Anna **not** consider, given the obligations for AI users?

A) Developing the AI model's algorithms further to enhance its decision-making capabilities without involving its provider
B) Keeping detailed records of the AI system's performance and ensuring compliance with relevant reporting requirements
C) Monitoring the performance of the AI system to ensure it operates as intended and complies with safety standards
D) Reporting any serious incidents or malfunctions with the AI system to the appropriate authorities as is required by law

A) Correct. Anna should not attempt to independently develop the AI system's algorithm or modify its decision-making capabilities without the involvement of its provider. This is outside the scope of user obligations and could result in compliance breach or unintended consequences. Users are not responsible for altering the system's internal structure. (Literature: A, Chapter 1.1)
B) Incorrect. Keeping records and ensuring transparency aligns with the legal requirements for users of high-risk systems under the AI Act. This supports accountability and regulatory compliance.
C) Incorrect. Monitoring performance is a key obligation for users under the AI Act to ensure the AI operates as intended and does not pose any safety risks.
D) Incorrect. Reporting malfunctions or serious incidents is a key requirement for users of high-risk systems under the AI Act, to maintain compliance and address potential risks promptly.

5 / 40
An AI system for facial recognition is used for security purposes in public spaces. One organization is most relevant to overseeing compliance with data protection and privacy regulations, such as the General Data Protection Regulation (GDPR), for this AI system.

Which organization is that?

A) The European Consumer Organization (BEUC)
B) The European Artificial Intelligence Board (EAIB)
C) The European Court of Justice (ECJ)
D) The European Data Protection Board (EDPB)

A) Incorrect. The BEUC focuses on consumer rights, which are related to biometric and data protection for AI specific regulations.
B) Incorrect. The EAIB oversees compliance with the AI Act, focusing on AI-specific regulations. However, this question concerns data protection and privacy, which fall under the GDPR.
C) Incorrect. The ECJ addresses judicial matters, not AI regulations or biometric data.
D) Correct. The EDPB is responsible for ensuring consistent application of GDPR across European Union (EU) member states. It works with national data protection authorities to address issues like the use of biometric data in AI security systems. (Literature: A, Chapter 3.9, 3.10, 4.5)

6 / 40
A business develops an AI system for personalized marketing. This system uses machine learning (ML) algorithms to tailor advertisements to individual customers. During a compliance review, the team identifies the following risks:

- There is no documentation that clearly shows how the AI system handles data.
- The process of how the AI system makes personalized recommendations is not fully understood.
- Customers are complaining about these issues.

The company must comply with the AI Act. The business uses the ISO/IEC 42001 standard and the NIST AI Risk Management Framework (RMF) to accomplish that.

According to this standard and framework, what should the business do to resolve the issues?

A) Conduct a series of user experience (UX) tests to get feedback on usability, learnability, and customer preferences
B) Focus on improving the system's prediction accuracy to improve cost efficiency, customer satisfaction, and engagement
C) Implement a documentation process that details data sources, processing methods, and algorithmic decision-making
D) Upgrade the system's hardware to ensure faster processing, greater efficiency, and higher customer satisfaction

A) Incorrect. User experience tests provide valuable insights into system effectiveness but do not solve the underlying issue of lacking documentation and transparency in data and decision processes.
B) Incorrect. While improving prediction accuracy can enhance consumer satisfaction, it does not address the core issue of documentation and transparency in data handling and decision-making.
C) Correct. Implementing a comprehensive documentation process aligns with the ISO/IEC 42001 standard, which emphasizes transparency and documentation throughout the AI lifecycle. The NIST AI Risk Management Framework also supports this by promoting detailed records of data and decisions to ensure traceability and accountability. (Literature: B, Chapter 2.3)
D) Incorrect. Upgrading hardware may improve processing speeds but does not address the issues of transparency or documentation required for compliance with the AI Act.

7 / 40
A business develops an AI system to monitor patients who are hospitalized. The system uses high-definition cameras inside the patients' rooms to monitor the status of the patients in real time. If the system detects a patient is in distress, it automatically calls a nurse to the patient's bed.

To improve the performance of the AI system, the business wants to start building a database of videos of the patients with a note from a professional at critical points in the video, to build more training data for the system.

The business is considering doing a data protection impact assessment (DPIA). The team responsible is unsure if a DPIA should be done at all. If a DPIA is mandatory, the team wants to know when the assessment should be done: now or only after deployment of the update.

The business must comply with the AI Act and the General Data Protection Regulation (GDPR).

Should the business do a DPIA now?

A) Yes, because a DPIA is required for AI projects that could pose a high risk to the rights of natural persons.
B) Yes, because a DPIA is required for any project that collects personal data, even if the project is low risk.
C) No, because a DPIA is not required for using data for training purposes, education, or scientific research.
D) No, because a DPIA is only required after the AI system has been fully developed, tested, and deployed.

A) Correct. This option accurately reflects the requirements under the GDPR. A DPIA is necessary when processing operations are likely to result in a high risk to the rights and freedoms of natural persons, especially when using new technologies like AI systems that process (highly) sensitive data such as patient videos. These fall under the category health-related data, requiring extra safeguards. (Literature: A, Chapter 4.5)
B) Incorrect. While a DPIA is important, it is not automatically required for all projects that collect personal data. The GDPR mandates a DPIA particularly when the data processing is likely to result in high risks to individuals' rights and freedoms, not simply due to the collection of personal data, such as biometric data, health data, or large-scale monitoring.
C) Incorrect. The purpose of data use (for example, training or research) does not exempt a project from the requirement to undertake a DPIA. The GDPR still applies, particularly when the processing could result in high risks to individuals, especially when sensitive data such as patient videos is involved.
D) Incorrect. A DPIA should be conducted before processing begins, particularly during the planning and development stages of a project to identify and mitigate risks proactively. Waiting until after deployment could lead to non-compliance with the GDPR.

8 / 40
A business develops an AI system for real-time facial recognition. A private security firm deploys the AI system to monitor a public shopping mall. The system scans all visitors, cross-checks them with databases of past offenders and political activists, and flags visitors that are listed in one of those databases. Visitors that are flagged are covertly tracked throughout their visit to assess whether they engage in what the security firm finds suspicious behavior.

According to the AI Act, in which category should the use of this AI system be classified?

