考试样卷

202511 版本

目录

考试说明

本试卷是 EXIN Artificial Intelligence Compliance Professional (AICP.CH)模拟考试。 EXIN 考试准则适用于该考试。

本试卷由 40 道单项选择题组成。每道选择题有多个选项，但这些选项中只有一个是正确答案。

本试卷的总分是 40 分。每道题的分数是 1 分。您需要获得 26 分或以上通过考试。

考试时间为 90 分钟。

在该考试过程中您可以参考《人工智能法案》。

祝您好运!

考试样卷

1 / 40
《人工智能法案》是欧盟制定的一项立法。在第1条中，该法案阐明了其立法目标。

《人工智能法案》的**主要**目标是什么?

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) 指导方针专注于环境的保护，没有针对高风险人工智能的特定规则和禁止性规定，创新措施只限于大型企业
Guidelines focused solely on environmental protection, with no specific rules for high-risk AI, no prohibitions, and innovation measures only for large corporations

B) 协同欧盟内部的AI系统规则，对某类人工智能实践的禁止，针对高风险AI系统的要求，透明度规则，市场监督，以及创新支持
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) 禁止特定人工智能实践，规则仅适用于通用人工智能（GPAI），透明度规则不包括高风险人工智能，以及仅限于非欧洲实体的创新支持
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) 人工智能系统的规则仅限于安全和健康，禁止所有人工智能实践，透明度规则仅适用于高风险人工智能，以及将初创企业排除在外的创新支持
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
根据《人工智能法案》，问责制和合规性味着什么?

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

A) 问责制侧重于维护用户隐私和数据安全，而合规性则涉及与现有信息技术基础设施的整合。
Accountability focuses on maintaining user privacy and data security, while compliance relates to the integration with existing IT infrastructure.

B) 问责制指的是让人工智能开发过程中的开发者和运营者承担相应责任，而合规性则意味着遵守法律法规的要求。
Accountability involves holding developers and operators in AI development responsible, and compliance means adhering to legal requirements.

C) 问责制是指确保人工智能系统对开发者具有盈利性，而合规性则涉及满足用户的需求和偏好。
Accountability is about ensuring that AI systems are profitable for developers, and compliance involves meeting user demands and preferences.

D) 问责制是指人工智能用户对其系统的正确使用负责，而合规性则意味着遵守人工智能创新的行业标准。
Accountability refers to AI users being accountable for correct use of the system, while compliance means following industry standards for AI innovation.

3 / 40
根据《人工智能法案》，受人工智能系统影响的个人享有特定权利，以确保透明度、公平性和问责制。

《人工智能法案》明确授予的一项权利是什么?

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) 知悉与人工智能系统进行交互或受到其影响的权利
The right to be informed of interacting with or being affected by an AI system
B) 要求访问人工智能系统源代码的权利
The right to demand access to the source code of the AI system
C) 禁止人工智能参与任何涉及自身的决策过程的权利
The right to prohibit the use of AI in any decision-making process that involves them
D) 要求删除人工智能系统所使用个人数据的权利
The right to request deletion of personal data used by the AI system

4 / 40
安娜是一家中小型企业（SME）的合规官，负责监督一个用于自动化客户支持的新人工智能系统的实施。该公司并未开发此系统，而是从另一供应商处购买。根据《人工智能法案》，该人工智能系统被归类为高风险人工智能系统。

安娜的任务是确保公司在部署和监控此人工智能系统时遵守用户义务。她必须确定哪些行动应优先考虑，哪些行动应避免。

考虑到人工智能用户的义务，安娜**不**应考虑什么？

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) 在不与供应商协作的情况下，进一步开发人工智能模型的算法以增强其决策能力
Developing the AI model's algorithms further to enhance its decision-making capabilities without involving its provider

B) 详细记录人工智能系统的性能，并确保符合相关的报告要求
Keeping detailed records of the AI system's performance and ensuring compliance with relevant reporting requirements

C) 监控人工智能系统的性能，以确保其按预期运行并符合安全标准
Monitoring the performance of the AI system to ensure it operates as intended and complies with safety standards

D) 根据法律要求，向相关主管机构报告人工智能系统的任何严重事故或故障
Reporting any serious incidents or malfunctions with the AI system to the appropriate authorities as is required by law

5 / 40
一个AI系统被用于公共场所安保目的的人脸识别。有一个组织在监督该AI系统的数据保护和隐私法规（例如《通用数据保护条例》（GDPR））合规性方面最相关。

这个组织是哪个?

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) 欧洲消费者组织 （BEUC）
The European Consumer Organization (BEUC)
B) 欧洲人工智能委员会 （EAIB）
The European Artificial Intelligence Board (EAIB)
C) 欧洲法院 （ECJ）
The European Court of Justice (ECJ)
D) 欧洲数据保护委员会 （EDPB）
The European Data Protection Board (EDPB)

6 / 40
一家企业开发了一个用于个性化营销的人工智能系统。该系统利用机器学习（ML）算法为个体客户量身定制广告。在一次合规审查中，团队发现了以下风险：

- 缺乏明确文档，未能清晰展示人工智能系统如何处理数据。
- 人工智能系统生成个性化推荐的机制尚未被完全理解。
- 客户投诉此类问题。

该公司必须遵守《人工智能法案》。为此，该企业采用了ISO/IEC 42001标准和NIST人工智能风险管理框架（RMF）。

根据此标准和框架，该企业应采取哪些措施来解决这些问题?

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) 进行一系列用户体验（UX）测试，以获取关于可用性、易学性和客户偏好的反馈。
Conduct a series of user experience (UX) tests to get feedback on usability, learnability, and customer preferences

B) 侧重于提高系统的预测准确性，以提升成本效益、客户满意度和用户参与度。
Focus on improving the system's prediction accuracy to improve cost efficiency, customer satisfaction, and engagement

C) 实施一套文档化流程，详细说明数据来源、处理方法和算法决策过程。
Implement a documentation process that details data sources, processing methods, and algorithmic decision-making

D) 升级系统硬件，以确保更快的处理速度、更高的效率和更高的客户满意度。
Upgrade the system's hardware to ensure faster processing, greater efficiency, and higher customer satisfaction

7 / 40
一家企业开发了一个人工智能系统，用于监测住院病人。该系统在病房内使用高清摄像头，实时监测病人的状况。如果系统检测到病人处于危急状态，它会自动呼叫护士到病床边。

为了提高人工智能系统的性能，该企业希望开始建立一个病人视频数据库，并在视频的关键时间点附上专业人员的注释，以此为系统构建更多训练数据。

该企业正在考虑进行数据保护影响评估（DPIA）。负责团队不确定是否根本需要进行DPIA。如果DPIA是强制性的，团队想知道评估应何时进行：是现在，还是仅在更新部署之后。

该企业必须遵守《人工智能法案》和《通用数据保护条例》（GDPR）。

该企业现在是否应该进行DPIA?

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) 是，因为对于可能对自然人权利构成高风险的人工智能项目，需要进行DPIA。
Yes, because a DPIA is required for AI projects that could pose a high risk to the rights of natural persons.

B) 是，因为任何收集个人数据的项目都需要进行DPIA，即使该项目风险较低。
Yes, because a DPIA is required for any project that collects personal data, even if the project is low risk.

C) 不，因为用于培训目的、教育或科学研究的数据不需要进行DPIA。
No, because a DPIA is not required for using data for training purposes, education, or scientific research.

D) 不，因为DPIA仅在人工智能系统完全开发、测试和部署之后才需要进行。
No, because a DPIA is only required after the AI system has been fully developed, tested, and deployed.

8 / 40
一家企业开发了一个用于实时人脸识别的人工智能系统。一家私人安保公司将该人工智能系统部署用于监控一个公共购物中心。该系统扫描所有访客，将其与过往罪犯和政治活动家数据库进行交叉比对，并标记出在这些数据库中列出的访客。被标记的访客在整个访问期间会被秘密跟踪，以评估他们是否从事安保公司认为的可疑行为。

根据《人工智能法案》，该人工智能系统的使用应归类于哪个类别？

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) 不可接受的风险
Unacceptable risk
B) 高风险的
High-risk
C) 有限风险的
Limited-risk
D) 低风险或零风险的
Minimal or no-risk

9 / 40
一家旅行社使用人工智能系统为其度假套餐开发动态精准营销活动。这些活动包括在社交媒体和旅行平台上进行实时广告投放，并利用个人的浏览历史。该旅行社利用人工智能推断用户的情绪状态，然后推荐定制化的目的地和活动。

该旅行社必须遵守《人工智能法案》。

该旅行社必须应对哪些风险?

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) 包含潜在偏见的风险。他们应该定期更新训练数据，以避免推荐不相关的目的地或错误地推断情绪状态。
The risk of including potential biases. They should update the training data regularly to avoid suggesting irrelevant destinations or infer wrong emotional states.

B) 无效广告活动的风险。他们应该侧重于更新算法，因为《人工智能法案》不涵盖个性化广告。
The risk of ineffective advertising activities. They should focus on updating the algorithm, because the AI Act does not cover personalized advertisements.

C) 缺乏透明度的风险。他们应该保证人工智能的公开性，减少推荐中的偏见，并评估广告活动是否符合伦理。
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) 滥用个人数据的风险。他们应该停止使用人工智能驱动的个性化功能，因为《人工智能法案》禁止将个人数据用于定向广告。
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
一家公司开发了一款人工智能模型，可应用于包括医疗保健和金融在内的多个行业。由于其广泛应用，该人工智能模型对公众健康带来了潜在风险。

该公司开发了什么，以及根据《人工智能法案》，该公司应实施哪些实践?

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) 该公司开发了具有系统风险的通用人工智能（GPAI）。它应进行额外的测试以减轻风险。
The company developed a general-purpose AI (GPAI) that carries systemic risks. It should conduct additional tests to mitigate the risks.

B) 该公司开发了一个高风险人工智能系统。它应实施《人工智能法案》中概述的所有高风险人工智能系统的要求。
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) 该公司开发了一个窄范围人工智能模型。它应确保该模型仅在预定义参数内运行以预防风险。
The company developed a narrow AI model. It should ensure the model operates only within predefined parameters to prevent risks.

D) 该公司开发了一个实验性人工智能模型。它应侧重于研究和开发，而无需立即进行风险管理。
The company developed an experimental AI model. It should focus on research and development without immediate risk management.

11 / 40
一个组织正在开发一个高风险人工智能系统。在测试过程中，开发团队识别出各种风险，包括数据完整性不一致和存在过时记录。这些风险可能对模型的性能产生负面影响。

该组织必须遵守《人工智能法案》。为此，他们采用了CEN/CLC/TR 18115框架。

根据该框架，该组织应采取什么措施来解决这些风险?

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) 进行数据保护影响评估（DPIA），以解决人工智能决策的公平性问题
Conduct a data protection impact assessment (DPIA) to address the fairness of AI decision-making
B) 使用协议加密所有训练和测试数据集，以防止未经授权访问个人数据
Encrypt all training and testing datasets using protocols to prevent unauthorized access to personal data
C) 实施通用风险控制措施，以减少上述运营和声誉风险
Implement general-purpose risk controls to reduce the mentioned operational and reputational risks
D) 通过应用结构化的质量指标和统计评估方法来提高数据质量
Improve the data quality by applying structured quality metrics and statistical evaluation methods

12 / 40
《人工智能法案》描述了与人工智能系统相关的几种角色。

"人工智能系统的进口者"这一角色的定义是什么?

The AI Act describes several roles connected to an AI system.

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

A) 以自己的名义或商标设计、开发和营销人工智能系统的个人或组织。
A person or organization that designs, develops, and markets an AI system under their own name or trademark.
B) 将人工智能系统投放市场但不对其原始开发负责的个人或组织。
A person or organization that places an AI system on the market but is not responsible for its original development.
C) 在其运营中使用人工智能系统并确保遵守本地用户义务的个人或组织。
A person or organization that uses an AI system in their operations and ensures local compliance with user obligations.
D) 负责监控人工智能系统进口是否符合《人工智能法案》法规的监管机构。
A regulatory authority tasked with monitoring if the AI system is imported in compliance with the AI Act regulations.

