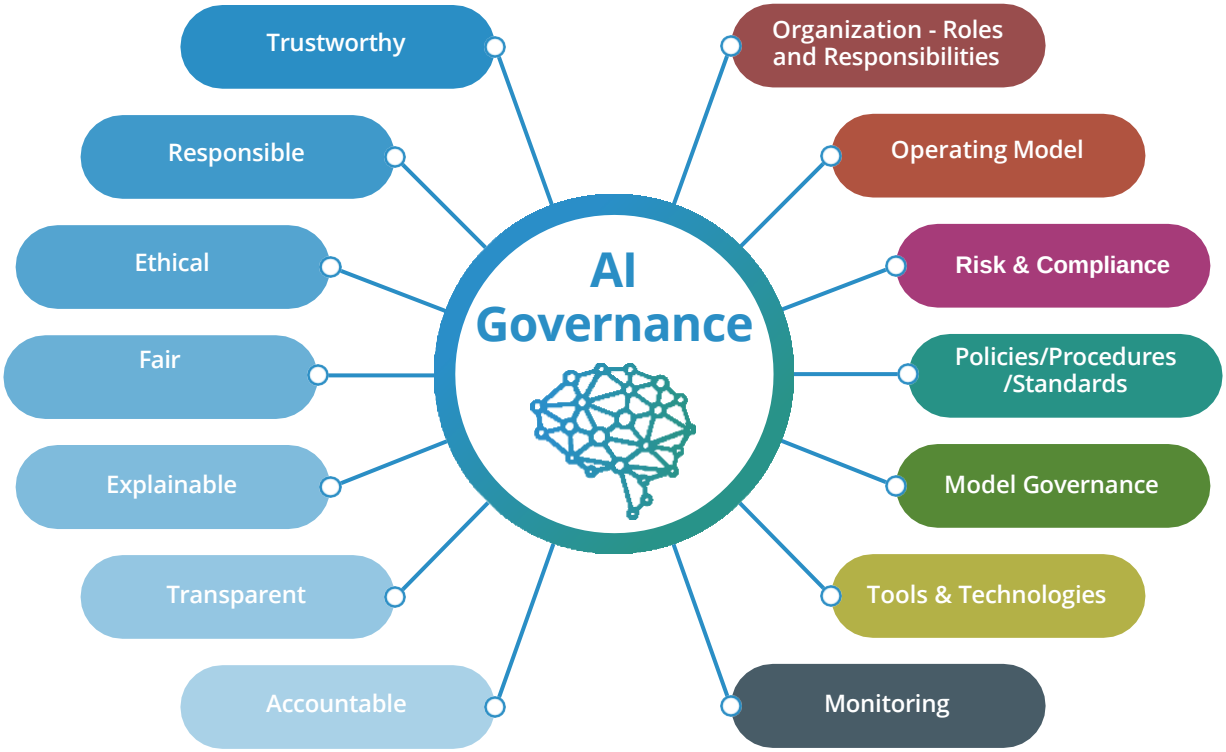
CRUSHBANK

The CrushBank AI Knowledge Management system is built with

Trustworthy AI from IBM watsonx™

AI Governance
Why it matters and what you can do about it

Managed Services Providers (MSPs) use a variety of software applications in their technology stack. Many of these are embedding generative AI into their systems, underpinned by Large Language Models (LLMs). In addition, their employees are making use of tools such as OpenAI and ChatGPT in their day-to-day jobs. Generative AI can do amazing things such as creating content, images, ideas, recommendations and more. It has many very beneficial uses in business. But the technology has spread so quickly, often without MSPs being clear on what they are actually using, that they may be exposed in several ways. The MSP must focus on the following areas to ensure safe and accurate use of LLMs for themselves and their clients.



What is AI Governance?