A) Unacceptable risk
B) High risk
C) Limited risk
D) Minimal or no risk

A) Correct. Real-time biometric identification in public to track individuals based on political activity is prohibited under Article 5 of the AI Act. The Act bans AI systems used for untargeted surveillance and social scoring that infringe on fundamental rights. (Literature: A, Chapter 3.3, 3.4; AI Act, Article 5(1)(d))
B) Incorrect. The system is not just high-risk, but falls under the category of unacceptable risk, because the system uses political activity to track individuals, and without their consent. That is a prohibited use of AI system.
C) Incorrect. Limited-risk covers systems like chatbots or emotion detection tools with transparency obligations. This case involves biometric surveillance with serious rights implications and does not qualify.
D) Incorrect. Minimal-risk applies to low-impact systems like spam filters. Facial recognition used for tracking exceeds this risk level and is explicitly prohibited.

9 / 40
A travel agency uses an AI system to develop dynamic, targeted marketing campaigns for their vacation packages. These campaigns include real-time advertisement placements on social media and travel platforms, using the individuals' browsing history. The travel agency uses AI to infer the user's emotional state and then suggests customized destinations and activities.

The travel agency must comply with the AI Act.

What risk must the travel agency address?

A) The risk of including potential biases. They should update the training data regularly to avoid suggesting irrelevant destinations or infer wrong emotional states.
B) The risk of ineffective advertising activities. They should focus on updating the algorithm, because the AI Act does not cover personalized advertisements.
C) The risk of lack of transparency. They should guarantee openness about the AI, reduce bias in suggestions, and evaluate if the advertising activities are ethical.
D) The risk of misusing personal data. They should stop using AI-driven personalization because the AI Act forbids using personal data for targeted advertising.

A) Incorrect. The biases meant are biases that disadvantage certain groups of customers. An irrelevant travel destination suggestion is unlikely to have much impact on the customers.
B) Incorrect. Though the AI Act gives high-risk AI applications top priority, its clauses also apply to commercial sectors, like advertising and tourism, especially when customer profiling and decision-making are involved.
C) Correct. Under the AI Act, this captures the main obligations. Agencies must solve transparency by telling consumers about AI involvement, prevent bias, and guarantee that advertising tactics follow ethical standards. (Literature: A, Chapter 7.8, 7.9)
D) Incorrect. The AI Act does not expressly forbid tailored advertising or AI-driven personalizing. Rather, it provides guidelines for moral behavior, which calls for openness, justice, and data security to make sure such methods follow the European Union's (EU) values.

10 / 40
A company developed an AI model that can be used in various industries, including healthcare and finance. Due to its wide application, the AI model carries potential risks to public health.

What did the company develop, and which practices should the company implement according to the AI Act?

A) The company developed a general-purpose AI (GPAI) that carries systemic risks. It should conduct additional tests to mitigate the risks.
B) The company developed a high-risk AI system. It should implement all the requirements for high-risk AI systems as outlined in the AI Act.
C) The company developed a narrow AI model. It should ensure the model operates only within predefined parameters to prevent risks.
D) The company developed an experimental AI model. It should focus on research and development without immediate risk management.

A) Correct. The company developed a GPAI model that carries systemic risks. The company should do an additional model assessment using protocols and state-of-the-art tools. This includes the implementation and documentation of security tests. (Literature: A, Chapter 3.7; AI Act, Article 3, Article 55)
B) Incorrect. While the AI model carries potential risks, it is classified as a GPAI not specifically as a high-risk system.
C) Incorrect. A narrow AI model is limited to specific tasks and does not carry the systemic risks associated with GPAI.
D) Incorrect. Even experimental AI models must adhere to risk management practices if they pose potential systemic risks.

11 / 40
An organization develops a high-risk AI system. During testing, the development team identifies various risks, including inconsistencies in data completeness and the presence of outdated records. These risks could negatively impact the model's performance.

The organization must comply with the AI Act. They use the CEN/CLC/TR 18115 framework to do so.

According to this framework, what should the organization do to address these risks?

A) Conduct a data protection impact assessment (DPIA) to address the fairness of AI decision-making
B) Encrypt all training and testing datasets using protocols to prevent unauthorized access to personal data
C) Implement general-purpose risk controls to reduce the mentioned operational and reputational risks
D) Improve the data quality by applying structured quality metrics and statistical evaluation methods

A) Incorrect. A DPIA is useful for assessing risks to individuals' rights and freedoms. However, it is not the appropriate tool to directly address problems with outdated or incomplete data. Data quality improvements require technical measures, not a legal assessment.
B) Incorrect. While encryption is important for data security, this does not address data quality issues like completeness and timeliness. Article 10 of the AI Act does not only emphasize the protection of data, but also ensures that the data used for AI training and testing is relevant, representative, and of high quality.
C) Incorrect. Although risk management is of great importance in AI, it does not provide the data quality framework needed to solve the identified issues. Managing data completeness and timeliness is done by increasing data quality, not by general AI risk standards.
D) Correct. CEN/CLC/TR 18115 provides guidance on evaluating and improving data quality throughout the lifecycle of AI systems. It emphasizes the use of metrics for characteristics like completeness and timeliness, especially during data preparation, to ensure compliance with Article 10 of the AI Act. (Literature: B, Chapter 1; AI Act, Article 10)

12 / 40
The AI Act describes several roles connected to an AI system.

What is the definition of the role 'importer of an AI system'?

A) A person or organization that designs, develops, and markets an AI system under their own name or trademark.
B) A person or organization that places an AI system on the market but is not responsible for its original development.
C) A person or organization that uses an AI system in their operations and ensures local compliance with user obligations.
D) A regulatory authority tasked with monitoring if the AI system is imported in compliance with the AI Act regulations.

A) Incorrect. This describes the role 'provider', who is responsible for the development and marketing of the AI system, not for importing them.
B) Correct. This is the definition of the role 'importer', typically when the system is developed outside of the European Union (EU). Importers are responsible for ensuring the system meets EU regulatory requirements and working with providers to demonstrate compliance. (Literature: A, Chapter 3.1)
C) Incorrect. This describes the role 'user', who operates and monitors the AI system, not an importer.
D) Incorrect. Regulatory authorities are not importers. They are responsible for enforcing compliance but do not actively participate in placing systems on the market.

