Professional Certificate in Artificial Intelligence Vendor Due Diligence Framework

Identifying AI Vendor Risks and Mitigation Strategies

Algorithm
: A set of rules or instructions given to an artificial intelligence (AI) system to help it complete a task. Related terms include: machine learning, deep learning, neural network.

Example: An algorithm for an AI system might include instructions for recognizing images of cats by analyzing features such as ears, whiskers, and tail shape.

Practical application: Algorithms are essential for AI systems to function and complete tasks, and the choice of algorithm can greatly impact the performance and accuracy of the system.

Challenge: Developing and optimizing algorithms can be complex and time-consuming, requiring a deep understanding of both the AI system and the task at hand.

Artificial Intelligence (AI)
: The simulation of human intelligence in machines that are programmed to think and learn. Related terms include: machine learning, deep learning, neural network.

Example: An AI system might be used to analyze medical images and diagnose diseases.

Practical application: AI systems can be used to automate tasks, improve efficiency, and make decisions based on large amounts of data.

Challenge: AI systems can be complex and difficult to understand, and can pose risks such as bias and lack of transparency.

Bias
: A tendency for an AI system to favor certain outcomes or decisions over others, often due to factors such as the data used to train the system or the algorithms used to make decisions. Related terms include: fairness, transparency, explainability.

Example: An AI system used for hiring might be biased against certain groups of people, such as those with certain names or from certain backgrounds.

Practical application: Bias in AI systems can lead to unfair outcomes and can damage trust in the system. It is important to identify and address bias in AI systems to ensure fairness and transparency.

Challenge: Identifying and addressing bias in AI systems can be complex and may require access to the underlying data and algorithms used to make decisions.

Cloud Computing
: The use of remote servers on the internet to store, manage, and process data, rather than using local servers or personal computers. Related terms include: artificial intelligence, machine learning, deep learning.

Example: A company might use cloud computing to store and analyze large amounts of data for an AI system.

Practical application: Cloud computing can provide flexibility, scalability, and cost savings for AI systems.

Challenge: Cloud computing can pose risks such as data breaches and loss of control over data.

Compliance
: The act of following laws, regulations, and standards related to the use of AI systems. Related terms include: data privacy, data security, ethics.

Example: A company might need to comply with regulations related to the use of AI systems in healthcare, such as the Health Insurance Portability and Accountability Act (HIPAA).

Practical application: Compliance is essential for AI systems to be used legally and ethically. It is important to understand and follow relevant laws, regulations, and standards.

Challenge: Compliance can be complex and may require specialized knowledge and resources.

Data Privacy
: The protection of personal data from unauthorized access, use, or disclosure. Related terms include: data security, compliance, ethics.

Example: A company might use data privacy measures such as encryption and access controls to protect personal data.

Practical application: Data privacy is essential for protecting the rights and interests of individuals and organizations. It is important to implement appropriate data privacy measures to protect personal data.

Challenge: Data privacy can be complex and may require specialized knowledge and resources.

Data Security
: The protection of data from unauthorized access, use, or disclosure. Related terms include: data privacy, compliance, ethics.

Example: A company might use data security measures such as firewalls and access controls to protect data.

Practical application: Data security is essential for protecting the integrity and confidentiality of data. It is important to implement appropriate data security measures to protect data.

Challenge: Data security can be complex and may require specialized knowledge and resources.

Deep Learning

: A type of machine learning that uses artificial neural networks with multiple layers to analyze and learn from data. Related terms include: artificial intelligence, machine learning, neural network.

Example: A deep learning system might be used to analyze images and recognize objects.

Practical application: Deep learning can be used to automate tasks, improve efficiency, and make decisions based on large amounts of data.

Challenge: Deep learning can be complex and resource-intensive, requiring large amounts of data and computational power.

Ethics
: The principles and values that guide the development, use, and governance of AI systems. Related terms include: bias, fairness, transparency.

Example: An ethical AI system might prioritize fairness and transparency in its decisions.

Practical application: Ethics are essential for ensuring that AI systems are developed and used in a responsible and trustworthy manner.

Challenge: Ethics can be complex and may require subjective judgments and trade-offs.

Explainability
: The ability of an AI system to provide clear, understandable explanations for its decisions and actions. Related terms include: bias, fairness, transparency.

Example: An explainable AI system might provide a detailed explanation of how it arrived at a particular decision, including the data and algorithms used.

Practical application: Explainability is essential for building trust in AI systems and for understanding and addressing bias and other issues.

Challenge: Explainability can be complex and may require specialized knowledge and resources.

Fairness
: The principle of ensuring that AI systems do not favor certain groups or individuals over others. Related terms include: bias, explainability, transparency.

Example: A fair AI system might use a diverse and representative dataset to train its algorithms.

Practical application: Fairness is essential for ensuring that AI systems are equitable and do not discriminate.

Challenge: Fairness can be complex and may require subjective judgments and trade-offs.

Machine Learning
: A type of artificial intelligence that uses algorithms and statistical models to learn and improve from data. Related terms include: artificial intelligence, deep learning, neural network.

Example: A machine learning system might be used to predict customer churn for a telecommunications company.

Practical application: Machine learning can be used to automate tasks, improve efficiency, and make decisions based on large amounts of data.

Challenge: Machine learning can be complex and may require large amounts of data and computational power.

Neural Network
: A type of artificial intelligence that is inspired by the structure and function of the human brain. Related terms include: artificial intelligence, machine learning, deep learning.

Example: A neural network might be used to analyze images and recognize objects.

Practical application: Neural networks can be used to automate tasks, improve efficiency, and make decisions based on large amounts of data.

Challenge: Neural networks can be complex and resource-intensive, requiring large amounts of data and computational power.

Risk
: The potential for harm or loss resulting from the use of an AI system. Related terms include: compliance, data privacy, data security.

Example: A risk associated with an AI system might be the potential for data breaches or loss of control over data.

Practical application: Risk management is essential for ensuring that AI systems are used in a safe and responsible manner.

Challenge: Risk can be complex and may require specialized knowledge and resources.

Transparency
: The principle of making the workings and decisions of an AI system clear and understandable to users and stakeholders. Related terms include: bias, fairness, explainability.

Example: A transparent AI system might provide users with information about how it makes decisions and how it uses data.

Practical application: Transparency is essential for building trust in AI systems and for understanding and addressing bias and other issues.

Challenge: Transparency can be complex and may require specialized knowledge and resources.

Vendor
: A company or individual that provides products or services to another company or individual. Related

terms include: due diligence, risk, compliance.

Example: A vendor might provide an AI system to a company for use in its operations.

Practical application: Vendor management is essential for ensuring that AI systems are used in a safe and responsible manner.

Challenge: Vendor management can be complex and may require specialized knowledge and resources.

Vendor Due Diligence
: The process of evaluating and assessing a vendor to ensure that it meets certain standards and requirements. Related terms include: risk, compliance, data privacy, data security.

Example: A company might conduct vendor due diligence on a vendor that provides an AI system to ensure that it meets data privacy and security requirements.

Practical application: Vendor due dilig