IRBAI AUDIT - HARDWARE (AH-G1)

The International Regulatory Body for AI (IRBAI) has developed a framework to ensure transparency, accountability, and the responsible use of hardware in AI systems.

Performing the Audit:

As AI technologies continue to evolve, it is crucial to assess the capabilities, reliability, and potential vulnerabilities of the underlying hardware infrastructure used by AI Systems. The hardware audit involves conducting a thorough assessment of various indicatives to gauge the suitability and performance of the hardware infrastructure. The process can be performed through the following steps:

	Indicatives	Answers
Processor Type	Define the type of processors being evaluated, such as CPU (Central Processing Unit), GPU (Graphics Processing Unit), TPU (Tensor Processing Unit), or Other.	[CPU, GPU, TPU, Other]
Cluster Management	Evaluate how the processors handle cluster management, which refers to the ability to efficiently distribute computational tasks across multiple processors or machines in a cluster. Assess the scalability, load balancing, and fault tolerance capabilities.	[Yes/No: Access the scalability, load balancing, fault tolerance capabilities, Risk: High, Medium, Low]

Resource Expansion	Determine the potential for resource expansion, including the ease of adding additional processors or scaling up the computational power.	[High, Medium, Low: the availability of compatible hardware, flexibility for future upgrades]
Dimensionality	Examine the processors capability to handle high-dimensional data. High-dimensional data refers to datasets with a large number of features or dimensions. Evaluate how well the processor can handle and process such data efficiently, as it may impact performance and scalability.	[High, Medium, Low]
Performance	Assess the performance metrics of the processor, including processing speed, throughput, and latency. Consider factors like clock speed, core count, memory bandwidth, and specialized architecture optimizations that may affect the performance of AI workloads.	[High, Medium, Low: clock speed, core count, memory bandwidth, and specialized architecture optimizations]
Power Consumption	Evaluate the power consumption and energy efficiency of the processor. AI workloads can be computationally intensive, so understanding the power requirements and efficiency of the processor is crucial. Check for generator and the risks for power outages.	[Risk: Low, Medium, High]
Compatibility	Determine the compatibility of the processor with the AI frameworks, libraries, and tools being used.	[Compatible, Partially compatible, Not compatible]

Cooling and Heat Dissipation	Evaluate the cooling and heat dissipation mechanisms required for the processor. Powerful processors generate significant heat, and efficient cooling systems are necessary to prevent overheating and maintain optimal performance. Assess the cooling infrastructure and ensure it can handle the heat dissipation requirements of the processor.	[Efficient, Adequate, Inadequate]
Cost	Consider the cost implications associated with the servers including the initial investment, maintenance, and operational expenses. Consult if the company can sustain running the servers and have required capital to support the operations	[Cost-effective, Moderate cost, Expensive]
Documentations/ Guarantee	Assess the availability of technical support, documentation. Asses if the staff is fully train.	{Full Access, Limited Access, No Access}
Network Connectivity	Evaluate the network connectivity options and capabilities associated with the hardware. Assess factors such as network bandwidth, latency, reliability, and compatibility with networking protocols. Consider the requirements of the AI workload and ensure that the network infrastructure can effectively handle the data transfer and communication needs.	[Reliable, Not Reliable]
Storage	Evaluate the storage capabilities and options associated with the hardware. Assess factors such as storage capacity, data access speed, data redundancy, and scalability. Consider the storage requirements of the AI workload, including the size of the dataset and the need for efficient data retrieval and storage. Ensure that the storage infrastructure meets the performance and scalability needs of the AI application.	[Adequate, Not Adequate]

Data Security	Assess the data security measures related to network and storage. Evaluate factors such as data encryption, access controls, backup and disaster recovery mechanisms, and compliance with data privacy regulations. Ensure that adequate security measures are in place to protect sensitive AI data during network transfer and storage.	[Safe, Unsafe]