13 / 40
A business develops an AI system for fraud detection in financial transactions. This system analyzes transaction patterns to identify suspicious activities and prevent fraudulent behavior. Given the potential for false positives that could impact legitimate transactions and the evolving nature of fraud tactics, the business recognizes the need for effective safeguards.

The business must comply with the AI Act. To help prevent issues concerning false positives, the business uses the ISO/IEC 23894 standard.

According to this standard, what should the business do to prevent these issues?

A) Embed risk management into all activities to ensure comprehensive oversight and proactive risk mitigation
B) Enhance data privacy measures to protect sensitive information and comply with privacy regulations
C) Focus on improving model accuracy to ensure reliable performance and minimize false positives
D) Implement cybersecurity measures to protect the system from external threats and unauthorized access

A) Correct. This approach integrates risk management throughout the organization, customizing frameworks to fit specific contexts and involving stakeholders to effectively identify and mitigate AI-related risks. This follows the ISO/IEC 23894 standard and helps most with compliance. (Literature: B, Chapter 3.2)
B) Incorrect. The business must address important privacy concerns. However, this does not specifically integrate the comprehensive risk management practices required for AI as outlined in the ISO/IEC 23894 standard, which would be necessary for compliance.
C) Incorrect. By focusing on improving model accuracy to ensure reliable performance and minimize false positives, the business enhances model effectiveness but does not address the broader aspects of risk management, such as identifying, assessing, and mitigating potential AI-related risks. The ISO/IEC 23894 standard emphasizes a comprehensive approach to risk management.
D) Incorrect. By implementing cybersecurity measures to protect the system from external threats and unauthorized access, the business addresses a key component of system security. However, this does not encompass the full scope of risk management practices required for AI, as specified in the ISO/IEC 23894 standard.

14 / 40
A manufacturing company uses robotic devices driven by AI for quality control on its assembly lines. The investigative team notes that an anonymous whistleblower claims the AI system lately shows an unusually low number of faulty products. The reason for the underreporting of faulty products is a software update of the AI system. Upon manual inspection, the products are faulty and unsafe to use.

The report states that the new defect detection algorithm produces a crucial error that causes the false negatives. According to the whistleblower, managers knew about the issue but did not address the issue, to avoid damaging the company's reputation.

What should the next actions be?

A) - Adjust the internal algorithm to address the problem
- Notify the relevant competent authority if the issue still exists after 30 days

B) - Investigate the problem internally and start solving it
- Notify the relevant competent authority of the occurrence immediately

C) - Research the whistleblower's reasons for reporting
- Notify the relevant competent authority if consumers start complaining

D) - Stop using the AI system and switch to an older method
- This makes it unnecessary to inform the relevant competent authority

A) Incorrect. Addressing the problem without notifying an authority avoids the legal requirement to report serious incidents. Penalties and mistrust of the company's handling of AI systems could follow from not reporting.

B) Correct. Investigating guarantees that the underlying cause of the issue is known and addressed. Reporting to the relevant competent authority guarantees compliance. (Literature: A, Chapter 7.4, 3.10; AI Act, Article 73)

C) Incorrect. Investigating a whistleblower's motives is a breach of whistleblower protection principles and discourages ethical reporting. This approach prioritizes reputational management over legal and ethical obligations, violating AI Act requirements and organizational integrity.

D) Incorrect. Although stopping the AI system might solve the problem, it does not satisfy the reporting criteria specified in the AI Act. This choice is unacceptable, because this was a serious incident that affects product safety, which must be reported as well as addressed.

15 / 40
MedTech Diagnostics uses a high-risk AI system for diagnosing medical conditions from X-ray images. They have the following in place:

- The company has passed an external audit to ensure the AI system adheres to the AI Act's standards.
- A robust risk management framework identifies and mitigates potential issues, with contingency plans in place.
- Detailed records of the AI system's operations are securely stored for accountability and audits.
- Clear documentation and training are provided to users, explaining AI decision-making and limitations.
- All AI-generated diagnoses are reviewed by medical professionals before being finalized, integrating human judgment.

What else should the company implement?

A) They should add robust data governance procedures to maintain the reliability and fairness of their AI system.
B) They should ensure that the AI system can operate independently without any human intervention for efficiency.
C) They should implement a system to automatically override human decisions to speed up the diagnosis process.
D) They should include a feature that allows patients to directly modify their medical records based on AI suggestions.

A) Correct. Robust data and data governance cover the quality, bias mitigation and traceability of training and operational data, ensuring the system is fair and reliable. (Literature: A, Chapter 3.3; AI Act, Article 15)
B) Incorrect. Full automation in medical diagnosis is not allowed under the AI Act. High-risk AI systems in healthcare require human oversight to ensure safety and accuracy, making full independence inappropriate. Human review is essential for patient safety and regulatory compliance.
C) Incorrect. Automatically overriding human decisions can compromise patient safety and undermine the essential role of human oversight in high-risk AI systems like medical diagnosis.
D) Incorrect. Allowing patients to modify medical records based on AI suggestions could lead to inaccuracies, and is not aligned with standard medical practices, which require professional oversight, and leads to legal risks.

16 / 40
An insurance company implements a new AI-based credit scoring system with access to both internal databases and public databases. The following risks are identified:

- **A lack of proper training data**. If the model is not trained well, it will be difficult to accurately determine a fair score for people.
- **Integration with other applications**. It will be difficult to integrate the AI-based engine into the rather complex and at some points outdated application environment.
- **Non-compliance with the GDPR**. The General Data Protection Regulation (GDPR) has specific requirements for the autonomous processing of personal data by automated systems.
- **Transparency and quality of the model**. Both the employees and the customers must be able to understand the results and decisions of the AI model.

The insurance company must comply with the AI Act.

Which risk is **not** important for compliance with the AI Act?

A) A lack of proper training data
B) Integration with other applications
C) Non-compliance with the GDPR
D) Transparency and quality of the model

A) Incorrect. AI systems must use high-quality, unbiased data to prevent discrimination or unfair decisions. Poor training data could lead to biased or inaccurate credit scores, violating AI Act requirements.
B) Correct. Integration with other applications that does not work well is certainly a risk, but not one defined in the AI Act. (Literature: A, Chapter 7.2, 7.3)
C) Incorrect. The GDPR provides specific constraints for systems that process personal data autonomously, but this is not the main challenge that must be addressed. The AI Act aligns with the GDPR, particularly regarding the processing of personal data, lawful basis for AI decisions, and individual rights (for example: the right to explanation and appeal).
D) Incorrect. Data quality and AI model accuracy are the main challenges to be addressed in this type of application projects. It is also essential that the output of the AI model is comprehensible and explainable. The AI Act requires explainability and transparency, especially for high-risk AI systems like credit scoring, where AI decisions impact financial access.

