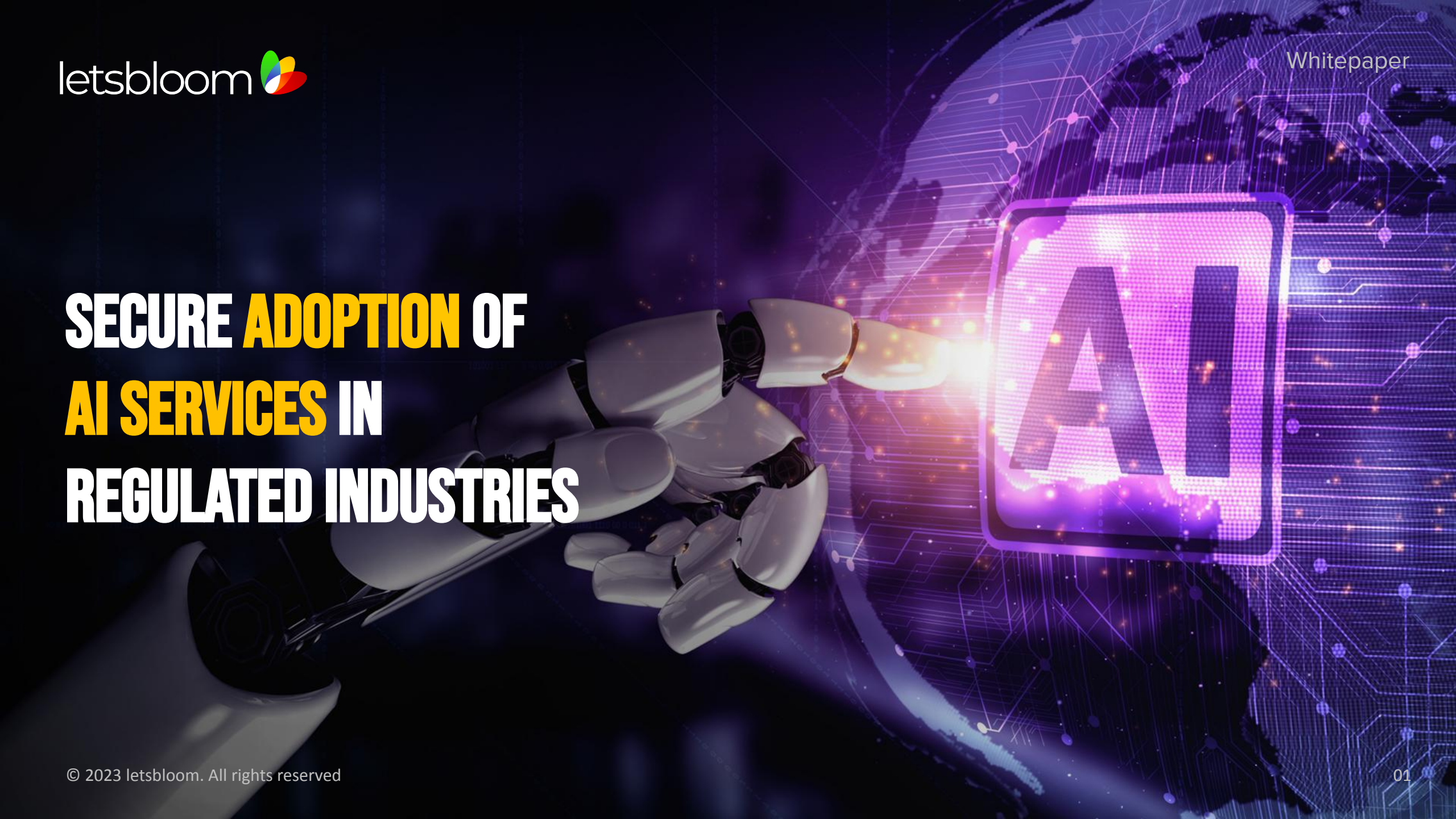
SECURE ADOPTION OF AI SERVICES IN REGULATED INDUSTRIES



Abstract

This paper provides a framework for the secure adoption of AI services for businesses in regulated industries to enable effective technology, cybersecurity and compliance risk management. The key principles that businesses should follow while adopting cloud AI services are:

1. **Data Privacy and Security:** Mitigate the risks of unauthorized access, theft, or misuse of sensitive customer data.