13 / 40
一家企业开发了一个用于检测金融交易欺诈的人工智能系统。该系统分析交易模式以识别可疑活动并预防欺诈行为。鉴于可能出现影响合法交易的误报以及欺诈策略不断演变的性质，该企业认识到需要有效的保障措施。

该企业必须遵守《人工智能法案》。为帮助预防误报问题，该企业使用了ISO/IEC 23894标准。

根据该标准，该企业应采取哪些措施来预防这些问题？

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) 将风险管理嵌入所有活动中，以确保全面的监督并主动降低风险
Embed risk management into all activities to ensure comprehensive oversight and proactive risk mitigation

B) 增强数据隐私措施，以保护敏感信息并遵守隐私法规
Enhance data privacy measures to protect sensitive information and comply with privacy regulations

C) 专注于提高模型准确性，以确保可靠的性能并最大限度地减少误报
Focus on improving model accuracy to ensure reliable performance and minimize false positives

D) 实施网络安全措施，以保护系统免受外部威胁和未经授权的访问
Implement cybersecurity measures to protect the system from external threats and unauthorized access

14 / 40
一家制造公司使用人工智能驱动的机器人设备对其装配线进行质量控制。调查小组注意到，一名匿名举报人声称人工智能系统最近显示异常低的缺陷产品数量。缺陷产品少报的原因是人工智能系统的软件更新。经人工检查，这些产品存在缺陷且不安全，无法使用。

报告指出，新的缺陷检测算法产生了一个关键错误，导致了漏报。据举报人称，经理们知道这个问题，但为了避免损害公司声誉而没有解决这个问题。

接下来的行动应该是什么？

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) - 调整内部算法以解决问题
- 如果问题在30天后仍然存在，则通知相关主管机构
- Adjust the internal algorithm to address the problem
- Notify the relevant competent authority if the issue still exists after 30 days

B) - 内部调查问题并开始解决
- 立即将发生的情况通知相关主管机构
- Investigate the problem internally and start solving it
- Notify the relevant competent authority of the occurrence immediately

C) - 调查举报人举报的原因
- 如果消费者开始投诉，则通知相关主管机构
- Research the whistleblower's reasons for reporting
- Notify the relevant competent authority if consumers start complaining

D) - 停止使用人工智能系统并切换到旧方法
- 这使得无需通知相关主管机构
- 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 公司使用一个高风险人工智能系统，通过X射线图像诊断医疗状况。他们已具备以下条件：

- 公司已通过外部审计，确保该人工智能系统符合《人工智能法案》的标准。
- 建立了健全的风险管理框架，用于识别和缓解潜在问题，并制定了应急预案。
- 人工智能系统操作的详细记录得到安全存储，以备问责和审计。
- 向用户提供了清晰的文档和培训，解释人工智能的决策过程和局限性。
- 所有人工智能生成的诊断结果在最终确定前，都经过医疗专业人员的审查，整合了人类判断。

该公司还应该实施什么？

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) 他们应该增加健全的数据治理程序，以维护其人工智能系统的可靠性和公平性。
They should add robust data governance procedures to maintain the reliability and fairness of their AI system.

B) 他们应该确保人工智能系统能够独立运行，无需任何人为干预以提高效率。
They should ensure that the AI system can operate independently without any human intervention for efficiency.

C) 他们应该实施一个系统，自动推翻人类决策，以加快诊断过程。
They should implement a system to automatically override human decisions to speed up the diagnosis process.

D) 他们应该包含一个功能，允许患者根据人工智能的建议直接修改他们的医疗记录。
They should include a feature that allows patients to directly modify their medical records based on AI suggestions.

16 / 40
一家保险公司实施了一套新的人工智能信用评分系统，该系统可以访问内部数据库和公共数据库。识别出以下风险：

- **缺乏适当的训练数据。**如果模型训练不当，将难以准确地为人们确定公平的评分。
- **与其他应用程序的集成。**将基于人工智能的引擎集成到相当复杂且在某些方面过时的应用程序环境中将很困难。
- **不符合GDPR。**《通用数据保护条例》（GDPR）对自动化系统自主处理个人数据有具体要求。
- **模型的透明度和质量。**员工和客户都必须能够理解人工智能模型的结果和决策。

该保险公司必须遵守《人工智能法案》。

哪个风险对于遵守《人工智能法案》来说**不**重要?

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) 缺乏适当的训练数据
A lack of proper training data
B) 与其他应用程序的集成
Integration with other applications
C) 不符合GDPR
Non-compliance with the GDPR
D) 模型的透明度和质量
Transparency and quality of the model

17 / 40
一家政府机构提议开发一套人工智能系统，用于预测大城镇市中心的犯罪热点。该系统将用于自动化监控。它被编程为自动识别显示可疑行为的人并向当地警方报告。这是一个预防犯罪、增强安全感和确保犯罪后正义的绝佳机会。

实施该人工智能系统是否存在任何风险?

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) 是，因为用于自动化决策的人工智能系统带有固有的偏见风险，这可能不公平地使个人处于不利地位。
Yes, because an AI system that is used for automated decisions carries the inherent risk of bias, which may unfairly disadvantage individuals.

B) 是，因为《人工智能法案》预见到监控系统存在如此多的隐私风险，以至于它彻底禁止在公共场所部署此类系统。
Yes, because the AI Act foresees so many privacy risks with surveillance systems that it outright forbids its employment in public spaces.

C) 不，因为在犯罪起诉和预防中，人工智能系统没有特定的风险，因为它们用于增强公共安全。
No, because in crime prosecution and prevention, AI systems carry no particular risks since they are used to enhance public safety.

D) 不，因为公共领域的人工智能系统提高了效率且没有风险，因为决策是客观的，没有人为错误。
No, because public domain AI systems boost efficiency and carry no risk, since the decisions are objective and free from human error.

18 / 40
一家组织正在开发一个用于招聘的人工智能系统。在内部测试中，团队识别出一个风险：该系统有时无意中偏袒来自特定背景的候选人，可能导致歧视性结果。团队现在不确定如何应对这些担忧。

该组织必须遵守《人工智能法案》。为帮助缓解此风险，该组织使用了ISO/IEC TR 24368标准。

根据该标准，该组织应采取哪些措施来缓解此风险?

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) 调整算法，根据就业统计数据优先考虑人口配额
Adjust the algorithm to prioritize demographic quotas based on employment statistics
B) 采纳零数据方法，从训练集中移除所有人口统计数据
Adopt a zero-data approach by removing all demographic data from the training set
C) 应用网络安全措施，保护候选人数据并增强系统完整性
Apply cybersecurity measures to protect candidate data and enhance system integrity
D) 实施利益相关者参与流程，以识别和缓解潜在偏见
Implement a stakeholder engagement process to identify and mitigate potential biases

19 / 40
一家组织正在开发一个用于贷款审批的人工智能系统。在内部测试中，合规团队发现一个风险：模型的决策过程缺乏透明度，并且风险评估的文档有限。

该组织必须遵守《人工智能法案》。该组织为此使用了ISO/IEC 42001标准和NIST人工智能风险管理框架（RMF）。

根据此标准和框架，该企业应采取哪些措施来解决这一风险?

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) 根据推荐的网络安全指南进行安全合规评估
Conduct a safety compliance assessment based on recommended cybersecurity guidelines
B) 立即停用人工智能系统并过渡到手动贷款审批流程
Decommission the AI system immediately and transition to a manual loan approval process
C) 定义一个包含透明度指标的衡量计划，并记录决策逻辑以便监督
Define a measurement plan with transparency metrics and record decision logic for oversight
D) 使用合成数据重建系统，以尽可能消除偏见来源
Rebuild the system using synthetic data to eliminate as many sources of bias as possible

20 / 40
一家领先的汽车制造商开发了一款高度自动化车辆（4级），该车辆配备了用于道路安全的人工智能物体识别技术。在测试过程中，发现了以下风险：

- 在弱光条件下，系统检测减速带的能力受损。
- 该模型可能难以销售，因为它不知道其他车辆的尺寸。
- 开发人员不太确定如何解释模型如何做出决策。
- 在人工智能系统开发阶段，并未向所有利益相关者征求意见。

当**仅**考虑《人工智能法案》合规性时，必须解决什么问题？

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) 现实世界条件下测试不足的风险
The risk of insufficient testing under real-world conditions
B) 人工智能决策缺乏透明度的风险
The risk of lack of transparency in AI decision-making
C) 人工智能系统对其他车辆模型规模化有限的风险
The risk of limited scalability of the AI system to other vehicle models
D) 人工智能开发过程中利益相关者参与有限的风险
The risk of limited stakeholder involvement during AI development

21 / 40
一家物流公司正在构建一个人工智能系统，以优化其配送路径并降低燃油消耗。该组织正在权衡两个选择：

- 一个闭源人工智能模型，由供应商保证更快的安装和经过验证的合规认证。
- 一个开源人工智能模型，可实现高度定制化和透明度。

该公司必须遵守《人工智能法案》，但同时也希望平衡创新和成本。

哪种模型**最**适合该公司?

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) 闭源人工智能模型，因为它本质上更安全，并受到当局的信任。这降低了不合规的可能性。
A closed-source AI model, because it is intrinsically more secure and trusted by authorities. This reduces the possibility of non-compliance.
B) 闭源人工智能模型，因为它提供预认证的合规性。这减轻了公司证明符合《人工智能法案》的负担。
A closed-source AI model, because it provides pre-certified compliance. This lessens the company's burden of proving AI Act compliance.
C) 开源人工智能模型，因为它保证完全透明。这有助于满足文档记录和可审计性要求。
An open-source AI model, because it guarantees complete transparency. This helps with documentation and auditability requirements.
D) 开源人工智能模型，因为它免受《人工智能法案》合规约束。这是因为源代码是公开可用的。
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
《人工智能法案》规定了人工智能开发应遵循的伦理原则。

哪项**不是**这些原则之一?

The AI Act defines ethical principles for AI development.

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

A) 可解释性
Explicability
B) 公平性
Fairness
C) 损失预防
Loss prevention
D) 尊重人工智能自主性
Respect for AI autonomy

23 / 40
一家初创公司正在开发一个人工智能系统，旨在通过根据个别学生的需求定制课程计划来辅助学校的个性化学习。该系统收集学生的表现和学习行为数据。

根据《人工智能法案》，这家初创公司在这里应该考虑什么，以平衡创新与监管？

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) 避免将系统标记为高风险，以规避额外的监管负担，并使创新过程更加简便
Avoid labeling the system as high-risk to circumvent additional regulatory burdens and streamline innovation

B) 确保人工智能系统经过一致性评估并符合高风险系统法规
Ensure the AI system undergoes a conformity assessment and complies with high-risk system regulations

C) 实施健全的数据保护功能，但取消用户通知，以避免部署延迟
Implement robust data protection features but take out user notifications to avoid delays in deployment

D) 将系统 仅销售给私立学校，以限制高风险合规要求的影响
Market the system to private schools exclusively to limit the impact of high-risk compliance requirements

24 / 40
一家金融机构 Fintegra 正在实施一个人工智能系统，用于检测交易中的欺诈行为。该系统需要访问客户的交易信息和人口统计数据进行分析。Fintegra 必须遵守《人工智能法案》的数据最小化要求。

Fintegra 遵守数据最小化要求的**最佳**方式是什么?

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) 他们应该匿名化所有交易数据并删除任何识别自然人的数据以符合要求，即使这些数据对于欺诈检测目的至关重要。
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) 他们应该收集所有个人详细信息，包括全名和精确地址，以确保精确分析并随时间推移的改进，并尽可能长时间地安全存储数据。
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) 他们应该将数据收集限制在与检测欺诈相关的交易数据，并避免处理个人详细信息，例如客户的全名或精确地址。
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) 他们应该只与符合《人工智能法案》的、获得认可的供应商共享所收集的数据，这最大限度地减少了对个人详细信息（如客户全名）的内部处理。
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正在实施一个自适应学习平台，该平台使用人工智能来个性化学生的学习路径 。该平台根据学生的个体表现调整任务的难度 。

EduTech应降低哪些风险，以确保该人工智能系统符合伦理地使用?

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) 偏见和歧视的风险，因为这些会导致某些学生获得不公平的优势或劣势。这种风险通过定期审查和更新人工智能系统的数据集和算法来缓解。
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) 过度依赖技术的风险，这可能导致学生无法培养批判性思维技能。这种风险通过对人工智能系统的决策过程保密来缓解，以刺激学生更多地思考。
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) 隐私泄露的风险，因为敏感的学生数据，包括他们的表现，可能会被不当处理或暴露。这种风险通过更多地侧重于提高人工智能系统的技术性能来缓解。
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) 透明度问题的风险，因为学生和教育工作者可能不理解决策是如何做出的。这种风险通过确保人工智能系统在没有人工监督的情况下运行来缓解，这确保了公平性。
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
一家医院科室专门从事疾病的诊断和治疗。他们开发了一个人工智能诊断系统，以协助识别罕见诊断。该系统分析患者数据、病史和影像扫描。

该系统在美国（US）成功应用。欧盟（EU）的一些医疗专家希望采用该系统，但他们对该人工智能系统的工作原理没有清晰的理解。他们也没有监控人工智能或识别故障或误诊的专业知识和经验。

哪项**不是**采用该人工智能系统相关的风险?

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) 缺乏有效人工监督的风险
The risk of lack of effective human supervision
B) 由于自动化偏见导致误诊的风险
The risk of misdiagnosis due to automation bias
C) 由于缺乏透明度导致不信任的风险
The risk of mistrust caused by lack of transparency
D) 未经授权访问患者记录的风险
The risk of unauthorized access to patient records

27 / 40
一家企业正在开发智能家居助手的人工智能系统。在测试过程中，团队发现语音识别错误（例如混淆发音相似的词语）会导致意外操作，比如错误开启电器。这些错误可能导致隐私泄露，例如未经同意录制对话或错误识别用户，从而可能与未经授权的第三方共享敏感信息。

该组织必须遵守《人工智能法案》。他们为此使用了CEN/CLC/TR 18115框架。

根据该框架，人工智能供应商应如何解决这个问题?

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) 制定利益相关者参与计划，以获取对人工智能系统工作原理的不同看法
Create a stakeholder engagement plan to get different views on how the AI system works
B) 进行伦理影响评估，以了解智能家居助手的隐私风险
Do an ethical impact assessment to understand privacy risks of smart home assistants
C) 通过使用系统的验证和错误检查方法来提高训练数据质量
Improve the training data quality by using systematic validation and error-checking methods
D) 通过加密保护语音数据并防止数据泄露来提高数据安全
Increase data security with encryption to protect voice data and prevent data breaches

28 / 40
一家科技公司被发现使用《人工智能法案》明确禁止的实时远程生物特征识别人工智能系统。

对这一违规行为的适当处罚是什么?