17 / 40
A government agency proposes an AI system to help with predicting crime hotspots around the downtown area of a larger town. The system will be used for automated surveillance. It is programmed to automatically identify persons that display suspicious behavior and report them to the local police. This is a great opportunity for preventing crime, increasing feelings of safety, and ensuring justice after crime.

Are there any risks related to implementing this AI system?

A) Yes, because an AI system that is used for automated decisions carries the inherent risk of bias, which may unfairly disadvantage individuals.
B) Yes, because the AI Act foresees so many privacy risks with surveillance systems that it outright forbids its employment in public spaces.
C) No, because in crime prosecution and prevention, AI systems carry no particular risks since they are used to enhance public safety.
D) No, because public domain AI systems boost efficiency and carry no risk, since the decisions are objective and free from human error.

A) Correct. The AI Act specifically mentions this main concern. In sensitive fields like crime prosecution, the possibility of biased data or faulty algorithms in AI systems can produce discriminating results. For AI systems in high-risk applications, the AI Act requires openness, risk evaluations, and bias mitigation techniques. (Literature: A, Chapter 8.1, 8.2, 8.3)
B) Incorrect. The AI Act aims to control and guarantee the safe, open, and fair use of AI rather than deter its use in public domains. While enforcing protections to handle hazards, the AI Act stimulates creativity.
C) Incorrect. Increasing public safety is a noble goal, but it does not negate the obligation to mitigate risks to privacy and disadvantaging individuals that are not misbehaving in public.
D) Incorrect. AI outputs rely on the training data and algorithms applied, so any bias from the training data carries over into the decisions the system will make. They are not necessarily more objective than human judgement. In addition, the AI Act gives individuals the right to have decisions made about them overseen by a human.

18 / 40
An organization develops an AI system for recruitment purposes. During internal testing, the team identified a risk: the system sometimes unintentionally favored candidates from certain backgrounds, leading to potentially discriminatory outcomes. The team is now unsure how to structure their response to these concerns.

The organization must comply with the AI Act. To help mitigate the risk, the organization uses the ISO/IEC TR 24368 standard.

According to this standard, what should the organization do to mitigate this risk?

A) Adjust the algorithm to prioritize demographic quotas based on employment statistics
B) Adopt a zero-data approach by removing all demographic data from the training set
C) Apply cybersecurity measures to protect candidate data and enhance system integrity
D) Implement a stakeholder engagement process to identify and mitigate potential biases

A) Incorrect. While aiming to balance representation may seem ethical, applying rigid quotas without context may introduce new biases. ISO/IEC TR 24368 emphasizes fairness and stakeholder involvement over arbitrary demographic targets.
B) Incorrect. Simply removing demographic data does not prevent discrimination and can even obscure existing biases. ISO/IEC TR 24368 encourages transparent methods and bias mitigation, not blind data removal.
C) Incorrect. While cybersecurity is important, it does not encompass ethical issues like bias or fairness. Addressing ethical concerns require approaches aligned with ISO/IEC TR 24368.
D) Correct. ISO/IEC TR 24368 promotes stakeholder engagement to uncover ethical risks, like bias, and develop inclusive, fair AI systems. This supports the AI Act's goals around fairness and non-discrimination. (Literature: B, Chapter 4)

19 / 40
An organization develops an AI system for loan approval. During internal testing, the compliance team finds a risk: they find a lack of transparency in how the model makes decisions, as well as limited documentation for risk evaluation.

The organization must comply with the AI Act. The organization uses the ISO/IEC 42001 standard and the NIST AI Risk Management Framework (RMF) to accomplish that.

According to this standard and framework, what should the business do to address this risk?

A) Conduct a safety compliance assessment based on recommended cybersecurity guidelines
B) Decommission the AI system immediately and transition to a manual loan approval process
C) Define a measurement plan with transparency metrics and record decision logic for oversight
D) Rebuild the system using synthetic data to eliminate as many sources of bias as possible

A) Incorrect. Adhering to security guidelines does not specifically address transparency or risk documentation. Therefore, it is not directly relevant to the identified issue.
B) Incorrect. There is no need to decommission the system, because it is only in internal testing. Switching to manual loan approvals would avoid the problem, but it would also result in the loss of all investment costs. The risk can be managed through structured governance.
C) Correct. ISO/IEC 42001 emphasizes transparent and explainable decision-making, along with thorough documentation across the AI lifecycle. The NIST AI RMF supports defining metrics through its Measure function and promoting traceability. Together, these approaches directly address the issues presented in the scenario. (Literature: B, Chapter 2.2, 2.5)
D) Incorrect. Using synthetic data alone does not ensure bias mitigation and fails to address core requirements around transparency and risk documentation.

20 / 40
A leading automotive manufacturer has developed a highly automated vehicle (level 4) equipped with an AI-based object recognition technology for road safety. During testing, the following risks are discovered:

- The system's ability to detect speed bumps is compromised under low-light conditions.
- It might be hard to sell the model, because it does not know dimensions of other vehicles.
- The developers are not quite sure how to explain how the model makes decisions.
- Not all stakeholders were asked for input during the development phase of the AI system.

When **only** looking at AI Act compliance, what must be addressed?

A) The risk of insufficient testing under real-world conditions
B) The risk of lack of transparency in AI decision-making
C) The risk of limited scalability of the AI system to other vehicle models
D) The risk of limited stakeholder involvement during AI development

A) Incorrect. The AI Act focuses more on mitigating identified risks and ensuring transparency and fundamental rights, rather than addressing insufficient real-world testing.
B) Correct. Article 11 of the AI Act emphasizes transparency in AI systems to identify and rectify potential risks, which is the central issue in this scenario. (Literature: A, Chapter 7.10)
C) Incorrect. While scalability is crucial commercially, it doesn't directly address the AI Act's requirements for risk mitigation and transparency.
D) Incorrect. Although stakeholder involvement is important, it is not the focus of the AI Act.

