Professional Certificate in Artificial Intelligence Vendor Due Diligence Framework

# Analyzing AI Vendor Business Continuity and Disaster Recovery Plans

Analyzing AI Vendor: The process of evaluating and understanding the capabilities, strengths, and weaknesses of an artificial intelligence (AI) vendor before making a decision to purchase their products or services. This includes assessing the vendor's technical expertise, business model, financial stability, and ability to meet the specific needs and requirements of the organization.

Artificial Intelligence (AI): A branch of computer science that deals with the creation of intelligent machines that can think and learn like humans. AI systems can perform tasks that typically require human intelligence, such as visual perception, speech recognition, decision-making, and language translation.

Business Continuity Plan (BCP): A set of procedures and processes that an organization puts in place to ensure that its critical business functions can continue to operate in the event of a disruption or disaster. A BCP typically includes contingency plans for various scenarios, such as power outages, cyber attacks, and natural disasters, and outlines the steps that the organization will take to maintain operations and minimize the impact on its customers, employees, and stakeholders.

Disaster Recovery Plan (DRP): A subset of the organization's BCP that focuses on restoring critical IT systems and infrastructure in the event of a disaster. A DRP typically includes backup and recovery procedures, as well as plans for data protection, system redundancy, and failover. The goal of a DRP is to ensure that the organization can quickly and efficiently recover from a disaster, and minimize downtime and data loss.

Due Diligence: The process of investigating and evaluating a potential investment or business partner to ensure that they are financially stable, legally compliant, and a good fit for the organization. Due diligence typically includes reviewing financial statements, legal documents, and business plans, as well as conducting interviews with key personnel and performing background checks.

Risk Assessment: The process of identifying, analyzing, and prioritizing potential risks to an organization's operations, assets, or reputation. A risk assessment typically includes identifying the sources of risk, evaluating the likelihood and impact of each risk, and developing strategies to mitigate or manage the risks.

Vendor Management: The process of selecting, evaluating, and overseeing the performance of external vendors or service providers. Vendor management includes setting clear expectations, establishing service level agreements, and monitoring vendor performance to ensure that they meet the organization's needs and requirements.

Vendor Selection: The process of evaluating and choosing a vendor to provide products or services to the

organization. Vendor selection typically includes reviewing vendor proposals, assessing their capabilities and strengths, and negotiating contracts and service level agreements.

Vendor Due Diligence: The process of investigating and evaluating a potential vendor to ensure that they are financially stable, legally compliant, and a good fit for the organization. Vendor due diligence typically includes reviewing financial statements, legal documents, and business plans, as well as conducting interviews with key personnel and performing background checks.

Vendor Lock-in: The situation in which an organization becomes dependent on a particular vendor or product, and finds it difficult or expensive to switch to a different vendor or product. Vendor lock-in can occur for a variety of reasons, such as high switching costs, proprietary technology, or lack of interoperability with other systems.

Vendor Performance Monitoring: The process of tracking and evaluating the performance of external vendors or service providers. Vendor performance monitoring includes setting clear expectations, establishing service level agreements, and monitoring vendor performance to ensure that they meet the organization's needs and requirements.

Vendor Risk Management: The process of identifying, analyzing, and mitigating potential risks associated with using external vendors or service providers. Vendor risk management includes assessing the vendor's financial stability, legal compliance, and security practices, as well as developing strategies to manage and mitigate potential risks.

Artificial Intelligence (AI) Vendor: A company that provides products or services based on artificial intelligence (AI) technology. AI vendors can include companies that specialize in machine learning, natural language processing, computer vision, or other AI-related technologies.

AI Vendor Due Diligence: The process of investigating and evaluating a potential AI vendor to ensure that they are financially stable, legally compliant, and a good fit for the organization. AI vendor due diligence typically includes reviewing financial statements, legal documents, and business plans, as well as conducting interviews with key personnel and performing background checks.

AI Vendor Selection: The process of evaluating and choosing an AI vendor to provide products or services to the organization. AI vendor selection typically includes reviewing vendor proposals, assessing their capabilities and strengths, and negotiating contracts and service level agreements.

AI Vendor Management: The process of selecting, evaluating, and overseeing the performance of AI vendor or service provider. AI vendor management includes setting clear expectations, establishing service level agreements, and monitoring vendor performance to ensure that they meet the organization's needs and requirements.

AI Vendor Performance Monitoring: The process of tracking and evaluating the performance of AI external

vendor or service provider. AI vendor performance monitoring includes setting clear expectations, establishing service level agreements, and monitoring vendor performance to ensure that they meet the organization's needs and requirements.

AI Vendor Risk Management: The process of identifying, analyzing, and mitigating potential risks associated with using external AI vendors or service providers. AI vendor risk management includes assessing the vendor's financial stability, legal compliance, and security practices, as well as developing strategies to manage and mitigate potential risks.

AI Vendor Lock-in: The situation in which an organization becomes dependent on a particular AI vendor or product, and finds it difficult or expensive to switch to a different vendor or product. AI vendor lock-in can occur for a variety of reasons, such as high switching costs, proprietary technology, or lack of interoperability with other systems.

AI Vendor Due Diligence Framework: A structured approach to investigating and evaluating a potential AI vendor, which includes assessing the vendor's financial stability, legal compliance, technical expertise, and ability to meet the specific needs and requirements of the organization. The AI vendor due diligence framework typically includes a set of guidelines, checklists, and templates to help organizations conduct a thorough and consistent evaluation of potential AI vendors.

AI Vendor Business Continuity Plan (BCP): A plan that outlines the steps that an AI vendor will take to ensure that its critical business functions can continue to operate in the event of a disruption or disaster. An AI vendor BCP typically includes contingency plans for various scenarios, such as power outages, cyber attacks, and natural disasters, and outlines the steps that the vendor will take to maintain operations and minimize the impact on its customers, employees, and stakeholders.

AI Vendor Disaster Recovery Plan (DRP): A subset of the AI vendor's BCP that focuses on restoring critical IT systems and infrastructure in the event of a disaster. An AI vendor DRP typically includes backup and recovery procedures, as well as plans for data protection, system redundancy, and failover. The goal of an AI vendor DRP is to ensure that the vendor can quickly and efficiently recover from a disaster, and minimize downtime and data loss.

AI Vendor Resilience: The ability of an AI vendor to withstand and recover from disruptions, disasters, or other unexpected events. AI vendor resilience is typically achieved through a combination of technical, operational, and organizational measures, such as redundant systems, backup and recovery procedures, and crisis management plans.

AI Vendor Redundancy: The use of multiple systems, components, or resources to provide backup and failover capabilities in the event of a failure or disruption. AI vendor redundancy is typically used to increase the reliability and availability of critical IT systems and infrastructure, and can help to minimize downtime and data loss in the event of a disaster.

AI Vendor Failover: The process of automatically switching to a backup or standby system in the event of a failure or disruption. AI vendor failover is typically used to minimize downtime and data loss in the event of a disaster, and can help to ensure that critical business functions can continue to operate.

AI Vendor Data Protection: The measures taken to protect and secure an AI vendor's data, including backup and recovery procedures, encryption, access controls, and other security measures. AI vendor data protection is typically used to minimize the risk of data loss, theft, or unauthorized access, and can help to ensure the confidentiality, integrity, and availability of critical data.

AI Vendor Security Practices: The policies, procedures, and technologies used