2. **Regulatory Compliance:** Ensure compliance with regulatory and data privacy requirements, such as NYDFS, PRA/FCA, GDPR, CCPA, and HIPAA.

3. **Vendor Management:** Mitigate the risks associated with third-party vendors' access to sensitive data and the associated attack vectors.

4 **Model Bias and Fairness:** Effectively address the risks of model bias and unfairness to provide transparency and explainability of decision-making.

5 **Operational Risks:** Mitigate the risks of system failures, errors, or cyber-attacks by building resilient architecture.

Overall, any business trying to adopt cloud AI services should implement a comprehensive risk management program that includes policies, procedures, and controls for each area of risk. The program should be regularly reviewed and updated to ensure that it remains effective and aligned with the business objectives and compliance requirements.

Index

Introduction

AI technologies, especially generative AI, have increasingly become business-critical as they provide invaluable support in decision making, insight generation, process automation, personalization of customer experiences, and cost savings for the business. Hence the adoption of such AI services and the use of said services with sensitive customer data is invariable.

Public cloud has become the inevitable choice for AI service adoption as businesses cannot keep pace with the scale of innovation at hyperscalers and SaaS providers. So, how do enterprises adopt cloud-based high-value managed AI services without introducing unacceptable levels of cybersecurity and compliance risk?

The traditional cybersecurity risks that enterprises face such as Malware / Ransomware, Insider Threats, Software Vulnerabilities, and Data Loss or Exfiltration are all applicable to the adoption and use of cloud AI services. So also, are compliance obligations for data protection, privacy, sovereignty, and effective technology risk management. However, the use of AI introduces new risks including amplification of bias, opaque decision-making, and fairness of outcomes.

The adoption of AI services, especially in regulated industries, needs a robust methodology for risk management and a standardized, extensible framework for service onboarding and management. This paper aims to provide a reusable methodology, framework and adoption architecture aimed at accelerating the adoption of AI services in regulated industries.

Challenges

The adoption of any new technology presents its own set of challenges. Similarly, cloud-based services with their low barrier to adoption present a unique set of challenges. Business teams in enterprises expect adoption at the speed of the cloud while cybersecurity, risk, and compliance teams struggle to get the services enterprise-ready leading to friction and potential revenue impacts.

The challenges of cloud-based AI services include:

Data Privacy and Security Risks

AI services may process sensitive customer data, which could be at risk of unauthorized access, theft, or misuse. Given the nature and scope of data-in-use in AI services, the impact of this risk can be manifold.

Compliance Risks

AI services may be subject to enhanced regulatory requirements, necessitating the implementation of additional data protection and privacy controls, conducting enhanced audits, and maintaining accurate records.

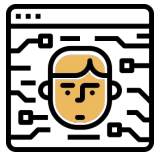
Vendor Management Risks

The use of third-party vendors introduces additional risks, such as data breaches, service disruptions, or non-compliance. In the context of AI services, this may present a unique set of challenges that are not associated with the use of third parties in traditional systems such as traceability, transparency, and accountability impacts.

Challenges

Model Bias and Fairness Risks

AI services may use machine learning models that are biased or unfair, which could result in discriminatory outcomes for certain groups of customers.