21 / 40
A logistics company is building an AI system to optimize its delivery paths and lower fuel usage. The organization is weighing two choices:

- A closed-source AI model from a vendor who guarantees speedier installation and verified compliance certifications.
- An open-source AI model that allows for great customizing and transparency.

The company must comply with the AI Act but also wants to balance innovation and cost.

Which model suits this company **best**?

A) A closed-source AI model, because it is intrinsically more secure and trusted by authorities. This reduces the possibility of non-compliance.
B) A closed-source AI model, because it provides pre-certified compliance. This lessens the company's burden of proving AI Act compliance.
C) An open-source AI model, because it guarantees complete transparency. This helps with documentation and auditability requirements.
D) An open-source AI model, because it is excepted from AI Act compliance. This is due to the source code being publicly available.

A) Incorrect. Closed-source approaches are not by nature more compliant or safe.
B) Incorrect. Though closed-source models can include compliance certifications, they might lack the flexibility and openness required to fit company needs or changing legal requirements.
C) Correct. Full transparency offered by open-source models fits the criteria of the AI Act for auditability, traceability, and risk control. These advantages let the logistics firm show compliance more easily. (Literature: A, Chapter 6)
D) Incorrect. Under the AI Act, open-source models are not free from compliance responsibilities.

22 / 40
The AI Act defines ethical principles for AI development.

What is **not** one of those principles?

A) Explicability
B) Fairness
C) Loss prevention
D) Respect for AI autonomy

A) Incorrect. This is a principle in the AI Act. It requires AI systems to be transparent and understandable, ensuring that users and stakeholders can comprehend how decisions are made and the rationale behind them.
B) Incorrect. This is a principle in the AI Act. It mandates that AI systems should be developed and deployed to operate without bias or discrimination, ensuring equitable and just outcomes for all individuals.
C) Incorrect. This is a principle in the AI Act. It emphasizes the importance of designing AI systems to minimize risks and prevent harm, ensuring safety and security for users and those impacted by AI technologies.
D) Correct. The correct principle is respect for human autonomy. The AI Act primarily focuses on principles such as fairness, loss prevention, and explicability, which aim to ensure that AI systems are developed and used responsibly, transparently, and without bias. (Literature: A, Chapter 9.1)

23 / 40
A startup develops an AI system to assist with personalized learning in schools by tailoring lesson plans to individual students' needs. The system collects data on students' performance and learning behaviors.

According to the AI Act, what should the startup consider here, to balance innovation with regulation?

A) Avoid labeling the system as high-risk to circumvent additional regulatory burdens and streamline innovation
B) Ensure the AI system undergoes a conformity assessment and complies with high-risk system regulations
C) Implement robust data protection features but take out user notifications to avoid delays in deployment
D) Market the system to private schools exclusively to limit the impact of high-risk compliance requirements

A) Incorrect. Mislabeling the system to avoid regulations is unethical and can lead to serious legal repercussions.
B) Correct. Conducting a conformity assessment and ensuring transparency are crucial for compliance with high-risk system regulations. (Literature: A, Chapter 7.6; AI Act, Article 6, Annex III)
C) Incorrect. User notifications are essential for transparency and compliance with data protection regulations.
D) Incorrect. Compliance is not necessarily more lenient in private schools, and regulations must be followed regardless of the market.

24 / 40
A financial institution, Fintegra, is implementing an AI system to detect fraud in transactions. The system requires access to customers' transaction information and demographic data for its analysis. Fintegra must comply with the AI Act's data minimization requirement.

What is the **best** way for Fintegra to comply with the data minimization requirement?

A) They should anonymize all transaction data and remove any data that identifies a natural person to comply with the requirement, even if that data is critical for fraud detection purposes.
B) They should collect all personal details, including full name and precise address, to ensure precise analysis and improvement over time, and securely store the data as long as needed.
C) They should limit data collection to transaction data that is relevant to detecting fraud, and avoid processing personal details, such as the customers' full name or precise address.
D) They should share the collected data only with recognized vendors compliant with the AI Act, which minimizes internal handling of personal details, like the customer's full name.

A) Incorrect. While anonymization is important, removing critical data required for fraud detection undermines the AI system's effectiveness and is not required by the principle of data minimization under the AI Act.
B) Incorrect. Collecting and storing all available data, even when done securely, violates the principle of data minimization and increases the risk of non-compliance with the AI Act.
C) Correct. The principle of data minimization under the AI Act requires organizations to collect and process only data that is strictly necessary for the specific purpose of the AI system. By focusing on transaction data relevant to fraud detection and avoiding any unnecessary personal details, the company complies with this requirement. (Literature: A, Chapter 4.1)
D) Incorrect. This is not a good option, as sharing data with external vendors may breach data protection rules. Even if Fintegra and the vendor are both compliant with the AI Act, this does not align with minimizing data usage either.

25 / 40
EduTech is implementing an adaptive learning platform that uses AI to personalize learning paths for students. The platform adjusts the difficulty of tasks based on individual performance.

What risk should EduTech mitigate to ensure the ethical use of this AI system?

A) The risk of bias and discrimination, because these would lead to unfair advantages or disadvantages for certain students. This risk is mitigated by regularly reviewing and updating the AI system's data sets and algorithms.
B) The risk of over-reliance on technology, which could result in students not developing critical thinking skills. This risk is mitigated by keeping the AI system's decision-making process confidential to stimulate students to think more.
C) The risk of privacy breaches, because sensitive student data, including their performance could be mishandled or exposed. This risk is mitigated by focusing more on improving the technical performance of the AI system.
D) The risk of transparency issues, because students and educators may not understand how decisions are made. This risk is mitigated by ensuring that the AI system operates without human oversight, which ensures fairness.

A) Correct. Bias and discrimination are big risks in education. Regularly reviewing and updating data sets and algorithms helps mitigate the risk of bias and discrimination. (Literature: A, Chapter 7.6)
B) Incorrect. Transparency is crucial for ethical AI use. Fostering critical thinking is important in education, but it has nothing to do with transparency of AI systems.
C) Incorrect. Technical performance alone does not address ethical concerns, nor does it decrease the risk of privacy breaches.
D) Incorrect. Although decisions without human intervention can increase fairness, a lack of human oversight for AI increases the risk of bias and discrimination. Human oversight is essential to ensure ethical use.