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) 给予正式警告，不处以罚款
A formal warning without financial penalties
B) 最高可达750万欧元或上一财政年度全球总年营业额1%的行政罚款
An administrative fine of up to €7.5 million or 1% of the total global annual turnover in the previous financial year
C) 最高可达1500万欧元或上一财政年度全球总年营业额3%的行政罚款
An administrative fine of up to €15 million or 3% of the total global annual turnover in the previous financial year
D) 最高可达3500万欧元或上一财政年度全球总年营业额7%的行政罚款
An administrative fine of up to €35 million or 7% of the total global annual turnover in the previous financial year

29 / 40
《人工智能法案》特别强调人工智能系统两个方面的重要性：透明度和可追溯性。

为什么透明度和可追溯性很重要?

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

Why are transparency and traceability important?

A) 因为它们对于确保人工智能系统的问责制和培养信任至关重要。
Because they are crucial for ensuring accountability and fostering trust in AI systems.
B) 因为它们是所有产品（包括人工智能系统）的强制性要求。
Because they are mandatory requirements for all products, including AI systems.
C) 因为它们对于人工智能系统的可靠性和自动化特别重要。
Because they are particularly essential for the reliability and automation of AI systems.
D) 因为它们在欧洲、中国和美国立法之间是共享的。
Because they are shared between European, Chinese, and American legislation.

30 / 40
一家零售机构使用的人工智能系统会根据用户偏好和所用设备自动改变网站元素的显示方式。该系统利用点击历史和页面停留时间推荐产品并增强用户体验。

根据《人工智能法案》，该人工智能系统的使用应归类于哪个类别?

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) 不可接受的风险
Unacceptable risk
B) 高风险的
High-risk
C) 有限风险的
Limited-risk
D) 低风险或零风险的
Minimal or no-risk

31 / 40
一家公司创建了一个用于招聘流程中自动化决策的人工智能系统。该人工智能系统将筛选简历、对候选人进行排名并提出面试建议。

该公司担心该人工智能系统可能存在影响招聘流程的偏见。

该公司缓解人工智能系统偏见的**最佳**方法是什么?

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) 允许人工智能系统在没有人为进一步干预的情况下学习和适应
Allow the AI system to learn and adapt without further human intervention
B) 忽略训练数据中的偏见，专注于人工智能系统的性能
Ignore biases in the training data and focus on the AI system's performance
C) 组建多元化的开发团队来创建和监控人工智能系统
Implement a diverse development team to create and monitor the AI system
D) 使用单一数据源来训练人工智能系统，以确保一致性
Use a single source of data for training the AI system to ensure consistency

32 / 40
一家名为 Feline Finesse 的网店销售猫咪配件和猫咪抱枕，其中包括根据顾客图片定制的猫咪毛绒玩具。该网店使用的人工智能系统可以完成以下任务：

- 根据消费者活动动态调整价格。
- 根据顾客偏好对搜索结果进行排序。
- 为顾客推荐它认为顾客可能喜欢的其他产品。

目前，该网店会告知顾客人工智能系统的功能，并且对算法的工作原理非常透明。然而，首席执行官对这种做法提出质疑，并想知道需要达到何种程度的透明度以及它如何影响销售。

参照《人工智能法案》，首席执行官应该了解哪些有关透明度的知识？

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) 透明度可以向消费者证明系统是客观的。消费者根据《人工智能法案》有权了解他们的数据是如何被使用的，这种理解能培养信任。
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) 透明度可以展示人工智能系统的局限性或约束。消费者在了解这一点后可能会对公司失去信任，这会损害公司的声誉。
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) 电子商务并非强制要求透明度。个性化带来的便利有助于消费者，他们不需要了解人工智能系统如何运作。
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) 透明度仅限于提供人工智能系统源代码。消费者对系统的信心可能会因为了解算法如何精确运作而下降。
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
一家高风险人工智能系统在招聘过程中使用，根据候选人的资格自动筛选。然而，部署者尚未实施任何机制，以在可疑决策情况下进行人工干预或监督。

根据《人工智能法案》，该系统是否需要人工监督?

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) 是，因为人工监督在决策过程中是必要的干预。
Yes, because human oversight is necessary for intervention in decision-making processes.
B) 是，因为人工监督确保符合公平和透明义务。
Yes, because human oversight ensures compliance with fairness and transparency obligations.
C) 不，因为自动化系统旨在无人为干预下运行。
No, because automated systems are designed to function without human intervention.
D) 不，因为招聘过程不涉及对自然人的关键安全风险。
No, because recruitment processes do not involve critical safety risks to natural persons.

34 / 40
一家公司正准备推出一个通用人工智能（GPAI）模型。该模型可适用于客户服务自动化、内容创建和数据分析等任务。该公司总部设在欧盟（EU）以外，但计划在多个欧盟成员国分销该模型。

根据《人工智能法案》，在欧盟分销该GPAI模型之前，哪项**不是**强制要求的?

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) 在欧盟任命一名授权代表，以处理合规事宜
Appoint an authorized representative in the EU to handle compliance matters
B) 遵守欧盟版权法规，以受版权保护的数据进行模型训练
Comply with EU copyright regulations for model training with copyrighted data
C) 进行彻底审计，以验证完全符合所有欧盟法律法规
Conduct a thorough audit to verify full conformity with all EU laws and regulations
D) 发布用于训练GPAI模型的详细内容摘要
Publish a detailed summary of the content used for training the GPAI model

35 / 40
一个组织部署了一个人工智能系统，用于工业设备的预测性维护。经过几个月的运行，该系统产生了大量的误报，扰乱了工作流程。一项调查显示以下情况：

- 该组织没有考虑工作现场动态环境变化的影响。
- 该组织缺乏部署后重新评估风险的正式流程。

该组织必须遵守《人工智能法案》。为帮助解决这些问题，该组织使用了ISO/IEC 23894标准。

根据该标准，该组织应采取什么措施来解决这些问题？

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) 开展以人为本的设计研讨会，以提高系统可用性
Conduct a human-centered design workshop to improve system usability
B) 设计一个包含持续评估和监控的风险管理流程
Design a risk management process with ongoing evaluation and monitoring
C) 进行网络安全审计，以识别和解决可能的漏洞
Perform a cybersecurity audit to identify and address possible vulnerabilities
D) 用更简单的、基于规则的模型替换人工智能系统，以便于控制
Replace the AI system with a simpler, rule-based model for easier control

36 / 40
一家汽车车队管理公司使用人工智能系统来追踪驾驶员行为并预测维护需求 。该系统收集并处理大量数据，例如GPS位置、驾驶模式和车辆性能指标 。最近的审计发现，该公司尚未实施充分的数据保护程序 。

根据《人工智能法案》，数据管理和隐私保护对这家企业至关重要 。

为什么这至关重要？

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) 因为它使企业能够优先考虑业务目标和运营效率
Because it enables the business to prioritize business objectives and operational efficiency
B) 因为它增强了用户信任，保障了个人数据，并防止未经授权的访问
Because it enhances user trust, safeguards personal data, and prevents unauthorized access
C) 因为它是强制性的，遵守《人工智能法案》可以避免法律麻烦和潜在罚款
Because it is mandatory and complying with the AI Act avoids legal trouble and potential fines
D) 因为它通过消除用户同意的需要来简化数据收集程序
Because it streamlines data gathering procedures by removing the need for user consent

37 / 40
根据《人工智能法案》，人工智能系统的哪种用途符合有限风险分类?

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

A) 旨在协助客户处理一般查询的聊天机器人，其编程表明它是人工智能。
A chatbot designed to assist customers with general inquiries, which is programmed to disclose it is an AI.
B) 用于在公共场所（例如商场）对客户进行实时识别的人脸识别系统。
A facial recognition system used for real-time identification of customers in public spaces, such as a mall.
C) 一种医疗诊断工具，通过提供基于患者数据的治疗建议来协助医生。
A medical diagnostic tool that assists doctors by giving treatment recommendations based on patient data.
D) 运行自动驾驶车辆的人工智能系统，该车辆在公共道路上无人监督地行驶。
An AI system that operates an autonomous vehicle, which drives on public roads without human supervision.

38 / 40
一家企业正在开发一个用于教育的人工智能系统。该人工智能系统将决定学生是否能获得学习材料、是否被学校录取或被分配到某个班级。该人工智能系统将通过云服务提供 。

根据《人工智能法案》，该人工智能系统的使用应归类于哪个类别?

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) 不可接受的风险
Unacceptable risk
B) 高风险的
High-risk
C) 有限风险的
Limited-risk
D) 低风险或零风险的
Minimal or no-risk

39 / 40
一家组织开发了一个用于自动化招聘的人工智能系统 。在测试过程中，团队发现以下问题：

- 由于训练数据中存在人口统计学偏见，系统对来自某些族裔背景的候选人评分始终较低 。
- 目前，没有内部审查流程或来自相关方的反馈机制可以指出这种特定偏见的风险 。

该组织必须遵守《人工智能法案》 。为帮助解决这些问题，该组织使用了ISO/IEC TR 24368标准 。

根据该标准，该组织应采取什么措施来解决这些问题 ?

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) 创建一个合成数据集，以解决人口统计学失衡并提高公平性
Create a synthetic dataset to address demographic imbalances and improve fairness
B) 实施透明度，以提高系统的可解释性和问责制
Implement transparency to increase the system's explainability and accountability
C) 加强数据加密实践并使用访问控制来防止泄露
Strengthen data encryption practices and use access control to prevent breaches
D) 使用一个包含利益相关者输入的伦理框架来评估人权问题
Use an ethical framework with stakeholder input to evaluate human rights issues

40 / 40
一家人工智能初创公司开发了一个通用人工智能（GPAI）模型，该模型使用公开可用的在线内容进行训练，包括新闻文章、研究论文和社交媒体帖子。发布后，该公司收到一组作者的法律通知，声称他们的知识产权（IP）未经授权被用于模型训练。

在这种情况下，应该采取什么措施来保护知识产权?

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) 主张GPAI模型符合开源条件，并可免除版权合规义务
Argue that the GPAI model qualifies as open-source, and is exempt from copyright compliance obligations

B) 根据《人工智能法案》主张合理使用，因为内容是公开可用的，并继续使用该数据集
Claim fair use under the AI Act, since the content was publicly available, and continue using the dataset

C) 删除包含与争议作品相似之处的人工智能生成输出，以避免侵权索赔
Delete the AI-generated outputs containing similarities to the disputed works to avoid infringement claims

D) 记录并分享GPAI训练数据集的详细信息，包括出处，以确保合规性
Document and share details of the GPAI training dataset, including provenance, to ensure compliance

答案解析

1 / 40
《人工智能法案》是欧盟制定的一项立法。在第1条中，该法案阐明了其立法目标。

《人工智能法案》的**主要**目标是什么?

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) 指导方针专注于环境的保护，没有针对高风险人工智能的特定规则和禁止性规定，创新措施只限于大型企业
Guidelines focused solely on environmental protection, with no specific rules for high-risk AI, no prohibitions, and innovation measures only for large corporations

B) 协同欧盟内部的AI系统规则，对某类人工智能实践的禁止，针对高风险AI系统的要求，透明度规则，市场监督，以及创新支持
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) 禁止特定人工智能实践，规则仅适用于通用人工智能（GPAI），透明度规则不包括高风险人工智能，以及仅限于非欧洲实体的创新支持
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) 人工智能系统的规则仅限于安全和健康，禁止所有人工智能实践，透明度规则仅适用于高风险人工智能，以及将初创企业排除在外的创新支持
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

（题目未完，接下一页）

A) 不正确。该选项仅关注环境保护，未涵盖针对高风险人工智能的具体规定、相关的禁止性条款、以及面向大型企业的创新支持措施，没有正确表述《人工智能法案》所体现的全面性方针。
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) 正确。此选项准确反映了AI法案的要点，包括：人工智能系统的统一规则、对某些人工智能实践的禁止、高风险系统的具体要求、透明度规则、市场监督，以及侧重于中小型企业（SMEs）的创新支持。（文献：A，第3.1和3.2章；《人工智能法案》第1条）
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) 不正确。这个选项提出：AI法案仅关注GPAI，并将高风险人工智能排除在透明度规则之外，同时将创新支持限制在非欧洲实体，这与AI法案的目标不符。
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) 不正确。《人工智能法案》的目标不仅仅是安全和健康。这个选项错误地宣称其规则仅限于安全和健康，将初创企业排除在创新支持之外，并指出禁止所有人工智能实践，这与《人工智能法案》的规定不符。
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
根据《人工智能法案》，问责制和合规性味着什么?

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

A) 问责制侧重于维护用户隐私和数据安全，而合规性则涉及与现有信息技术基础设施的整合。
Accountability focuses on maintaining user privacy and data security, while compliance relates to the integration with existing IT infrastructure.

B) 问责制指的是让人工智能开发过程中的开发者和运营者承担相应责任，而合规性则意味着遵守法律法规的要求。
Accountability involves holding developers and operators in AI development responsible, and compliance means adhering to legal requirements.

C) 问责制是指确保人工智能系统对开发者具有盈利性，而合规性则涉及满足用户的需求和偏好。
Accountability is about ensuring that AI systems are profitable for developers, and compliance involves meeting user demands and preferences.

D) 问责制是指人工智能用户对其系统的正确使用负责，而合规性则意味着遵守人工智能创新的行业标准。
Accountability refers to AI users being accountable for correct use of the system, while compliance means following industry standards for AI innovation.