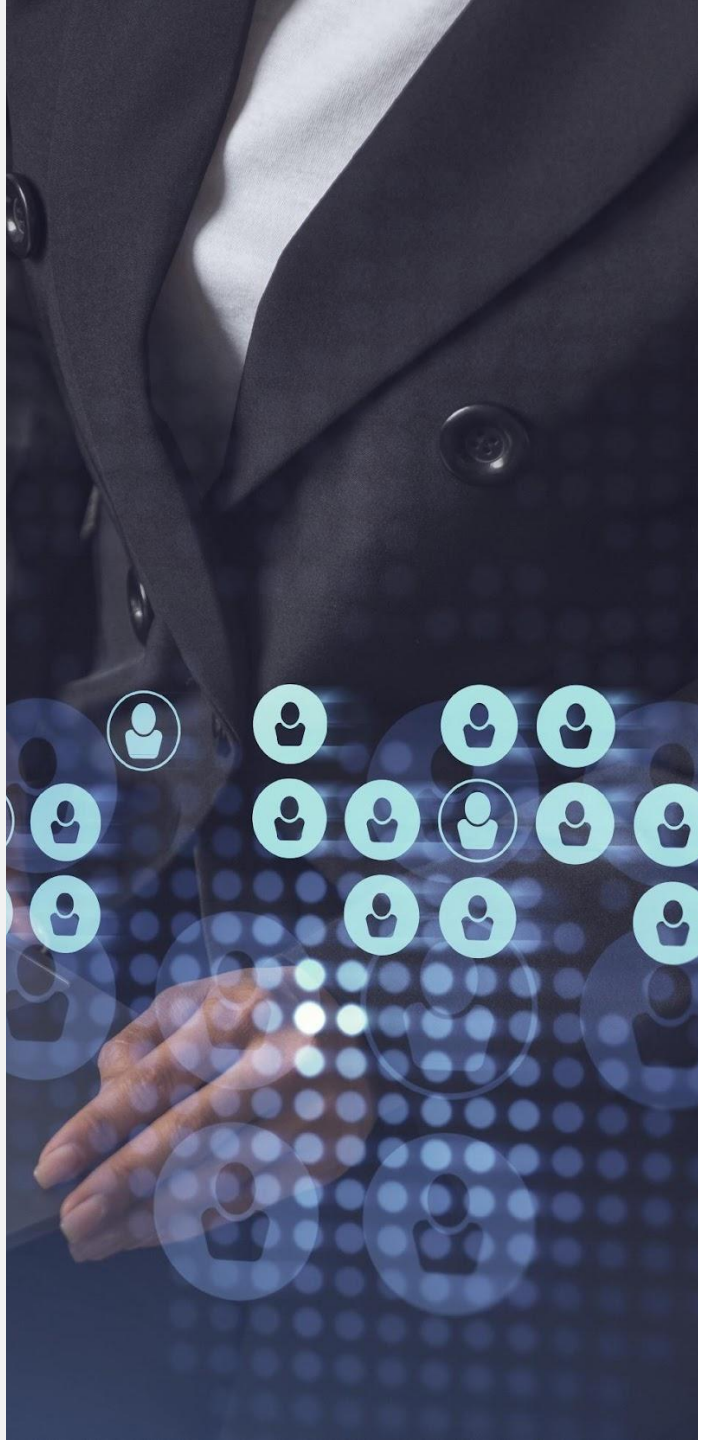
Operational Risks

Like any other technology service, AI services are subject to operational risks, such as system failures, errors, or cyber-attacks but with outsized impacts of any disruption or breach due to the critical part they play in decision-making processes. This requires the implementation of enhanced cybersecurity and compliance controls consummate with the level of risk they present.

Managing FATE

The use of AI for decision-making brings additional risk areas for consideration. When algorithms drive decisions that impact their users' economic outcomes and well-being, considerations of fairness, accountability, transparency, and ethics (FATE) become paramount. Algorithmic biases can cause large disparities in outcomes, hence ensuring adequate safeguards for FATE will not only ensure equitable outcomes but also enhance customer trust.