26 / 40
A hospital department specializes in the diagnosis and treatment diseases. They develop an AI diagnostic system to assist in identifying rare diagnoses. The system analyses patient data, medical history, and imaging scans.

The system is successfully adopted in the United States (US). Some medical specialists in the European Union (EU) want to adopt the system, but they do not have clear understanding of how the AI system works. They also do not have special knowledge and experience in monitoring AI or recognizing malfunctions or misdiagnoses.

What is **not** a risk associated with the adoption of this AI system?

A) The risk of lack of effective human supervision
B) The risk of misdiagnosis due to automation bias
C) The risk of mistrust caused by lack of transparency
D) The risk of unauthorized access to patient records

A) Incorrect. Due to the lack of specialist knowledge of the team using the system, they may not be able to monitor AI and recognize malfunctions or inaccurate output.
B) Incorrect. Due to lack of specialist knowledge on how to correctly interpret the output, biases and misdiagnoses may occur.
C) Incorrect. The medical specialists do not understand how the AI system works, which may lead to mistrust due to lack of transparency.
D) Correct. While data privacy and unauthorized access are important concerns, they are not specifically highlighted as risks related to the operational adoption and understanding of the AI diagnostic system in this scenario. (Literature: A, Chapter 7.7)

27 / 40
A business makes an AI system for smart home assistants. During testing, the team finds that voice recognition errors, such as confusing similar-sounding words, lead to unintended actions, like turning on the wrong appliance. These mistakes can cause privacy breaches, such as recording conversations without consent or misidentifying users, potentially sharing sensitive information with unauthorized parties.

The organization must comply with the AI Act. They use the CEN/CLC/TR 18115 framework to do so.

According to this framework, what should the AI provider do to address the issue?

A) Create a stakeholder engagement plan to get different views on how the AI system works
B) Do an ethical impact assessment to understand privacy risks of smart home assistants
C) Improve the training data quality by using systematic validation and error-checking methods
D) Increase data security with encryption to protect voice data and prevent data breaches

A) Incorrect. Engaging stakeholders is beneficial for understanding broader implications, but it does not address the immediate technical need for improving data quality.
B) Incorrect. While ethical impact assessments are important, they do not solve the issue of low-quality data that causes the misinterpretations.
C) Correct. Enhancing data quality through systematic validation and error-checking aligns with the CEN/CLC/TR 18115 framework, addressing the need for accurate and complete data to ensure safe and effective AI system performance. (Literature: B, Chapter 1)
D) Incorrect. Although data security is important, encryption does not address the problem with data quality, which is central to this scenario.

28 / 40
A technology company was found to be using an AI system for real-time remote biometric identification, which is explicitly prohibited by the AI Act.

What is the appropriate penalty for this violation?

A) A formal warning without financial penalties
B) An administrative fine of up to €7.5 million or 1% of the total global annual turnover in the previous financial year
C) An administrative fine of up to €15 million or 3% of the total global annual turnover in the previous financial year
D) An administrative fine of up to €35 million or 7% of the total global annual turnover in the previous financial year

A) Incorrect. A formal warning without a financial penalty is not adequate for a serious breach of AI regulations.
B) Incorrect. This fine is too low for a violation involving prohibited actions by a company.
C) Incorrect. While substantial, this fine does not match the severity of such a serious breach.
D) Correct. This penalty aligns with the maximum possible fine for the most severe violations under the AI regulation. (Literature: A, Chapter 3.11; AI Act, Article 52, Article 99)

29 / 40
The AI Act particularly emphasizes the importance of two aspects of AI systems: transparency and traceability.

Why are transparency and traceability important?

A) Because they are crucial for ensuring accountability and fostering trust in AI systems.
B) Because they are mandatory requirements for all products, including AI systems.
C) Because they are particularly essential for the reliability and automation of AI systems.
D) Because they are shared between European, Chinese, and American legislation.

A) Correct. Detailed information about the data used helps to understand, explain, and comprehend the decisions and actions of an AI system. Traceability ensures that AI decision-making processes, datasets, and system operations can be reviewed and audited. This is crucial for identifying biases, errors, and accountability issues. Transparency and traceability are important for the accountability and trust of users in the AI systems. (Literature: A, Chapter 3.1)
B) Incorrect. While transparency and traceability are important for AI systems, they are not mandatory for all products.
C) Incorrect. Transparency and traceability are important for the accountability and trust (not reliability) of European Union (EU) citizens and users in the AI systems and technologies. Reliability and automation are more related to AI system performance and robustness, not necessarily these two principles.
D) Incorrect. Consistency and homogeneity among the three major global regulations on AI is not an aspect taken into consideration by the European Union (EU). The AI Act is a European regulation. China and the United States have different focuses and legal frameworks.

30 / 40
An AI system, used by a retail organization, automatically changes the way elements of the website are displayed based on user preferences and device used. The system recommends products and enhances user experience using click history and time spent on a page.

According to the AI Act, in which category should the use of this AI system be classified?

A) Unacceptable risk
B) High risk
C) Limited risk
D) Minimal or no risk

A) Incorrect. The system falls short of the standards for unacceptable risk, which relates to AI systems endangering human dignity, safety, or basic rights. Influencing buying decisions within a retail environment is not intrinsically harmful.
B) Incorrect. AI systems in fields like healthcare, banking, or employment where major rights or safety concerns are likely, are considered high-risk. The way this technology uses non-sensitive data to enhance website appearance does not satisfy the high-risk criteria.
C) Incorrect. Although the system influences consumer choices, its modest impact and use of non-sensitive data more closely relate with the minimal or no-risk classification.
D) Correct. The system employs non-sensitive data, runs in a low-stakes setting, and only affects users' purchasing experience, so it is categorized as either little or no risk. (Literature: A, Chapter 3.3, 3.4)

31 / 40
A company creates an AI system for automated decision-making in its hiring process. The AI system will screen resumes, rank candidates, and make recommendations for interviews.

The company is worried that the AI system may have biases that could affect the hiring process.

What is the **best** approach for the company to mitigate biases in the AI system?