A) 不正确。尽管用户隐私和数据安全固然重要，但《人工智能法案》中的问责制和合规性是更广泛的概念。它们侧重于责任承担以及遵守法律和监管法规要求，而不仅仅是隐私或技术整合问题。合规性关乎遵循法律和伦理规范，而非IT集成。
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) 正确。问责制意味着人工智能系统的开发者和运营者需对其行为和结果负责。合规性则指遵循《人工智能法案》中概述的法律和监管要求，以确保系统安全、透明且公平。（文献：A，第3.10章）
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) 不正确。问责制与盈利能力或用户偏好无关，合规性也并非为了满足用户需求。相反，它们都侧重于人工智能系统的责任承担和对法律标准的遵循。
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) 不正确。问责制是指让人工智能系统的开发者和运营者对其行为负责，而非推卸责任。合规性则更多是关于满足具体的法律和监管标准，而非一般的行业标准。
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
根据《人工智能法案》，受人工智能系统影响的个人享有特定权利，以确保透明度、公平性和问责制。

《人工智能法案》明确授予的一项权利是什么?

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) 知悉与人工智能系统进行交互或受到其影响的权利
The right to be informed of interacting with or being affected by an AI system
B) 要求访问人工智能系统源代码的权利
The right to demand access to the source code of the AI system
C) 禁止人工智能参与任何涉及自身的决策过程的权利
The right to prohibit the use of AI in any decision-making process that involves them
D) 要求删除人工智能系统所使用个人数据的权利
The right to request deletion of personal data used by the AI system

A) 正确。当个人与人工智能系统进行交互时，必须被告知，除非对一个了解情况的理性人而言这已是显而易见的。这确保了透明度，并帮助个人理解人工智能何时正在影响可能对其产生影响的决策。（文献：A，第3.6章；《人工智能法案》，第50条）
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) 不正确。《人工智能法案》并未赋予个人访问人工智能系统源代码的权利。透明度义务侧重于提供解释和披露，而非完全开放专有代码的访问权限。
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) 不正确。《人工智能法案》并未赋予个人禁止人工智能用于决策过程的权利，但它确实确保了监督和透明度。
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) 不正确。尽管数据保护法确实赋予个人对其数据的某些权利，但《人工智能法案》并未授予一揽子权利，允许个人要求删除人工智能系统使用的所有数据。
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
安娜是一家中小型企业（SME）的合规官，负责监督一个用于自动化客户支持的新人工智能系统的实施。该公司并未开发此系统，而是从另一供应商处购买。根据《人工智能法案》，该人工智能系统被归类为高风险人工智能系统。

安娜的任务是确保公司在部署和监控此人工智能系统时遵守用户义务。她必须确定哪些行动应优先考虑，哪些行动应避免。

考虑到人工智能用户的义务，安娜**不**应考虑什么？

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) 在不与供应商协作的情况下，进一步开发人工智能模型的算法以增强其决策能力
Developing the AI model's algorithms further to enhance its decision-making capabilities without involving its provider
B) 详细记录人工智能系统的性能，并确保符合相关的报告要求
Keeping detailed records of the AI system's performance and ensuring compliance with relevant reporting requirements
C) 监控人工智能系统的性能，以确保其按预期运行并符合安全标准
Monitoring the performance of the AI system to ensure it operates as intended and complies with safety standards
D) 根据法律要求，向相关主管机构报告人工智能系统的任何严重事故或故障
Reporting any serious incidents or malfunctions with the AI system to the appropriate authorities as is required by law

（题目未完，接下一页）

A) 正确。安娜不应在未与供应商协作的情况下，试图独立开发人工智能系统的算法或修改其决策能力。这超出了用户义务的范围，可能导致合规违规，或产生意外后果。用户不负责改变系统的内部结构。（文献：A，第1.1章）
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) 不正确。保留记录和确保透明度符合《人工智能法案》对高风险系统用户的法律要求。这有助于实现问责制和监管合规。
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) 不正确。监控性能是《人工智能法案》规定用户的一项关键义务，旨在确保人工智能系统按预期运行且不会造成任何安全风险。
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) 不正确。报告故障或严重事故是《人工智能法案》对高风险系统用户的一项关键要求，旨在维持合规性并及时处理潜在风险。
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
一个AI系统被用于公共场所安保目的的人脸识别。有一个组织在监督该AI系统的数据保护和隐私法规（例如《通用数据保护条例》（GDPR））合规性方面最相关。

这个组织是哪个?

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) 欧洲消费者组织 （BEUC）
The European Consumer Organization (BEUC)
B) 欧洲人工智能委员会 （EAIB）
The European Artificial Intelligence Board (EAIB)
C) 欧洲法院 （ECJ）
The European Court of Justice (ECJ)
D) 欧洲数据保护委员会 （EDPB）
The European Data Protection Board (EDPB)

A) 不正确。 BEUC侧重于消费者权利，这与生物识别和人工智能特定法规的数据保护相关。
Incorrect. The BEUC focuses on consumer rights, which are related to biometric and data protection for AI specific regulations.
B) 不正确。 EAIB监督《人工智能法案》的合规性，侧重于人工智能特定法规。然而，这个问题涉及数据保护和隐私，这些属于GDPR的范畴。
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) 不正确。ECJ处理司法事务，而非人工智能法规或生物识别数据。
Incorrect. The ECJ addresses judicial matters, not AI regulations or biometric data.
D) 正确。EDPB负责确保GDPR在欧盟（EU）成员国之间的一致应用。它与各国数据保护机构合作，处理诸如人工智能安保系统中生物识别数据使用等问题。（文献：A，第3.9、3.10、4.5章）
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
一家企业开发了一个用于个性化营销的人工智能系统。该系统利用机器学习（ML）算法为个体客户量身定制广告。在一次合规审查中，团队发现了以下风险：

- 缺乏明确文档，未能清晰展示人工智能系统如何处理数据。
- 人工智能系统生成个性化推荐的机制尚未被完全理解。
- 客户投诉此类问题。

该公司必须遵守《人工智能法案》。为此，该企业采用了ISO/IEC 42001标准和NIST人工智能风险管理框架（RMF）。

根据此标准和框架，该企业应采取哪些措施来解决这些问题？

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) 进行一系列用户体验（UX）测试，以获取关于可用性、易学性和客户偏好的反馈。
Conduct a series of user experience (UX) tests to get feedback on usability, learnability, and customer preferences

B) 侧重于提高系统的预测准确性，以提升成本效益、客户满意度和用户参与度。
Focus on improving the system's prediction accuracy to improve cost efficiency, customer satisfaction, and engagement

C) 实施一套文档化流程，详细说明数据来源、处理方法和算法决策过程。
Implement a documentation process that details data sources, processing methods, and algorithmic decision-making

D) 升级系统硬件，以确保更快的处理速度、更高的效率和更高的客户满意度。
Upgrade the system's hardware to ensure faster processing, greater efficiency, and higher customer satisfaction

（题目未完，接下一页）

A) 不正确。用户体验测试虽然能为系统有效性提供宝贵见解，但无法解决数据处理和决策过程中缺乏文档和透明度的根本问题。
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) 不正确。尽管提高预测准确性可以提升消费者满意度，但它并未解决数据处理和决策制定中文档和透明度的核心问题。
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) 正确。实施全面的文档化流程符合ISO/IEC 42001标准，该标准强调人工智能全生命周期的透明度和文档化。NIST人工智能风险管理框架也通过促进详细记录数据和决策来支持这一点，以确保可追溯性和问责制。（文献：B，第2.3章）
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) 不正确。升级硬件可能会提高处理速度，但不能解决《人工智能法案》所要求的透明度或文档化问题以实现合规。
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
一家企业开发了一个人工智能系统，用于监测住院病人。该系统在病房内使用高清摄像头，实时监测病人的状况。如果系统检测到病人处于危急状态，它会自动呼叫护士到病床边。

为了提高人工智能系统的性能，该企业希望开始建立一个病人视频数据库，并在视频的关键时间点附上专业人员的注释，以此为系统构建更多训练数据。

该企业正在考虑进行数据保护影响评估（DPIA）。负责团队不确定是否根本需要进行DPIA。如果DPIA是强制性的，团队想知道评估应何时进行：是现在，还是仅在更新部署之后。

该企业必须遵守《人工智能法案》和《通用数据保护条例》（GDPR）。

该企业现在是否应该进行DPIA?

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) 是，因为对于可能对自然人权利构成高风险的人工智能项目，需要进行DPIA。
Yes, because a DPIA is required for AI projects that could pose a high risk to the rights of natural persons.

B) 是，因为任何收集个人数据的项目都需要进行DPIA，即使该项目风险较低。
Yes, because a DPIA is required for any project that collects personal data, even if the project is low risk.

C) 不，因为用于培训目的、教育或科学研究的数据不需要进行DPIA。
No, because a DPIA is not required for using data for training purposes, education, or scientific research.

D) 不，因为DPIA仅在人工智能系统完全开发、测试和部署之后才需要进行。
No, because a DPIA is only required after the AI system has been fully developed, tested, and deployed.

（题目未完，接下一页）

A) 正确。此选项准确反映了GDPR下的要求。当处理操作可能对自然人的权利和自由造成高风险时，特别是使用像人工智能系统这样处理（高度）敏感数据（如病人视频）的新技术时，DPIA是必要的。这些数据属于健康相关数据类别，需要额外的保障措施。（文献：A，第4.5章）
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) 不正确。尽管DPIA很重要，但并非所有收集个人数据的项目都自动需要进行。GDPR明确要求在数据处理可能对个人权利和自由造成高风险时进行DPIA，而不仅仅是因为收集了个人数据，例如生物识别数据、健康数据或大规模监测。
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) 不正确。数据使用目的（例如，用于训练或研究）并不能豁免项目进行DPIA的要求。GDPR仍然适用，特别是当数据处理可能对个人造成高风险时，尤其是在涉及病人视频等敏感数据的情况下。
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) 不正确。DPIA应在处理开始之前进行，特别是在项目的规划和开发阶段，以便主动识别和缓解风险。等到部署之后再进行，可能导致不符合GDPR的规定。
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
一家企业开发了一个用于实时人脸识别的人工智能系统。一家私人安保公司将该人工智能系统部署用于监控一个公共购物中心。该系统扫描所有访客，将其与过往罪犯和政治活动家数据库进行交叉比对，并标记出在这些数据库中列出的访客。被标记的访客在整个访问期间会被秘密跟踪，以评估他们是否从事安保公司认为的可疑行为。

根据《人工智能法案》，该人工智能系统的使用应归类于哪个类别?

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) 不可接受的风险
Unacceptable risk
B) 高风险的
High-risk
C) 有限风险的
Limited-risk
D) 低风险或零风险的
Minimal or no-risk

A) 正确。根据《人工智能法案》第5条，在公共场所基于政治活动实时生物识别以追踪个人是被禁止的。该法案禁止将人工智能系统用于侵犯基本权利的无差别监控和社会评分。（文献：A，第3.3、3.4章；《人工智能法案》，第5条第1款(d)项）
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) 不正确。该系统不仅是高风险，而且是被禁止的，因为该系统在未经个人同意的情况下，利用政治活动来追踪个人。这是《人工智能法案》所禁止的使用方式。
Incorrect. The system is not just high-risk, but prohibited, because the system uses political activity to track individuals, and without their consent. That is a prohibited use of AI system.
C) 不正确。有限风险类别涵盖了诸如聊天机器人或情感识别工具等具有透明度义务的系统。本案例涉及具有严重权利影响的生物识别监控，因此不符合该类别。
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) 不正确。最低风险适用于垃圾邮件过滤器等低影响系统。用于追踪的人脸识别超出了这一风险级别，并被明确禁止。
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
一家旅行社使用人工智能系统为其度假套餐开发动态精准营销活动。这些活动包括在社交媒体和旅行平台上进行实时广告投放，并利用个人的浏览历史。该旅行社利用人工智能推断用户的情绪状态，然后推荐定制化的目的地和活动。

该旅行社必须遵守《人工智能法案》。

该旅行社必须应对哪些风险?

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) 包含潜在偏见的风险。他们应该定期更新训练数据，以避免推荐不相关的目的地或错误地推断情绪状态。
The risk of including potential biases. They should update the training data regularly to avoid suggesting irrelevant destinations or infer wrong emotional states.

B) 无效广告活动的风险。他们应该侧重于更新算法，因为《人工智能法案》不涵盖个性化广告。
The risk of ineffective advertising activities. They should focus on updating the algorithm, because the AI Act does not cover personalized advertisements.

C) 缺乏透明度的风险。他们应该保证人工智能的公开性，减少推荐中的偏见，并评估广告活动是否符合伦理。
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) 滥用个人数据的风险。他们应该停止使用人工智能驱动的个性化功能，因为《人工智能法案》禁止将个人数据用于定向广告。
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) 不正确。此处所指的偏见是指对某些客户群体不利的偏见。不相关的旅行目的地推荐不太可能对客户产生太大影响。
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) 不正确。尽管《人工智能法案》优先关注高风险人工智能应用，但其条款也适用于商业领域，例如广告和旅游业，尤其是在涉及客户画像和决策制定时。
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) 正确。根据《人工智能法案》，这涵盖了主要义务。机构必须通过告知消费者人工智能的参与情况来履行透明度义务，防止偏见，并确保广告策略符合伦理标准。（文献：A，第 7.8、7.9 章）
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) 不正确。《人工智能法案》并未明确禁止定制广告或人工智能驱动的个性化。相反，它提供了道德行为准则，要求公开性、公正性以及数据安全，以确保此类方法符合欧盟（EU）的价值观。
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
一家公司开发了一款人工智能模型，可应用于包括医疗保健和金融在内的多个行业。由于其广泛应用，该人工智能模型对公众健康带来了潜在风险。

该公司开发了什么，以及根据《人工智能法案》，该公司应实施哪些实践?