Technical controls alone won't suffice in managing FATE considerations in AI. This requires adequate process safeguards and training for developers and users of AI solutions. A good place to start would be ensuring diversity and cultural pluralism in teams working on developing AI-based solutions. Organizations should also promote complete transparency in how they develop and use AI in their decision-making systems that allow users to trust the system.



'Data Colonialism' is an increasing area of concern for users. It refers to the commercialization of user data collected through apps and online services often for purposes unrelated to the original intent. Traceability and accountability in the use of data within AI systems and strong data protection and privacy controls that clearly demonstrate compliance with regulations such as GDPR, CCPA, and PDPA can alleviate some of these concerns.

Methodology and Framework

An effective risk management methodology provides a systemic approach for identifying, assessing, mitigating, monitoring, and reporting risks that allow organizations to continuously manage their risk appetite in the face of an emergent threat landscape.

Methodology for Risk Management

1. **Identification:** Identify and document all inherent technology, cyber security, privacy, regulatory, social, and ethical risks in the use of AI technologies in decision-making systems.

2. **Assessment:** Evaluate the identified risks for probability (likelihood of occurrence), impact (magnitude of damage of an occurrence), and detectability (how likely would you be able to detect the risk before it occurs). This helps in prioritizing the risks for mitigation.

3. **Mitigation:** Implement a clear mitigation plan for prioritized risks to reduce the likelihood and impact of the risk and to improve its detectability.

4 **Monitor:** Implement a continuous monitoring capability to detect and assess any changes to the risk profile through the addition of new risks, change in the likelihood or impact of existing risks, or change in the effectiveness of mitigation plans.

5 **Report:** Reporting is not only a critical part of the risk management framework but is often a mandatory step in regulatory compliance. Effective monitoring and reporting are crucial to ensure continued compliance.

Key Principles of the Framework

These principles outline the key risk areas for risk management during the adoption of high-value AI services in regulated industries.

1. Data Privacy and Security

To mitigate the risks of unauthorized access, theft, or misuse of sensitive customer data, implement the following controls:

- **Strong access controls:** Implement multi-factor authentication, role-based access controls, and least privilege access to ensure that only authorized personnel can access sensitive data.
- **Encryption:** Encrypt data both in transit and at rest to protect against data breaches and theft.
- **Data loss prevention:** Implement data loss prevention measures, such as monitoring and blocking of sensitive data transfers, to prevent accidental or intentional data leaks.

2. Compliance

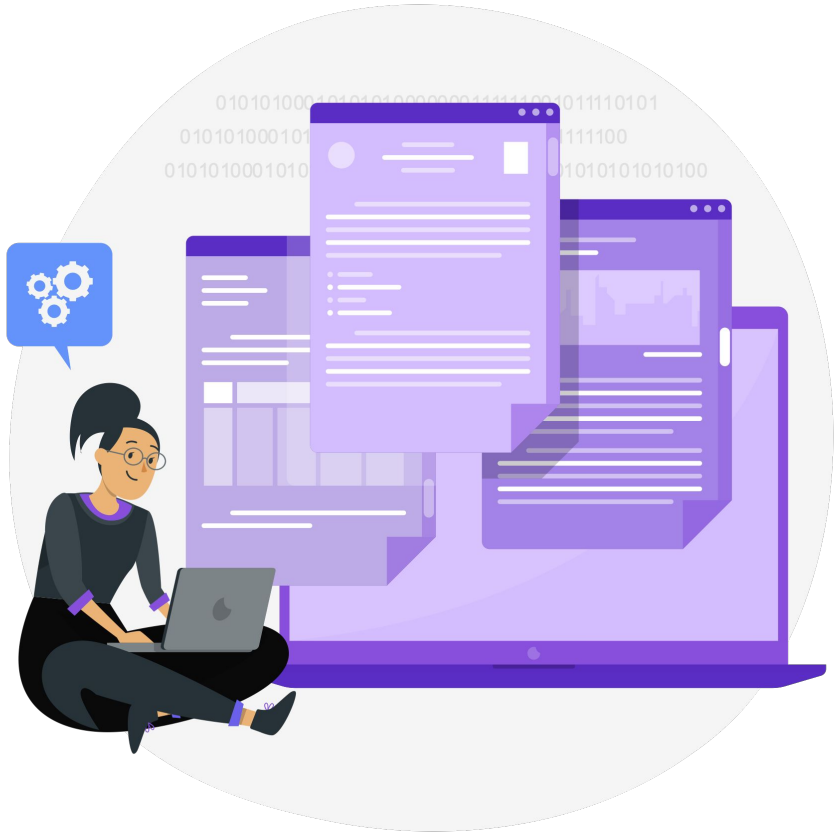
To ensure compliance with regulatory requirements, such as NYDFS, PRA/FCA, GDPR, CCPA, and HIPAA, implement the following controls:

- **Data protection and privacy controls:** Implement appropriate data protection and privacy controls, such as data classification, data retention, and data deletion policies, to ensure compliance with regulatory requirements.
- **Regular audits:** Conduct regular audits of its cloud-based AI services to ensure compliance with regulatory requirements and identify any potential compliance issues.
- **Accurate records:** Maintain accurate records of its cloud-based AI services, including data processing activities, to demonstrate compliance with regulatory requirements.

3. Vendor Management

To mitigate the risks associated with third-party vendors, implement the following controls:

- **Due diligence:** Conduct due diligence on vendors to ensure appropriate security and compliance controls are in place.
- **Contractual terms:** Establish clear contractual terms with vendors, including security and compliance requirements, service level agreements, and termination clauses.
- **Vendor performance monitoring:** Monitor vendor performance to ensure they meet contractual obligations and comply with security and compliance requirements.



4. Model Bias and Fairness

To address the risks of model bias and fairness, implement the following controls:

- **Model validation and testing:** Implement model validation and testing procedures to identify and address any biases or unfairness in machine learning models.
- **Transparency and explainability:** Ensure that machine learning models are transparent and explainable so customers can understand how decisions are made.

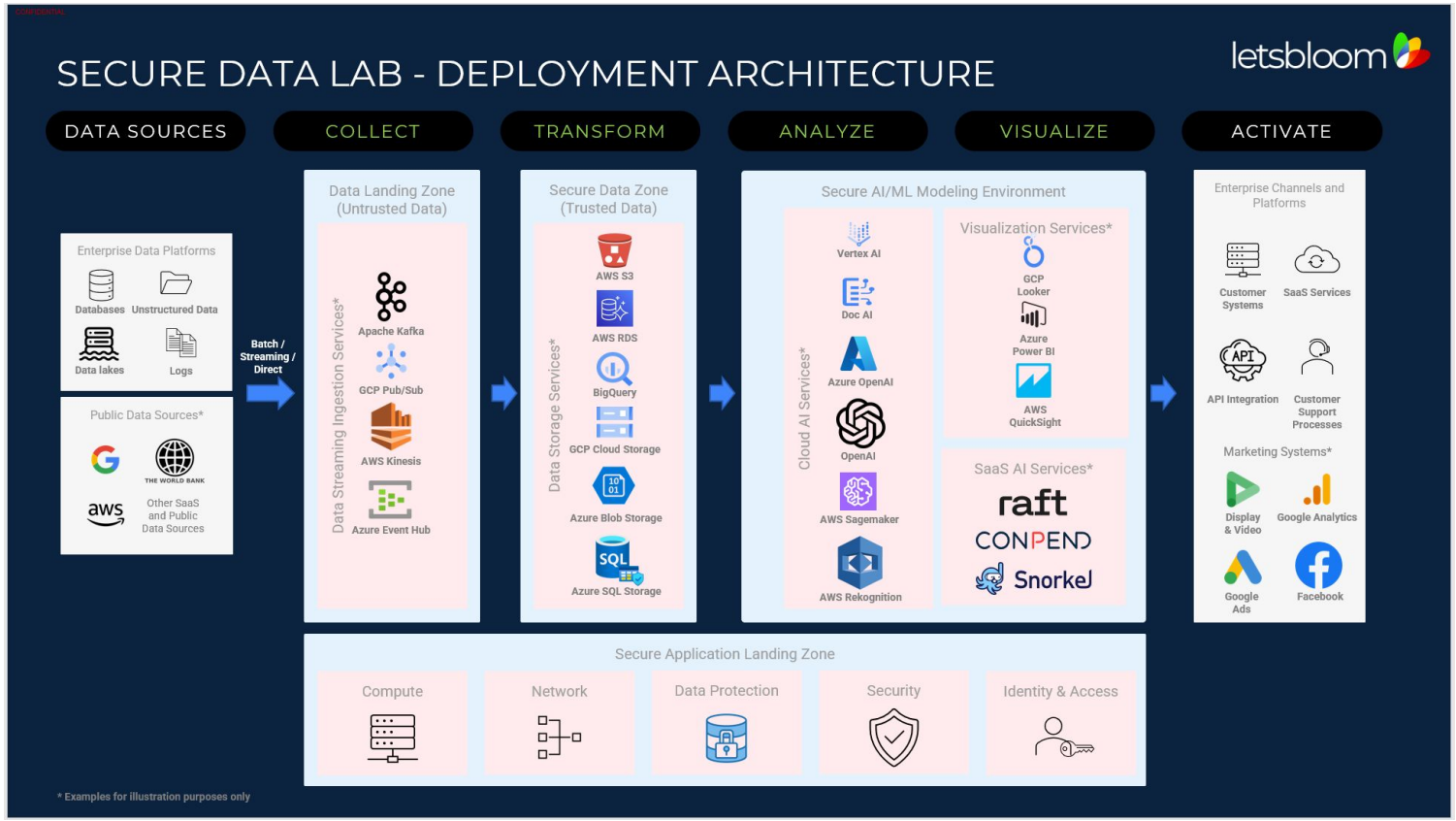
5. Operational Risks

To mitigate the risks of system failures, errors, or cyber-attacks, implement the following controls:

- **Disaster recovery and business continuity plans:** Implement robust disaster recovery and business continuity plans to ensure that cloud-based AI services can be quickly restored in the event of a disruption.