A) Allow the AI system to learn and adapt without further human intervention
B) Ignore biases in the training data and focus on the AI system's performance
C) Implement a diverse development team to create and monitor the AI system
D) Use a single source of data for training the AI system to ensure consistency

A) Incorrect. Allowing the AI system to learn without human intervention can lead to unintended biases and lack of accountability. (AI Act, Guideline 65)
B) Incorrect. Ignoring biases can lead to discriminatory outcomes and is not compliant with ethical guidelines. The system must learn to recognize and adjust for the biases. (AI Act, Guideline 72)
C) Correct. A diverse team can help identify and mitigate biases, ensuring the AI system is fair and inclusive. (Literature: A, Chapter 4.5; AI Act, Guideline 81)
D) Incorrect. Using a single source of data can limit the AI system's ability to generalize and may introduce biases. (AI Act, Guideline 73)

32 / 40
Feline Finesse is a webshop that sells cat accessories and cat pillows, including personalized cat plushies based on customer pictures. The webshop uses an AI system that can do the following things:

- It dynamically changes prices depending on consumer activity.
- It ranks search results, based on customer preferences.
- It gives personal recommendations for other products it thinks the customer likes.

Currently, the webshop makes customers aware of what the AI system does and is very transparent about how the algorithm works. However, the CEO questions this practice and wants to know what degree of transparency is required and how it affects sales.

With reference to the AI Act, what should the CEO know about transparency?

A) Transparency can prove to consumers that the system is objective. Consumers have a right under the AI Act to understand how their data is used and this understanding fosters trust.
B) Transparency can show the limits or constraints of the AI system. Consumers may lose trust in the company after understanding this, which damages the company's reputation.
C) Transparency is not mandated for e-commerce. Consumers are helped by the convenience of personalization and do not need knowledge or understanding of how the AI system operates.
D) Transparency is restricted to making the source code of the AI system available. Consumers' confidence in the system may decrease from understanding how the algorithm works exactly.

A) Correct. A pillar of the AI Act and a major determinant of public confidence is transparency. (Literature: A, Chapter 3.6)
B) Incorrect. Though it is part of transparency, revealing constraints is not meant to lower trust. It is meant to build trust by guaranteeing responsibility and realistic expectations.
C) Incorrect. While convenience is nice for most consumers, the AI Act legally mandates transparency. Consumers are growingly conscious of and worried about ethical AI methods. Transparency, therefore, promotes confidence in the system.
D) Incorrect. Transparency is not limited to making source code public. It includes clearly outlining the AI's operational policies, data-usage, and decision-making. Building trust and guaranteeing responsibility depend on this.

33 / 40
A high-risk AI system is used in the recruitment process, automatically filtering candidates based on their qualifications. However, the deployer has not implemented any mechanism for human intervention or oversight in cases of questionable decisions.

According to the AI Act, does this system require human oversight?

A) Yes, because human oversight is necessary for intervention in decision-making processes.
B) Yes, because human oversight ensures compliance with fairness and transparency obligations.
C) No, because automated systems are designed to function without human intervention.
D) No, because recruitment processes do not involve critical safety risks to natural persons.

A) Correct. The AI Act emphasizes the importance of human oversight for high-risk AI systems to ensure that there is a mechanism for human intervention, especially in scenarios where decisions may be questionable or have significant impacts on individuals. (Literature: A, Chapter 10.2.3)
B) Incorrect. While fairness and transparency are important aspects of the AI Act, human oversight is only required when there is limited or high-risk.
C) Incorrect. The AI Act emphasizes the importance of human oversight for high-risk AI systems to ensure that there is a mechanism for human intervention, especially in scenarios where decisions may be questionable or have significant impacts on individuals.
D) Incorrect. While recruitment may not involve safety risks, the AI Act considers the ethical and societal implications of AI systems. Human oversight is required to address concerns related to fairness and transparency, which are critical in recruitment processes.

34 / 40
A company prepares to launch a general-purpose AI (GPAI) model. The model can be adapted for tasks such as customer service automation, content creation, and data analysis. The company is based outside the European Union (EU) but plans to distribute the model across several EU member states.

According to the AI Act, what is **not** required before distributing the GPAI model in the EU?

A) Appoint an authorized representative in the EU to handle compliance matters
B) Comply with EU copyright regulations for model training with copyrighted data
C) Conduct a thorough audit to verify full conformity with all EU laws and regulations
D) Publish a detailed summary of the content used for training the GPAI model

A) Incorrect. Any provider based outside the EU must appoint an authorized representative in the EU to handle compliance matters. (AI Act, Article 54)
B) Incorrect. Even though GPAI models do not require a full conformity assessment, they must still comply with EU copyright laws, ensuring that protected content used in training respects legal requirements. (AI Act, Article 53(1)(c))
C) Correct. A full conformity assessment is required only for high-risk AI systems, and general-purpose AI models do not fall under the high-risk category. Therefore, the company is not required to conduct a full conformity assessment. (Literature: A, Chapter 3)
D) Incorrect. According to the AI Act, a summary of the data used for training the model must be published. This ensures transparency. (AI Act, Article 53)

35 / 40
An organization deploys an AI system for predictive maintenance for industrial equipment. After several months of operation, the system generates a very high number of false alerts, disrupting workflows. An investigation shows the following:

- The organization did not consider the dynamic environmental changes on the work floor.
- The organization lacks a formal process for reassessing risks after deployment.

The organization must comply with the AI Act. To help solve these issues, the organization uses the ISO/IEC 23894 standard.

According to this standard, what should the organization do to address these issues?

A) Conduct a human-centered design workshop to improve system usability
B) Design a risk management process with ongoing evaluation and monitoring
C) Perform a cybersecurity audit to identify and address possible vulnerabilities
D) Replace the AI system with a simpler, rule-based model for easier control

A) Incorrect. While human-centered design improves usability, it does not address the root cause: a lack of dynamic and adaptive risk management for deployed AI systems.
B) Correct. ISO/IEC 23894 highlights the importance of embedding dynamic, ongoing risk management throughout the AI lifecycle, including post-deployment. A re-evaluation could have adjusted the system before the high number of false alerts was generated. (Literature: B, Chapter 3.2, 3.4)
C) Incorrect. It is unlikely that cybersecurity causes the false alerts. This solution does not address lifecycle risk management or the need for continuous re-evaluation of the AI system.
D) Incorrect. Replacing the system ignores ISO/IEC 23894's emphasis on treating and reassessing risks iteratively, rather than abandoning the technology.

36 / 40
An AI system is used by a car fleet management company to track driver behavior and forecast maintenance requirements. Large volumes of data, such as GPS locations, driving patterns, and vehicle performance indicators, are gathered and processed by the system. A recent audit found that the business had not put in place sufficient data protection procedures.