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) 该公司开发了具有系统风险的通用人工智能（GPAI）。它应进行额外的测试以减轻风险。
The company developed a general-purpose AI (GPAI) that carries systemic risks. It should conduct additional tests to mitigate the risks.

B) 该公司开发了一个高风险人工智能系统。它应实施《人工智能法案》中概述的所有高风险人工智能系统的要求。
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) 该公司开发了一个窄范围人工智能模型。它应确保该模型仅在预定义参数内运行以预防风险。
The company developed a narrow AI model. It should ensure the model operates only within predefined parameters to prevent risks.

D) 该公司开发了一个实验性人工智能模型。它应侧重于研究和开发，而无需立即进行风险管理。
The company developed an experimental AI model. It should focus on research and development without immediate risk management.

A) 正确。该公司开发了具有系统风险的GPAI模型。该公司应使用协议和最先进的工具进行额外的模型评估。这包括实施和记录安全测试。（文献：A，第3.7章；《人工智能法案》，第3条，第55条）
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) 不正确。尽管该人工智能模型具有潜在风险，但它被归类为GPAI，而非特指的高风险系统。
Incorrect. While the AI model carries potential risks, it is classified as a GPAI not specifically as a high-risk system.

C) 不正确。窄范围人工智能模型仅限于特定任务，不带有与GPAI相关的系统风险。
Incorrect. A narrow AI model is limited to specific tasks and does not carry the systemic risks associated with GPAI.

D) 不正确。即使是实验性人工智能模型，如果它们带来潜在的系统风险，也必须遵守风险管理实践。
Incorrect. Even experimental AI models must adhere to risk management practices if they pose potential systemic risks.

11 / 40
一个组织正在开发一个高风险人工智能系统。在测试过程中，开发团队识别出各种风险，包括数据完整性不一致和存在过时记录。这些风险可能对模型的性能产生负面影响。

该组织必须遵守《人工智能法案》。为此，他们采用了CEN/CLC/TR 18115框架。

根据该框架，该组织应采取什么措施来解决这些风险?

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) 进行数据保护影响评估（DPIA），以解决人工智能决策的公平性问题
Conduct a data protection impact assessment (DPIA) to address the fairness of AI decision-making

B) 使用协议加密所有训练和测试数据集，以防止未经授权访问个人数据
Encrypt all training and testing datasets using protocols to prevent unauthorized access to personal data

C) 实施通用风险控制措施，以减少上述运营和声誉风险
Implement general-purpose risk controls to reduce the mentioned operational and reputational risks

D) 通过应用结构化的质量指标和统计评估方法来提高数据质量
Improve the data quality by applying structured quality metrics and statistical evaluation methods

A) 不正确。DPIA 有助于评估对个人权利和自由的风险。然而，它并非直接解决数据过时或不完整问题的合适工具。数据质量的改进需要技术措施，而非法律评估。
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) 不正确。虽然加密对于数据安全很重要，但这并不能解决诸如完整性和及时性等数据质量问题。《人工智能法案》第 10 条不仅强调数据的保护，还确保用于人工智能训练和测试的数据是相关的、有代表性的且高质量的。
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) 不正确。尽管风险管理在人工智能中非常重要，但它不提供解决已识别问题所需的数据质量框架。管理数据完整性和及时性是通过提高数据质量来完成的，而不是通过通用人工智能风险标准。
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) 正确。CEN/CLC/TR 18115 提供了关于在人工智能系统整个生命周期中评估和改进数据质量的指导。它强调使用指标来衡量数据特征，如完整性和及时性，特别是在数据准备阶段，以确保符合《人工智能法案》第 10 条的规定。（文献：B，第 1 章；《人工智能法案》，第 10 条）
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
《人工智能法案》描述了与人工智能系统相关的几种角色。

“人工智能系统的进口者”这一角色的定义是什么?

The AI Act describes several roles connected to an AI system.

What is the definition of the role ‘importer of an AI system’?

A) 以自己的名义或商标设计、开发和营销人工智能系统的个人或组织。
A person or organization that designs, develops, and markets an AI system under their own name or trademark.
B) 将人工智能系统投放市场但不对其原始开发负责的个人或组织。
A person or organization that places an AI system on the market but is not responsible for its original development.
C) 在其运营中使用人工智能系统并确保遵守本地用户义务的个人或组织。
A person or organization that uses an AI system in their operations and ensures local compliance with user obligations.
D) 负责监控人工智能系统进口是否符合《人工智能法案》法规的监管机构。
A regulatory authority tasked with monitoring if the AI system is imported in compliance with the AI Act regulations.

A) 不正确。这描述的是“供应商”的角色，他们负责人工智能系统的开发和营销，而不是进口它们。
Incorrect. This describes the role ‘provider’, who is responsible for the development and marketing of the AI system, not for importing them.
B) 正确。这是“进口者”这一角色的定义，通常指系统在欧盟以外地区开发的情况。进口者负责确保系统符合欧盟监管要求，并与供应商合作以证明合规性。（文献：A，第3.1章）
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) 不正确。这描述的是“用户”的角色，他们操作和监控人工智能系统，而不是进口者。
Incorrect. This describes the role ‘user’, who operates and monitors the AI system, not an importer.
D) 不正确。监管机构并非进口者 。它们负责强制执行合规性，但不会积极参与系统上市 。
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
一家企业开发了一个用于检测金融交易欺诈的人工智能系统。该系统分析交易模式以识别可疑活动并预防欺诈行为。鉴于可能出现影响合法交易的误报以及欺诈策略不断演变的性质，该企业认识到需要有效的保障措施。

该企业必须遵守《人工智能法案》。为帮助预防误报问题，该企业使用了ISO/IEC 23894标准。

根据该标准，该企业应采取哪些措施来预防这些问题？

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) 将风险管理嵌入所有活动中，以确保全面的监督并主动降低风险
Embed risk management into all activities to ensure comprehensive oversight and proactive risk mitigation

B) 增强数据隐私措施，以保护敏感信息并遵守隐私法规
Enhance data privacy measures to protect sensitive information and comply with privacy regulations

C) 专注于提高模型准确性，以确保可靠的性能并最大限度地减少误报
Focus on improving model accuracy to ensure reliable performance and minimize false positives

D) 实施网络安全措施，以保护系统免受外部威胁和未经授权的访问
Implement cybersecurity measures to protect the system from external threats and unauthorized access

（题目未完，接下一页）

A) 正确。这种方法将风险管理融入到整个组织的各项活动中，根据特定背景定制框架，并让利益相关者参与进来，以有效地识别和缓解人工智能相关风险 。这符合 ISO/IEC 23894 标准，并最有助于合规性 。(文献：B，第3.2章)
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) 不正确。该企业必须解决重要的隐私问题。然而，这并未具体整合ISO/IEC 23894标准中概述的、合规性所必需的人工智能综合风险管理实践。
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) 不正确。通过侧重于提高模型准确性以确保可靠性能并最大限度地减少误报，该企业增强了模型有效性，但并未解决风险管理的更广泛方面，例如识别、评估和缓解潜在的人工智能相关风险。ISO/IEC 23894标准强调全面的风险管理方法。
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) 不正确。通过实施网络安全措施来保护系统免受外部威胁和未经授权的访问，该企业解决了系统安全的关键组成部分。然而，这并未涵盖ISO/IEC 23894标准中规定的人工智能所需风险管理实践的全部范围。
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
一家制造公司使用人工智能驱动的机器人设备对其装配线进行质量控制。调查小组注意到，一名匿名举报人声称人工智能系统最近显示异常低的缺陷产品数量。缺陷产品少报的原因是人工智能系统的软件更新。经人工检查，这些产品存在缺陷且不安全，无法使用。

报告指出，新的缺陷检测算法产生了一个关键错误，导致了漏报。据举报人称，经理们知道这个问题，但为了避免损害公司声誉而没有解决这个问题。

接下来的行动应该是什么？

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) - 调整内部算法以解决问题
- 如果问题在30天后仍然存在，则通知相关主管机构
- Adjust the internal algorithm to address the problem
- Notify the relevant competent authority if the issue still exists after 30 days

B) - 内部调查问题并开始解决
- 立即将发生的情况通知相关主管机构
- Investigate the problem internally and start solving it
- Notify the relevant competent authority of the occurrence immediately

C) - 调查举报人举报的原因
- 如果消费者开始投诉，则通知相关主管机构
- Research the whistleblower's reasons for reporting
- Notify the relevant competent authority if consumers start complaining

D) - 停止使用人工智能系统并切换到旧方法
- 这使得无需通知相关主管机构
- Stop using the AI system and switch to an older method
- This makes it unnecessary to inform the relevant competent authority

（题目未完，接下一页）

A) 不正确。在不通知主管机构的情况下解决问题，会规避报告严重事故的法律要求 。不报告可能导致罚款和对公司人工智能系统处理方式的不信任 。
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) 正确。调查保证了问题的根本原因被查明并得到解决 。向相关主管机构报告保证了合规性 。 (文献：A，第7.4，3.10章；《人工智能法案》，第73条)
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) 不正确。调查举报人的动机违反了举报人保护原则，并阻碍了伦理报告 。这种做法将声誉管理置于法律和伦理义务之上，违反了《人工智能法案》的要求和组织诚信 。
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) 不正确。尽管停止人工智能系统可能解决问题，但它不符合《人工智能法案》中规定的报告标准 。这种选择是不可接受的，因为这是一个影响产品安全的严重事故，必须报告并加以处理 。
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 公司使用一个高风险人工智能系统，通过X射线图像诊断医疗状况。他们已具备以下条件：

- 公司已通过外部审计，确保该人工智能系统符合《人工智能法案》的标准。
- 建立了健全的风险管理框架，用于识别和缓解潜在问题，并制定了应急预案。
- 人工智能系统操作的详细记录得到安全存储，以备问责和审计。
- 向用户提供了清晰的文档和培训，解释人工智能的决策过程和局限性。
- 所有人工智能生成的诊断结果在最终确定前，都经过医疗专业人员的审查，整合了人类判断。

该公司还应该实施什么？

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) 他们应该增加健全的数据治理程序，以维护其人工智能系统的可靠性和公平性。
They should add robust data governance procedures to maintain the reliability and fairness of their AI system.

B) 他们应该确保人工智能系统能够独立运行，无需任何人为干预以提高效率。
They should ensure that the AI system can operate independently without any human intervention for efficiency.

C) 他们应该实施一个系统，自动推翻人类决策，以加快诊断过程。
They should implement a system to automatically override human decisions to speed up the diagnosis process.

D) 他们应该包含一个功能，允许患者根据人工智能的建议直接修改他们的医疗记录。
They should include a feature that allows patients to directly modify their medical records based on AI suggestions.

（题目未完，接下一页）

A) 正确。健全的数据和数据治理涵盖了训练数据和操作数据的质量、偏见缓解和可追溯性，确保系统公平可靠 。 (文献：A，第3.3章；《人工智能法案》，第15条)
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) 不正确。根据《人工智能法案》，医疗诊断中不允许完全自动化 。医疗保健领域的高风险人工智能系统需要人工监督，以确保安全性和准确性，从而使完全独立不合适 。人工审查对于患者安全和监管合规至关重要 。
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) 不正确。自动推翻人类决策可能会损害患者安全，并削弱医疗诊断等高风险人工智能系统中人工监督的重要作用 。
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) 不正确。允许患者根据人工智能的建议修改医疗记录可能导致不准确，不符合需要专业监督的标准医疗实践，并导致法律风险 。
Incorrect. Allowing patients to modify medical records based on AI suggestions could lead to inaccuracies, is not aligned with standard medical practices, which require professional oversight, and leads to legal risks.

16 / 40
一家保险公司实施了一套新的人工智能信用评分系统，该系统可以访问内部数据库和公共数据库。识别出以下风险：

- **缺乏适当的训练数据。**如果模型训练不当，将难以准确地为人们确定公平的评分。
- **与其他应用程序的集成。**将基于人工智能的引擎集成到相当复杂且在某些方面过时的应用程序环境中将很困难。
- **不符合GDPR。**《通用数据保护条例》（GDPR）对自动化系统自主处理个人数据有具体要求。
- **模型的透明度和质量。**员工和客户都必须能够理解人工智能模型的结果和决策。

该保险公司必须遵守《人工智能法案》。

哪个风险对于遵守《人工智能法案》来说**不**重要?

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) 缺乏适当的训练数据
A lack of proper training data
B) 与其他应用程序的集成
Integration with other applications
C) 不符合GDPR
Non-compliance with the GDPR
D) 模型的透明度和质量
Transparency and quality of the model

（题目未完，接下一页）

A) 不正确。人工智能系统必须使用高质量、无偏见的数据来防止歧视或不公平的决策。不良的训练数据可能导致有偏见或不准确的信用评分，从而违反《人工智能法案》的要求。
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) 正确。与其他应用程序集成不畅确实是一种风险，但《人工智能法案》并未定义此类风险 。(文献：A，第7.2、7.3章)
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) 不正确。GDPR对自主处理个人数据的系统规定了具体限制，但这并不是必须解决的主要挑战。《人工智能法案》与GDPR保持一致，特别是在个人数据处理、人工智能决策的合法基础以及个人权利（例如：解释权和申诉权）方面。
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) 不正确。数据质量和人工智能模型准确性是此类应用项目中需要解决的主要挑战。同样重要的是，人工智能模型的输出必须是可理解和可解释的。《人工智能法案》要求可解释性和透明度，特别是对于信用评分等高风险人工智能系统，因为人工智能决策会影响金融访问。
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
一家政府机构提议开发一套人工智能系统，用于预测大城镇市中心的犯罪热点。该系统将用于自动化监控。它被编程为自动识别显示可疑行为的人并向当地警方报告。这是一个预防犯罪、增强安全感和确保犯罪后正义的绝佳机会。

实施该人工智能系统是否存在任何风险?