AI governance refers to the policies and practices put in place to ensure responsible and ethical development and use of AI and the underlying LLMs. Its goal is to allow the use of AI, while mitigating risks, protecting individual rights, and creating accountability. AI governance is crucial as AI systems become increasingly integrated into all aspects of business and personal life. Some of the key components are:

- Ethical Principles
- Regulations and Compliance
- Data Governance
- Accountability
- Transparency of decision-making process
- Bias Mitigation
- User Safety Considerations
- Human Oversight
- Education and Awareness
- Continuous Monitoring and Evaluation

Key Elements of AI Governance

1.Data Sources and Model Accuracy:
MSPs need a good understanding of the data sources that are used to create the AI LLMs they use. This includes knowing the quality, relevance, and bias of the data. Regularly monitoring these sources is essential to ensure that the model remains accurate and up-to-date. **INCLUDED WITH CRUSHBANK**

2. Data Security and Responsible Usage:
MSPs must prioritize the security and responsible handling of client data as it relates to generative and other AI uses. Adhering to data privacy regulations and obtaining client consent for data usage is paramount. MSPs should have clear policies and procedures in place for data handling and disposal to minimize the risk of data breaches or misuse. **INCLUDED WITH CRUSHBANK**

3. Copyright and Intellectual Property Considerations:
MSPs should be acutely aware of the risks associated with copyright and intellectual property infringement when using AI LLMs for tasks such as summarization, transfer or translation. Information protected under HIPAA, GDPR or other regulations could be inadvertently exposed. Sensitive data could be at risk. The MSP must examine how and where the data will be input and output and how data protection requirements will be satis ed. **INCLUDED WITH CRUSHBANK**

4. Liability and Insurance Coverage:
MSPs should evaluate their liability and insurance coverage in light of AI LLM usage. Understanding the risks involved and the potential legal consequences is critical. It may be necessary to update insurance policies to cover AI-related liabilities and to have a clear plan for handling legal disputes or claims related to AI-generated content. Ideally, the MSP should be able to leverage indemni cation provided by the operator of the LLM. **INCLUDED THROUGH IBM WATSONX**

5. Cost Transparency:
Transparency in cost management is essential for MSPs. MSPs must ensure they have clear and detailed information about the costs associated with AI LLM usage, including licensing fees, infrastructure costs, and any additional expenses. **INCLUDED WITH CRUSHBANK**

In conclusion, MSPs can leverage AI LLMs to deliver valuable services to their clients. However, they must be diligent in managing data, ensuring security, protecting third party content, addressing liability, and maintaining cost transparency to navigate the complexities of AI LLM implementation safely and responsibly. This leads to a required focus on AI governance, which is the **foundation of safe and secure usage of AI.**

The steps below are needed for responsible use of Artificial Intelligence at an MSP. Using the CrushBank AI Knowledge Management system addresses these. If you are doing this on your own, you need to make sure you complete the steps.

	Operational confidence	Manage risk and reputation	Strengthen compliance	Meet stakeholder demands
Plan	Define measurable performance metrics for AI usage across your organization	Review existing processes that monitor fairness and explainability	Conduct gap analysis against current and potential AI regulations	Review existing skills and demand for responsible AI, and align with business objectives
Build	Establish traceability and auditability of current processes	Operationalize updated processes and checkpoints throughout the AI lifecycle	Make sure model documentation is accessible	Specify the new roles, skills and learning agendas required to implement responsible AI
Create	Create automatic documentation of model lineage and metadata	Enable AI models that are fair, explainable, high-quality, minimize drift and conduct regular policy reviews	Act to strengthen regulatory compliance for data science teams without overhead	Establish a repeatable, end-to-end workflow with built-in stakeholder approvals to lower risk and increase scale

Large Language Models (LLMs)

They are in the software you are using today, but do you know the answer to these questions?

- How was the model trained?
- Are you willing to bet on the data it was trained on?
- Can the platform detect and minimize bias and hallucinations?
- Is the model transparent in terms of its contents and sources?
- Does it contain copyright materials?
- Can the model and its answers be audited?
- Does it comply with privacy and government regulations?
- Who controls the model and its input/output data?

Trustworthy AI from IBM
watsonx™

The CrushBank AI Knowledge Management system uses WatsonX from IBM. WatsonX is different from other AI platforms as it allows transparency and control of the LLM environment and uses.

The watsonx.ai component is used for building foundation models, generative AI and machine learning. watsonx.ai is used to train, validate, tune and deploy foundation and machine learning models. It can be used with different LLMs.

watsonx.governance creates responsibility, transparency and explainability in the data and AI work ows. This solution helps you direct, manage and monitor your AI activities.