According to the AI Act, data management and privacy protection are essential for this business.

Why is this essential?

A) Because it enables the business to prioritize business objectives and operational efficiency
B) Because it enhances user trust, safeguards personal data, and prevents unauthorized access
C) Because it is mandatory and complying with the AI Act avoids legal trouble and potential fines
D) Because it streamlines data gathering procedures by removing the need for user consent

A) Incorrect. Implementing data management and privacy protection is not meant to help the business to prioritize efficiency over compliance.
B) Correct. The AI Act emphasizes protecting individual privacy and ensuring ethical data management, which supports accurate and fair AI system operations. (Literature: A, Chapter 4.3, 4.4, 4.6)
C) Incorrect. While compliance is important, the primary focus of the AI Act is on protecting individual rights and maintaining ethical standards.
D) Incorrect. The AI Act and other relevant data protection regulations require user consent and data protection. Bypassing these requirements is unlawful and unethical.

37 / 40
According to the AI Act, which use of an AI system fits the classification of limited risk?

A) A chatbot designed to assist customers with general inquiries, which is programmed to disclose it is an AI.
B) A facial recognition system used for real-time identification of customers in public spaces, such as a mall.
C) A medical diagnostic tool that assists doctors by giving treatment recommendations based on patient data.
D) An AI system that operates an autonomous vehicle, which drives on public roads without human supervision.

A) Correct. The AI Act categorizes AI systems that interact with users but do not have significant potential to impact rights, safety or legal obligations as limited risk. They must comply with transparency obligations, such as informing users they are interacting with an AI system. (Literature: A, Chapter 3.3)
B) Incorrect. Depending on the decisions taken after identification, this system will fall under high risk or may even be forbidden, due to its implications for privacy and surveillance.
C) Incorrect. This tool falls under high-risk application because the AI system deals with health and safety data.
D) Incorrect. Autonomous vehicles are considered high risk due to safety concerns and the impact of possible accidents.

38 / 40
A business develops an AI system for education. The AI system will determine if a student gets access to materials, is admitted to a school, or gets assigned to a class. The AI system will be provided via cloud services.

According to the AI Act, in which category should the use of this AI system be classified?

A) Unacceptable risk
B) High risk
C) Limited risk
D) Minimal or no risk

A) Incorrect. AI systems that can have large impacts on natural persons, such as access to education, are classified as high-risk under the AI Act, not as unacceptable risk, as they are regulated with strict requirements rather than outright banned.
B) Correct. AI systems designed to assess access to education should be classified as high-risk, because they can have a large impact on natural persons. AI is directly influencing whether a student can access educational resources or be admitted, which affects their fundamental rights. (Literature: A, Chapter 3.3, 3.4; AI Act, Article 6(Annex III))
C) Incorrect. Limited-risk AI includes AI-powered chatbots, recommendation systems, or AI assistants that do not make critical decisions about people's rights or opportunities and have the potential to exclude persons from access to education. This poses a high level of risk.
D) Incorrect. A low-risk classification does not accurately reflect the potential risks associated with this type of AI system, as its ability to exclude persons from access to education may have large consequences for them.

39 / 40
An organization has developed an AI system for automated hiring. During testing, the team finds the following:

- The system consistently scores candidates from certain ethnic backgrounds lower, because there is demographic bias in the training data.
- Currently, there is no internal review process or feedback mechanism from relevant parties that could have pointed the risk of this specific bias out.

The organization must comply with the AI Act. To help solve these issues, the organization uses the ISO/IEC TR 24368 standard.

According to this standard, what should the organization do to solve these issues?

A) Create a synthetic dataset to address demographic imbalances and improve fairness
B) Implement transparency to increase the system's explainability and accountability
C) Strengthen data encryption practices and use access control to prevent breaches
D) Use an ethical framework with stakeholder input to evaluate human rights issues

A) Incorrect. Using synthetic data alone does not ensure bias mitigation and fails to address core requirements around ethical AI development. Moreover, it is not part of the ISO/IEC TR 24368 standard being referred to.
B) Incorrect. Transparency does not directly address fairness, ethical review processes, or stakeholder inclusion as required. The relevant solution to solve the issues is implementing an ethical review process.
C) Incorrect. While data encryption and access control are critical for ensuring information security, they are not relevant to the issue at hand. A more relevant focus would be on implementing an ethical review process.
D) Correct. ISO/IEC TR 24368 emphasizes the importance of ethical frameworks, human rights practices, stakeholder involvement, and fairness in AI development. Establishing an ethical review process helps identify and mitigate discrimination, aligning with the standard's core principles. (Literature: B, Chapter 4.2, 4.3)

40 / 40
An AI startup develops a general-purpose AI (GPAI) model, trained on publicly available online content, including news articles, research papers, and social media posts. After launching, the company receives a legal notice from a group of authors claiming their intellectual property (IP) was used for training the model without authorization.

What should be done to protect IP rights in this case?

A) Argue that the GPAI model qualifies as open-source, and is exempt from copyright compliance obligations
B) Claim fair use under the AI Act, since the content was publicly available, and continue using the dataset
C) Delete the AI-generated outputs containing similarities to the disputed works to avoid infringement claims
D) Document and share details of the GPAI training dataset, including provenance, to ensure compliance

A) Incorrect. Open-source AI models are not automatically exempt from copyright compliance if they pose systematic risks or are monetized.
B) Incorrect. The AI Act does not provide a fair use exemption. Publicly available content may still be protected by copyright.
C) Incorrect. The AI Act does not mandate the deletion of AI-generated outputs based solely on similarity to copyrighted works.
D) Correct. Under Article 53 of the AI Act, providers must document the training process and include detailed information on the data's provenance and characteristics. (Literature: A, Chapter 3)

Evaluation

The table below shows the correct answers to the questions in this sample exam.

Question	Answer	Question	Answer
1	B	21	C
2	B	22	D
3	A	23	B
4	A	24	C
5	D	25	A
6	C	26	D
7	A	27	C
8	A	28	D
9	C	29	A
10	A	30	D
11	D	31	C
12	B	32	A
13	A	33	A
14	B	34	C
15	A	35	B
16	B	36	B
17	A	37	A
18	D	38	B
19	C	39	D
20	B	40	D

Contact EXIN

www.exin.com