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) 是，因为用于自动化决策的人工智能系统带有固有的偏见风险，这可能不公平地使个人处于不利地位。
Yes, because an AI system that is used for automated decisions carries the inherent risk of bias, which may unfairly disadvantage individuals.

B) 是，因为《人工智能法案》预见到监控系统存在如此多的隐私风险，以至于它彻底禁止在公共场所部署此类系统。
Yes, because the AI Act foresees so many privacy risks with surveillance systems that it outright forbids its employment in public spaces.

C) 不，因为在犯罪起诉和预防中，人工智能系统没有特定的风险，因为它们用于增强公共安全。
No, because in crime prosecution and prevention, AI systems carry no particular risks since they are used to enhance public safety.

D) 不，因为公共领域的人工智能系统提高了效率且没有风险，因为决策是客观的，没有人为错误。
No, because public domain AI systems boost efficiency and carry no risk, since the decisions are objective and free from human error.

A) 正确。《人工智能法案》明确提到了这一主要关注点 。在刑事起诉等敏感领域，人工智能系统中存在偏见数据或有缺陷的算法可能产生歧视性结果 。对于高风险应用中的人工智能系统，《人工智能法案》要求公开性、风险评估和偏见缓解技术 。(文献：A，第8.1、8.2、8.3章)
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) 不正确。《人工智能法案》旨在控制和保证人工智能的安全、开放和公平使用，而不是阻止其在公共领域的应用 。在强制执行危害防护的同时，《人工智能法案》鼓励创新 。
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) 不正确。提高公共安全是一个崇高目标，但这并不能否定减轻侵犯隐私和使未有不当行为的个人处于不利地位的义务 。
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) 不正确。人工智能的输出依赖于训练数据和应用的算法，因此训练数据中的任何偏见都会延续到系统将做出的决策中 。它们不一定比人类判断更客观 。此外，《人工智能法案》赋予个人由人类监督其决策的权利 。
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
一家组织正在开发一个用于招聘的人工智能系统。在内部测试中，团队识别出一个风险：该系统有时无意中偏袒来自特定背景的候选人，可能导致歧视性结果。团队现在不确定如何应对这些担忧。

该组织必须遵守《人工智能法案》。为帮助缓解此风险，该组织使用了ISO/IEC TR 24368标准。

根据该标准，该组织应采取哪些措施来缓解此风险?

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) 调整算法，根据就业统计数据优先考虑人口配额
Adjust the algorithm to prioritize demographic quotas based on employment statistics
B) 采纳零数据方法，从训练集中移除所有人口统计数据
Adopt a zero-data approach by removing all demographic data from the training set
C) 应用网络安全措施，保护候选人数据并增强系统完整性
Apply cybersecurity measures to protect candidate data and enhance system integrity
D) 实施利益相关者参与流程，以识别和缓解潜在偏见
Implement a stakeholder engagement process to identify and mitigate potential biases

A) 不正确。虽然旨在平衡代表性可能看似符合伦理，但不加背景地应用僵硬的配额可能会引入新的偏见 。ISO/IEC TR 24368 标准强调公平性和利益相关者参与，而非任意的人口统计目标 。
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) 不正确。仅仅移除人口统计数据并不能防止歧视，甚至可能掩盖现有偏见 。ISO/IEC TR 24368 标准鼓励透明的方法和偏见缓解措施，而非盲目地移除数据 。
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) 不正确。虽然网络安全很重要，但它不包括偏见或公平等伦理问题 。解决伦理问题需要与ISO/IEC TR 24368 标准相符的方法 。
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) 正确。ISO/IEC TR 24368 标准促进利益相关者参与，以发现偏见等伦理风险，并开发包容、公平的人工智能系统 。这支持了《人工智能法案》关于公平和非歧视的目标。(文献：B，第4章)
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
一家组织正在开发一个用于贷款审批的人工智能系统。在内部测试中，合规团队发现一个风险：模型的决策过程缺乏透明度，并且风险评估的文档有限。

该组织必须遵守《人工智能法案》。该组织为此使用了ISO/IEC 42001标准和NIST人工智能风险管理框架（RMF）。

根据此标准和框架，该企业应采取哪些措施来解决这一风险?

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) 根据推荐的网络安全指南进行安全合规评估
Conduct a safety compliance assessment based on recommended cybersecurity guidelines
B) 立即停用人工智能系统并过渡到手动贷款审批流程
Decommission the AI system immediately and transition to a manual loan approval process
C) 定义一个包含透明度指标的衡量计划，并记录决策逻辑以便监督
Define a measurement plan with transparency metrics and record decision logic for oversight
D) 使用合成数据重建系统，以尽可能消除偏见来源
Rebuild the system using synthetic data to eliminate as many sources of bias as possible

A) 不正确。遵守安全指南并不能专门解决透明度或风险文档问题 。因此，它与已识别的问题没有直接关联 。
Incorrect. Adhering to security guidelines does not specifically address transparency or risk documentation. Therefore, it is not directly relevant to the identified issue.
B) 不正确。没有必要停用系统，因为它仅处于内部测试阶段 。切换到手动贷款审批将避免问题，但也会导致所有投资成本的损失 。风险可以通过结构化治理进行管理 。
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) 正确。ISO/IEC 42001 强调透明和可解释的决策制定，以及人工智能生命周期中的详尽文档 。NIST AI RMF 通过其衡量功能支持定义指标并促进可追溯性 。总而言之，这些方法直接解决了场景中提出的问题 。(文献：B，第2.2、2.5章)
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) 不正确。单独使用合成数据并不能确保偏见缓解，也未能解决围绕透明度和风险文档的核心要求 。
Incorrect. Using synthetic data alone does not ensure bias mitigation and fails to address core requirements around transparency and risk documentation.

20 / 40
一家领先的汽车制造商开发了一款高度自动化车辆（4级），该车辆配备了用于道路安全的人工智能物体识别技术。在测试过程中，发现了以下风险：

- 在弱光条件下，系统检测减速带的能力受损。
- 该模型可能难以销售，因为它不知道其他车辆的尺寸。
- 开发人员不太确定如何解释模型如何做出决策。
- 在人工智能系统开发阶段，并未向所有利益相关者征求意见。

当**仅**考虑《人工智能法案》合规性时，必须解决什么问题？

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) 现实世界条件下测试不足的风险
The risk of insufficient testing under real-world conditions
B) 人工智能决策缺乏透明度的风险
The risk of lack of transparency in AI decision-making
C) 人工智能系统对其他车辆模型规模化有限的风险
The risk of limited scalability of the AI system to other vehicle models
D) 人工智能开发过程中利益相关者参与有限的风险
The risk of limited stakeholder involvement during AI development

A) 不正确。《人工智能法案》更侧重于缓解已识别的风险和确保透明度与基本权利，而不是解决现实世界中测试不足的问题。
Incorrect. The AI Act focuses more on mitigating identified risks and ensuring transparency and fundamental rights, rather than addressing insufficient real-world testing.
B) 正确。《人工智能法案》第11条强调人工智能系统的透明度，以识别和纠正潜在风险，这是本场景中的核心问题。(文献：A，第7.10章)
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) 不正确。虽然可扩展性在商业上至关重要，但它并未直接解决《人工智能法案》对风险缓解和透明度的要求。
Incorrect. While scalability is crucial commercially, it doesn't directly address the AI Act's requirements for risk mitigation and transparency.
D) 不正确。尽管利益相关者的参与很重要，但这并非《人工智能法案》的重点。
Incorrect. Although stakeholder involvement is important, it is not the focus of the AI Act.

21 / 40
一家物流公司正在构建一个人工智能系统，以优化其配送路径并降低燃油消耗。该组织正在权衡两个选择：

- 一个闭源人工智能模型，由供应商保证更快的安装和经过验证的合规认证。
- 一个开源人工智能模型，可实现高度定制化和透明度。

该公司必须遵守《人工智能法案》，但同时也希望平衡创新和成本。

哪种模型**最**适合该公司?

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) 闭源人工智能模型，因为它本质上更安全，并受到当局的信任。这降低了不合规的可能性。
A closed-source AI model, because it is intrinsically more secure and trusted by authorities. This reduces the possibility of non-compliance.
B) 闭源人工智能模型，因为它提供预认证的合规性。这减轻了公司证明符合《人工智能法案》的负担。
A closed-source AI model, because it provides pre-certified compliance. This lessens the company's burden of proving AI Act compliance.
C) 开源人工智能模型，因为它保证完全透明。这有助于满足文档记录和可审计性要求。
An open-source AI model, because it guarantees complete transparency. This helps with documentation and auditability requirements.
D) 开源人工智能模型，因为它免受《人工智能法案》合规约束。这是因为源代码是公开可用的。
An open-source AI model, because it is excepted from AI Act compliance. This is due to the source code being publicly available.

A) 不正确。闭源方法在本质上并非更合规或更安全。
Incorrect. Closed-source approaches are not by nature more compliant or safe.
B) 不正确。尽管闭源模型可以包含合规认证，但它们可能缺乏满足公司需求或不断变化的法律要求所需的灵活性和开放性。
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) 正确。开源模型提供的完全透明度符合《人工智能法案》关于可审计性、可追溯性和风险控制的标准。这些优势使得物流公司能够更轻松地展示合规性。(文献：A，第6章)
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) 不正确。根据《人工智能法案》，开源模型并非没有合规责任。
Incorrect. Under the AI Act, open-source models are not free from compliance responsibilities.

22 / 40
《人工智能法案》规定了人工智能开发应遵循的伦理原则。

哪项**不是**这些原则之一?

The AI Act defines ethical principles for AI development.

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

A) 可解释性
Explicability
B) 公平性
Fairness
C) 损失预防
Loss prevention
D) 尊重人工智能自主性
Respect for AI autonomy

A) 不正确。这是《人工智能法案》中的一项原则。它要求人工智能系统透明且可理解，确保用户和利益相关者能够理解决策是如何做出的，以及其背后的理由。
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) 不正确。这是《人工智能法案》中的一项原则。它强制要求人工智能系统应在开发和部署时避免偏见或歧视，确保所有个人都能获得公平公正的结果。
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) 不正确。这是《人工智能法案》中的一项原则。它强调设计人工智能系统以最大限度地降低风险和预防危害的重要性，确保用户和受人工智能技术影响者的安全保障。
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) 正确。正确的原则是尊重人类自主性 。 《人工智能法案》主要侧重于公平性、损失预防和可解释性等原则，旨在确保人工智能系统以负责任、透明和无偏见的方式开发和使用 。(文献：A，第9.1章)
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
一家初创公司正在开发一个人工智能系统，旨在通过根据个别学生的需求定制课程计划来辅助学校的个性化学习。该系统收集学生的表现和学习行为数据。

根据《人工智能法案》，这家初创公司在这里应该考虑什么，以平衡创新与监管?

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) 避免将系统标记为高风险，以规避额外的监管负担，并使创新过程更加简便
Avoid labeling the system as high-risk to circumvent additional regulatory burdens and streamline innovation
B) 确保人工智能系统经过一致性评估并符合高风险系统法规
Ensure the AI system undergoes a conformity assessment and complies with high-risk system regulations
C) 实施健全的数据保护功能，但取消用户通知，以避免部署延迟
Implement robust data protection features but take out user notifications to avoid delays in deployment
D) 将系统 仅销售给私立学校，以限制高风险合规要求的影响
Market the system to private schools exclusively to limit the impact of high-risk compliance requirements

A) 不正确。为了规避法规而对系统进行错误标记是不道德的，并可能导致严重的法律后果。
Incorrect. Mislabeling the system to avoid regulations is unethical and can lead to serious legal repercussions.
B) 正确。进行符合性评估并确保透明度对于遵守高风险系统法规至关重要 。 (文献：A，第7.6章；《人工智能法案》，第6条，附件三)
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) 不正确。用户通知对于透明度和遵守数据保护法规至关重要。
Incorrect. User notifications are essential for transparency and compliance with data protection regulations.
D) 不正确。私立学校的合规性不一定更宽松，无论市场如何，都必须遵守法规。
Incorrect. Compliance is not necessarily more lenient in private schools, and regulations must be followed regardless of the market.

24 / 40
一家金融机构 Fintegra 正在实施一个人工智能系统，用于检测交易中的欺诈行为。该系统需要访问客户的交易信息和人口统计数据进行分析。Fintegra 必须遵守《人工智能法案》的数据最小化要求。

Fintegra 遵守数据最小化要求的**最佳**方式是什么?