- **Security testing and vulnerability assessments:** Conduct regular security testing and vulnerability assessments to identify and address any security weaknesses in its cloud-based AI services.

Deployment Architecture

Deployment architectures for cloud-based AI service adoption should be outcome-oriented and consider the entire use case. This includes enabling the organization to securely upload/share data within its teams as well as with third parties, ensuring appropriate access levels for each persona (e.g., only data owners can upload/download data and results), ensuring access to high-value AI services for data scientists and ability to enrich data from public data sources. The entire deployment should be based on a secure-by-design and compliant-by-default infrastructure with continuous monitoring for security and compliance posture.



The above diagram illustrates a sample logical deployment reference architecture.

Conclusion

The adoption of AI is inevitable for modern enterprises due to the nature and impact of technological paradigms such as generative AI. However, this adoption doesn't have to come at the cost of increased cybersecurity and compliance risk. Establishing a robust framework for the identification, assessment, mitigation, ongoing monitoring and reporting of risks would lead to a sustainable path for adoption and allow businesses to innovate at scale.

Looking for more information on how your organization can quickly adopt cloud-based managed AI services and use them with your sensitive data? Reach out to us at: support@letsbloom.io

Key Takeaways

- Conduct a thorough risk assessment using a well-established methodology.
- Focus not only on traditional cybersecurity and compliance risks but also consider new risks introduced by AI.
- Implement, enforce, and monitor fit-for-purpose controls in your cloud environments.
- Consider any additional attack vectors introduced by using cloud and third-party solutions.
- Adopt templatization and reusability principles to standardize the use of AI in your enterprise.

letsbloom