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) 他们应该匿名化所有交易数据并删除任何识别自然人的数据以符合要求，即使这些数据对于欺诈检测目的至关重要。
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) 他们应该收集所有个人详细信息，包括全名和精确地址，以确保精确分析并随时间推移的改进，并尽可能长时间地安全存储数据。
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) 他们应该将数据收集限制在与检测欺诈相关的交易数据，并避免处理个人详细信息，例如客户的全名或精确地址。
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) 他们应该只与符合《人工智能法案》的、获得认可的供应商共享所收集的数据，这最大限度地减少了对个人详细信息（如客户全名）的内部处理。
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) 不正确。虽然匿名化很重要，但移除欺诈检测所需的关键数据会损害人工智能系统的有效性，且《人工智能法案》的数据最小化原则不要求这样做。
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) 不正确。收集和存储所有可用数据，即使是安全地进行，也违反了数据最小化原则，并增加了不符合《人工智能法案》规定的风险。
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) 正确。《人工智能法案》下的数据最小化原则要求组织仅收集和处理对人工智能系统的特定目的严格必要的数据 。通过侧重于与欺诈检测相关的交易数据并避免任何不必要的个人详细信息，该公司遵守了这一要求 。(文献：A，第4.1章)
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) 不正确。这不是一个好选择，因为与外部供应商共享数据可能会违反数据保护规则。即使 Fintegra 和供应商都符合《人工智能法案》的规定，这也不符合最小化数据使用的原则。
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正在实施一个自适应学习平台，该平台使用人工智能来个性化学生的学习路径 。该平台根据学生的个体表现调整任务的难度 。

EduTech应降低哪些风险，以确保该人工智能系统符合伦理地使用?

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) 偏见和歧视的风险，因为这些会导致某些学生获得不公平的优势或劣势。这种风险通过定期审查和更新人工智能系统的数据集和算法来缓解。
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) 过度依赖技术的风险，这可能导致学生无法培养批判性思维技能。这种风险通过对人工智能系统的决策过程保密来缓解，以刺激学生更多地思考。
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) 隐私泄露的风险，因为敏感的学生数据，包括他们的表现，可能会被不当处理或暴露。这种风险通过更多地侧重于提高人工智能系统的技术性能来缓解。
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) 透明度问题的风险，因为学生和教育工作者可能不理解决策是如何做出的。这种风险通过确保人工智能系统在没有人工监督的情况下运行来缓解，这确保了公平性。
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) 正确。偏见和歧视在教育领域是一个重大风险 。定期审查和更新数据集及算法有助于缓解偏见和歧视的风险 。(文献：A，第7.6章)
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) 不正确。透明度对于人工智能的伦理使用至关重要。培养批判性思维在教育中很重要，但这与人工智能系统的透明度无关。
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) 不正确。仅仅技术性能并不能解决伦理问题，也不能降低隐私泄露的风险。
Incorrect. Technical performance alone does not address ethical concerns, nor does it decrease the risk of privacy breaches.

D) 不正确。尽管没有人工干预的决策可以增加公平性，但缺乏对人工智能的人工监督会增加偏见和歧视的风险。人工监督对于确保符合伦理地使用至关重要。
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
一家医院科室专门从事疾病的诊断和治疗。他们开发了一个人工智能诊断系统，以协助识别罕见诊断。该系统分析患者数据、病史和影像扫描。

该系统在美国（US）成功应用。欧盟（EU）的一些医疗专家希望采用该系统，但他们对该人工智能系统的工作原理没有清晰的理解。他们也没有监控人工智能或识别故障或误诊的专业知识和经验。

哪项**不是**采用该人工智能系统相关的风险?

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) 缺乏有效人工监督的风险
The risk of lack of effective human supervision
B) 由于自动化偏见导致误诊的风险
The risk of misdiagnosis due to automation bias
C) 由于缺乏透明度导致不信任的风险
The risk of mistrust caused by lack of transparency
D) 未经授权访问患者记录的风险
The risk of unauthorized access to patient records

A) 不正确。由于团队缺乏使用该系统的专业知识，他们可能无法监控人工智能并识别故障或不准确的输出。
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) 不正确。由于缺乏关于如何正确解释输出的专业知识，可能会出现偏见和误诊。
Incorrect. Due to lack of specialist knowledge on how to correctly interpret the output, biases and misdiagnoses may occur.
C) 不正确。医疗专家不理解人工智能系统的工作原理，这可能导致因缺乏透明度而产生不信任。
Incorrect. The medical specialists do not understand how the AI system works, which may lead to mistrust due to lack of transparency.
D) 正确。虽然数据隐私和未经授权的访问是重要问题，但在本场景中，它们并未被特别强调为与人工智能诊断系统的操作采用和理解相关的风险。(文献：A，第7.7章)
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
一家企业正在开发智能家居助手的人工智能系统。在测试过程中，团队发现语音识别错误（例如混淆发音相似的词语）会导致意外操作，比如错误开启电器。这些错误可能导致隐私泄露，例如未经同意录制对话或错误识别用户，从而可能与未经授权的第三方共享敏感信息。

该组织必须遵守《人工智能法案》。他们为此使用了CEN/CLC/TR 18115框架。

根据该框架，人工智能供应商应如何解决这个问题?

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) 制定利益相关者参与计划，以获取对人工智能系统工作原理的不同看法
Create a stakeholder engagement plan to get different views on how the AI system works
B) 进行伦理影响评估，以了解智能家居助手的隐私风险
Do an ethical impact assessment to understand privacy risks of smart home assistants
C) 通过使用系统的验证和错误检查方法来提高训练数据质量
Improve the training data quality by using systematic validation and error-checking methods
D) 通过加密保护语音数据并防止数据泄露来提高数据安全
Increase data security with encryption to protect voice data and prevent data breaches

A) 不正确。让利益相关者参与进来有助于理解更广泛的影响，但它不能解决提高数据质量的直接技术需求。
Incorrect. Engaging stakeholders is beneficial for understanding broader implications, but it does not address the immediate technical need for improving data quality.
B) 不正确。虽然伦理影响评估很重要，但它们不能解决导致误解的低质量数据问题。
Incorrect. While ethical impact assessments are important, they do not solve the issue of low-quality data that causes the misinterpretations
C) 正确。通过系统验证和错误检查来提高数据质量符合 CEN/CLC/TR 18115 框架，解决了对准确和完整数据的需求，以确保人工智能系统安全有效地运行 。(文献：B，第1章)
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) 不正确。尽管数据安全很重要，但加密并不能解决数据质量问题，而这正是本场景的核心问题。
Incorrect. Although data security is important, encryption does not address the problem with data quality, which is central to this scenario.

28 / 40
一家科技公司被发现使用《人工智能法案》明确禁止的实时远程生物特征识别人工智能系统。

对这一违规行为的适当处罚是什么?

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) 给予正式警告，不处以罚款
A formal warning without financial penalties
B) 最高可达750万欧元或上一财政年度全球总年营业额1%的行政罚款
An administrative fine of up to €7.5 million or 1% of the total global annual turnover in the previous financial year
C) 最高可达1500万欧元或上一财政年度全球总年营业额3%的行政罚款
An administrative fine of up to €15 million or 3% of the total global annual turnover in the previous financial year
D) 最高可达3500万欧元或上一财政年度全球总年营业额7%的行政罚款
An administrative fine of up to €35 million or 7% of the total global annual turnover in the previous financial year

A) 不正确。对于严重违反人工智能法规的行为，不处以罚款的正式警告是不够的。
Incorrect. A formal warning without a financial penalty is not adequate for a serious breach of AI regulations.
B) 不正确。对于公司涉及禁止行为的违规行为，此罚款过低。
Incorrect. This fine is too low for a violation involving prohibited actions by a company.
C) 不正确。虽然数额可观，但此罚款与如此严重违规的严重程度不符。
Incorrect. While substantial, this fine does not match the severity of such a serious breach.
D) 正确。此处罚与《人工智能法案》中针对最严重违规行为的最高可能罚款相符 。(文献：A，第3.11章；《人工智能法案》，第52条，第99条)
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
《人工智能法案》特别强调人工智能系统两个方面的重要性：透明度和可追溯性。

为什么透明度和可追溯性很重要?

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

Why are transparency and traceability important?

A) 因为它们对于确保人工智能系统的问责制和培养信任至关重要。
Because they are crucial for ensuring accountability and fostering trust in AI systems.
B) 因为它们是所有产品（包括人工智能系统）的强制性要求。
Because they are mandatory requirements for all products, including AI systems.
C) 因为它们对于人工智能系统的可靠性和自动化特别重要。
Because they are particularly essential for the reliability and automation of AI systems.
D) 因为它们在欧洲、中国和美国立法之间是共享的。
Because they are shared between European, Chinese, and American legislation.

A) 正确。关于所用数据的详细信息有助于理解、解释和理解人工智能系统的决策和行动 。可追溯性确保人工智能决策过程、数据集和系统操作能够被审查和审计 。这对于识别偏见、错误和问责问题至关重要 。透明度和可追溯性对于人工智能系统中的问责制和用户信任很重要 。(文献：A，第3.1章)
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) 不正确。虽然透明度和可追溯性对人工智能系统很重要，但它们并非所有产品的强制性要求。
Incorrect. While transparency and traceability are important for AI systems, they are not mandatory for all products.
C) 不正确。透明度和可追溯性对于欧盟公民和人工智能系统及技术的问责制和信任（而非可靠性）很重要。可靠性和自动化更多与人工智能系统性能和稳健性相关，不一定与这两个原则相关。
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) 不正确。三大主要全球人工智能法规之间的一致性和同质性并非欧盟考虑的方面。人工智能法案是一项欧洲法规。中国和美国有不同的侧重点和法律框架。
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
一家零售机构使用的人工智能系统会根据用户偏好和所用设备自动改变网站元素的显示方式。该系统利用点击历史和页面停留时间推荐产品并增强用户体验。

根据《人工智能法案》，该人工智能系统的使用应归类于哪个类别?

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) 不可接受的风险
Unacceptable risk
B) 高风险的
High-risk
C) 有限风险的
Limited-risk
D) 低风险或零风险的
Minimal or no-risk

A) 不正确。该系统不符合不可接受风险的标准，该风险涉及人工智能系统危害人类尊严、安全或基本权利。在零售环境中影响购买决策并非本质上有害。
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) 不正确。医疗保健、银行或就业等领域的人工智能系统，如果可能涉及重大权利或安全问题，则被视为高风险。该技术使用非敏感数据来增强网站外观的方式不符合高风险标准。
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) 不正确。尽管该系统会影响消费者选择，但其适度的影响以及使用非敏感数据的方式更接近于低风险或零风险分类。
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) 正确。该系统在低风险环境中运行，使用非敏感数据，且仅影响用户的购买体验，因此被归类为低风险或无风险。(文献：A，第3.3、3.4章)
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
一家公司创建了一个用于招聘流程中自动化决策的人工智能系统。该人工智能系统将筛选简历、对候选人进行排名并提出面试建议。

该公司担心该人工智能系统可能存在影响招聘流程的偏见。

该公司缓解人工智能系统偏见的**最佳**方法是什么?

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) 允许人工智能系统在没有人为进一步干预的情况下学习和适应
Allow the AI system to learn and adapt without further human intervention
B) 忽略训练数据中的偏见，专注于人工智能系统的性能
Ignore biases in the training data and focus on the AI system's performance
C) 组建多元化的开发团队来创建和监控人工智能系统
Implement a diverse development team to create and monitor the AI system
D) 使用单一数据源来训练人工智能系统，以确保一致性
Use a single source of data for training the AI system to ensure consistency

A) 不正确。允许人工智能系统在没有人为干预的情况下学习，可能导致意外偏见和缺乏问责制。(《人工智能法案》，指南65)
Incorrect. Allowing the AI system to learn without human intervention can lead to unintended biases and lack of accountability. (AI Act, Guideline 65)
B) 不正确。忽视偏见可能导致歧视性结果，并且不符合伦理准则。系统必须学会识别和调整偏见。(《人工智能法案》，指南72)
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) 正确。多元化的团队可以帮助识别和缓解偏见，确保人工智能系统公平和包容。(文献：A，第4.5章；《人工智能法案》，指南81)
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) 不正确。使用单一数据源可能会限制人工智能系统的泛化能力，并可能引入偏见。(《人工智能法案》，指南73)
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
一家名为 Feline Finesse 的网店销售猫咪配件和猫咪抱枕，其中包括根据顾客图片定制的猫咪毛绒玩具。该网店使用的人工智能系统可以完成以下任务：

- 根据消费者活动动态调整价格。
- 根据顾客偏好对搜索结果进行排序。
- 为顾客推荐它认为顾客可能喜欢的其他产品。

目前，该网店会告知顾客人工智能系统的功能，并且对算法的工作原理非常透明。然而，首席执行官对这种做法提出质疑，并想知道需要达到何种程度的透明度以及它如何影响销售。

参照《人工智能法案》，首席执行官应该了解哪些有关透明度的知识?

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) 透明度可以向消费者证明系统是客观的。消费者根据《人工智能法案》有权了解他们的数据是如何被使用的，这种理解能培养信任。
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) 透明度可以展示人工智能系统的局限性或约束。消费者在了解这一点后可能会对公司失去信任，这会损害公司的声誉。
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) 电子商务并非强制要求透明度。个性化带来的便利有助于消费者，他们不需要了解人工智能系统如何运作。
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) 透明度仅限于提供人工智能系统源代码。消费者对系统的信心可能会因为了解算法如何精确运作而下降。
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.

（题目未完，接下一页）

A) 正确。《人工智能法案》的支柱和公众信心的主要决定因素是透明度 。(文献：A，第3.6章)
Correct. A pillar of the AI Act and a major determinant of public confidence is transparency. (Literature: A, Chapter 3.6)

B) 不正确。尽管揭示限制是透明度的一部分，但其目的并非降低信任。其目的是通过保证责任和切合实际的期望来建立信任。
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) 不正确。虽然便利性对大多数消费者来说很好，但《人工智能法案》在法律上强制要求透明度。消费者越来越意识到并担心人工智能的伦理方法。因此，透明度可以提升对系统的信心。
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) 不正确。透明度不限于公开源代码。它包括清晰地概述人工智能的操作政策、数据使用和决策制定。建立信任和保证责任取决于此。
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
一家高风险人工智能系统在招聘过程中使用，根据候选人的资格自动筛选。然而，部署者尚未实施任何机制，以在可疑决策情况下进行人工干预或监督。

根据《人工智能法案》，该系统是否需要人工监督?

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) 是，因为人工监督在决策过程中是必要的干预。
Yes, because human oversight is necessary for intervention in decision-making processes.
B) 是，因为人工监督确保符合公平和透明义务。
Yes, because human oversight ensures compliance with fairness and transparency obligations.
C) 不，因为自动化系统旨在无人为干预下运行。
No, because automated systems are designed to function without human intervention.
D) 不，因为招聘过程不涉及对自然人的关键安全风险。
No, because recruitment processes do not involve critical safety risks to natural persons.

A) 正确。《人工智能法案》强调高风险人工智能系统人工监督的重要性，以确保存在人工干预机制，特别是在决策可能存在疑问或对个人产生重大影响的场景中 。(文献：A，第10.2.3章)
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) 不正确。尽管公平性和透明度是《人工智能法案》的重要方面，但仅在存在有限风险或高风险时才需要人工监督。
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) 不正确。《人工智能法案》强调高风险人工智能系统人工监督的重要性，以确保存在人工干预机制，特别是在决策可能存在疑问或对个人产生重大影响的场景中。
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) 不正确。尽管招聘可能不涉及安全风险，但《人工智能法案》考虑的是人工智能系统的伦理和社会影响。为了解决与公平性和透明度相关的担忧，需要人工监督，这在招聘过程中至关重要。
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
一家公司正准备推出一个通用人工智能（GPAI）模型。该模型可适用于客户服务自动化、内容创建和数据分析等任务。该公司总部设在欧盟（EU）以外，但计划在多个欧盟成员国分销该模型。

根据《人工智能法案》，在欧盟分销该GPAI模型之前，哪项**不是**强制要求的?

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) 在欧盟任命一名授权代表，以处理合规事宜
Appoint an authorized representative in the EU to handle compliance matters
B) 遵守欧盟版权法规，以受版权保护的数据进行模型训练
Comply with EU copyright regulations for model training with copyrighted data
C) 进行彻底审计，以验证完全符合所有欧盟法律法规
Conduct a thorough audit to verify full conformity with all EU laws and regulations
D) 发布用于训练GPAI模型的详细内容摘要
Publish a detailed summary of the content used for training the GPAI model

A) 不正确。任何设在欧盟以外的供应商都必须在欧盟任命一名授权代表，以处理合规事宜 。(《人工智能法案》，第54条)
Incorrect. Any provider based outside the EU must appoint an authorized representative in the EU to handle compliance matters. (AI Act, Article 54)
B) 不正确。即使GPAI模型不需要全面的合格性评估，它们仍然必须遵守欧盟版权法，确保用于训练的受保护内容符合法律要求 。(《人工智能法案》，第53条第1款(c)项)
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) 正确。只有高风险人工智能系统才需要全面的合格性评估，而GPAI模型不属于高风险类别。因此，该公司不需要进行全面的合格性评估 。(文献：A，第3章)
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) 不正确。根据《人工智能法案》，必须公布用于训练模型的详细数据摘要 。这确保了透明度。(《人工智能法案》，第53条)
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
一个组织部署了一个人工智能系统，用于工业设备的预测性维护。经过几个月的运行，该系统产生了大量的误报，扰乱了工作流程。一项调查显示以下情况：

- 该组织没有考虑工作现场动态环境变化的影响。
- 该组织缺乏部署后重新评估风险的正式流程。

该组织必须遵守《人工智能法案》。为帮助解决这些问题，该组织使用了ISO/IEC 23894标准。

根据该标准，该组织应采取什么措施来解决这些问题？

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) 开展以人为本的设计研讨会，以提高系统可用性
Conduct a human-centered design workshop to improve system usability
B) 设计一个包含持续评估和监控的风险管理流程
Design a risk management process with ongoing evaluation and monitoring
C) 进行网络安全审计，以识别和解决可能的漏洞
Perform a cybersecurity audit to identify and address possible vulnerabilities
D) 用更简单的、基于规则的模型替换人工智能系统，以便于控制
Replace the AI system with a simpler, rule-based model for easier control

A) 不正确。虽然以人为本的设计可以改善可用性，但它未能解决根本原因：已部署人工智能系统缺乏动态和自适应的风险管理。
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) 正确。ISO/IEC 23894 标准强调在人工智能整个生命周期中嵌入动态、持续的风险管理的重要性，包括部署后阶段 。重新评估本可以在生成大量误报之前调整系统 。(文献：B，第3.2、3.4章)
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) 不正确。网络安全不太可能导致误报。该解决方案未能解决生命周期风险管理或人工智能系统需要持续重新评估的需求。
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) 不正确。替换系统忽略了ISO/IEC 23894标准关于迭代处理和重新评估风险的强调，而不是放弃该技术。
Incorrect. Replacing the system ignores ISO/IEC 23894's emphasis on treating and reassessing risks iteratively, rather than abandoning the technology.

36 / 40
一家汽车车队管理公司使用人工智能系统来追踪驾驶员行为并预测维护需求 。该系统收集并处理大量数据，例如GPS位置、驾驶模式和车辆性能指标 。最近的审计发现，该公司尚未实施充分的数据保护程序 。

根据《人工智能法案》，数据管理和隐私保护对这家企业至关重要 。

为什么这至关重要？

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) 因为它使企业能够优先考虑业务目标和运营效率
Because it enables the business to prioritize business objectives and operational efficiency
B) 因为它增强了用户信任，保障了个人数据，并防止未经授权的访问
Because it enhances user trust, safeguards personal data, and prevents unauthorized access
C) 因为它是强制性的，遵守《人工智能法案》可以避免法律麻烦和潜在罚款
Because it is mandatory and complying with the AI Act avoids legal trouble and potential fines
D) 因为它通过消除用户同意的需要来简化数据收集程序
Because it streamlines data gathering procedures by removing the need for user consent

A) 不正确。实施数据管理和隐私保护并非旨在帮助企业将效率置于合规之上。
Incorrect. Implementing data management and privacy protection is not meant to help the business to prioritize efficiency over compliance.
B) 正确。《人工智能法案》强调保护个人隐私和确保伦理数据管理，这支持了准确和公平的人工智能系统操作。(文献：A，第4.3、4.4、4.6章)
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) 不正确。虽然合规很重要，但《人工智能法案》主要侧重于保护个人权利和维护伦理标准。
Incorrect. While compliance is important, the primary focus of the AI Act is on protecting individual rights and maintaining ethical standards.
D) 不正确。《人工智能法案》和其他相关数据保护法规要求用户同意和数据保护。规避这些要求是非法和不道德的。
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
根据《人工智能法案》，人工智能系统的哪种用途符合有限风险分类?

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

A) 旨在协助客户处理一般查询的聊天机器人，其编程表明它是人工智能。
A chatbot designed to assist customers with general inquiries, which is programmed to disclose it is an AI.

B) 用于在公共场所（例如商场）对客户进行实时识别的人脸识别系统。
A facial recognition system used for real-time identification of customers in public spaces, such as a mall.

C) 一种医疗诊断工具，通过提供基于患者数据的治疗建议来协助医生。
A medical diagnostic tool that assists doctors by giving treatment recommendations based on patient data.

D) 运行自动驾驶车辆的人工智能系统，该车辆在公共道路上无人监督地行驶。
An AI system that operates an autonomous vehicle, which drives on public roads without human supervision.

A) 正确。《人工智能法案》将与用户互动但对权利、安全或法律义务没有重大影响潜力的人工智能系统归类为有限风险 。它们必须遵守透明度义务，例如告知用户正在与人工智能系统互动 。(文献：A，第3.3章)
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) 不正确。根据识别后所做出的决策，该系统将属于高风险，甚至可能被禁止，因为其对隐私和监控有影响。
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) 不正确。该工具属于高风险应用，因为该人工智能系统处理健康和安全数据。
Incorrect. This tool falls under high-risk application because the AI system deals with health and safety data.

D) 不正确。自动驾驶车辆由于安全问题和可能发生事故的影响，被认为是高风险。
Incorrect. Autonomous vehicles are considered high risk due to safety concerns and the impact of possible accidents.

38 / 40
一家企业正在开发一个用于教育的人工智能系统。该人工智能系统将决定学生是否能获得学习材料、是否被学校录取或被分配到某个班级。该人工智能系统将通过云服务提供 。

根据《人工智能法案》，该人工智能系统的使用应归类于哪个类别?

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) 不可接受的风险
Unacceptable risk
B) 高风险的
High-risk
C) 有限风险的
Limited-risk
D) 低风险或零风险的
Minimal or no-risk

A) 不正确。对自然人可能产生重大影响的人工智能系统，例如影响受教育机会的系统，根据《人工智能法案》被归类为高风险，而不是禁止，因为它们受到严格要求而非彻底禁止的监管。
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 prohibited, as they are regulated with strict requirements rather than outright banned.
B) 正确。旨在评估受教育机会的人工智能系统应归类为高风险，因为它们可以直接影响学生是否能获得教育资源或被录取，这会影响他们的基本权利。 (文献：A，第3.3、3.4章；《人工智能法案》，第6条（附件三）)
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) 不正确。有限风险人工智能包括人工智能驱动的聊天机器人、推荐系统或不做出影响个人权利或机会的关键决策且有可能将个人排除在受教育机会之外的人工智能助手。这会带来高风险。
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) 不正确。低风险分类不能准确反映此类人工智能系统相关的潜在风险，因为它将个人排除在受教育机会之外的能力可能对他们造成重大后果。
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
一家组织开发了一个用于自动化招聘的人工智能系统 。在测试过程中，团队发现以下问题：

- 由于训练数据中存在人口统计学偏见，系统对来自某些族裔背景的候选人评分始终较低 。
- 目前，没有内部审查流程或来自相关方的反馈机制可以指出这种特定偏见的风险 。

该组织必须遵守《人工智能法案》 。为帮助解决这些问题，该组织使用了ISO/IEC TR 24368标准 。

根据该标准，该组织应采取什么措施来解决这些问题 ？

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) 创建一个合成数据集，以解决人口统计学失衡并提高公平性
Create a synthetic dataset to address demographic imbalances and improve fairness
B) 实施透明度，以提高系统的可解释性和问责制
Implement transparency to increase the system's explainability and accountability
C) 加强数据加密实践并使用访问控制来防止泄露
Strengthen data encryption practices and use access control to prevent breaches
D) 使用一个包含利益相关者输入的伦理框架来评估人权问题
Use an ethical framework with stakeholder input to evaluate human rights issues

A) 不正确。单独使用合成数据并不能确保偏见缓解，也未能解决围绕伦理人工智能开发的核心要求 。此外，它不属于所提及的 ISO/IEC TR 24368 标准的一部分 。
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) 不正确。透明度并不能直接解决所需的公平性、伦理审查流程或利益相关者包容性 。解决这些问题的相关方案是实施伦理审查流程 。
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) 不正确。虽然数据加密和访问控制对于确保信息安全至关重要，但它们与手头的问题无关 。更相关的重点将是实施伦理审查流程 。
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) 正确。ISO/IEC TR 24368 强调伦理框架、人权实践、利益相关者参与以及人工智能开发中公平性的重要性 。建立伦理审查流程有助于识别和缓解歧视，这与标准的核心原则相符 。 (文献：B，第 4.2、4.3 章)
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
一家人工智能初创公司开发了一个通用人工智能（GPAI）模型，该模型使用公开可用的在线内容进行训练，包括新闻文章、研究论文和社交媒体帖子。发布后，该公司收到一组作者的法律通知，声称他们的知识产权（IP）未经授权被用于模型训练。

在这种情况下，应该采取什么措施来保护知识产权?

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) 主张GPAI模型符合开源条件，并可免除版权合规义务
Argue that the GPAI model qualifies as open-source, and is exempt from copyright compliance obligations
B) 根据《人工智能法案》主张合理使用，因为内容是公开可用的，并继续使用该数据集
Claim fair use under the AI Act, since the content was publicly available, and continue using the dataset
C) 删除包含与争议作品相似之处的人工智能生成输出，以避免侵权索赔
Delete the AI-generated outputs containing similarities to the disputed works to avoid infringement claims
D) 记录并分享GPAI训练数据集的详细信息，包括出处，以确保合规性
Document and share details of the GPAI training dataset, including provenance, to ensure compliance

A) 不正确。开源人工智能模型如果带来系统性风险或实现商业化，则不会自动免除版权合规义务。
Incorrect. Open-source AI models are not automatically exempt from copyright compliance if they pose systematic risks or are monetized.
B) 不正确。《人工智能法案》不提供合理使用豁免。公开可用的内容仍可能受版权保护。
Incorrect. The AI Act does not provide a fair use exemption. Publicly available content may still be protected by copyright.
C) 不正确。《人工智能法案》不强制要求仅根据与受版权保护作品的相似性来删除人工智能生成的输出。
Incorrect. The AI Act does not mandate the deletion of AI-generated outputs based solely on similarity to copyrighted works.
D) 正确。根据《人工智能法案》第53条，供应商必须记录训练过程，并包含关于数据出处和特征的详细信息。(文献：A，第3章)
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)

试题评分

如下表格为本套样题的正确答案，供参考使用。

问题	答案	问题	答案
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

联系 EXIN

www.exinchina.cn

info.china@exin.com

WeChat ID: EXINCH