Digital Risk
AWARE
LIMITED

BOARD INSIGHTS · MICRO LEARNING · II · APRIL 2026

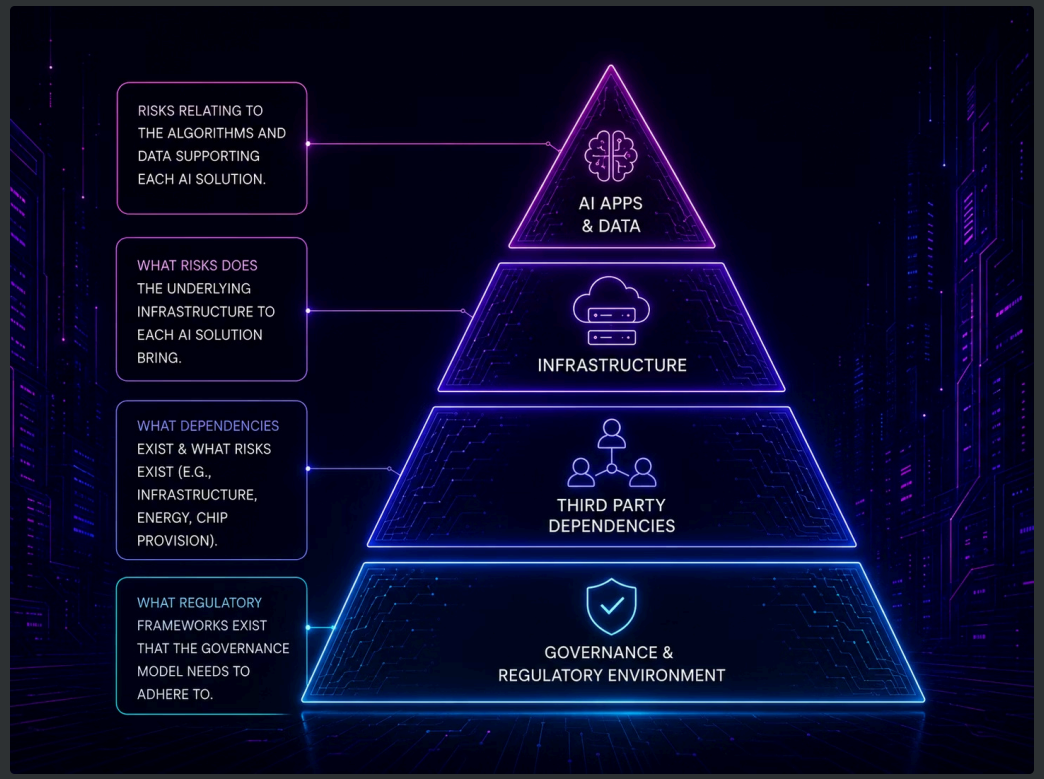
The Artificial Intelligence Integrity Stack

What are the **Killer Questions** every board must ask to understand and govern AI risk across the enterprise.

FRAMEWORK OVERVIEW

Navigating Strategic Risk Across the AI Stack

As the use of artificial intelligence continues to evolve, it is important that Boards and Senior Managers have a grasp of the impact this may have on their risk landscape.



Critical strategic risks

... will emerge across all layers of the new AI stack and working with the right risk practitioners with the experience and skills will be key to help you understand the risk priorities you may face across each dimension of the AL stack.

THE KILLER QUESTIONS

What Every Board Must Ask

Application & Data

1. How do you know the algorithms will not make invalid changes?
2. How is the AI solution protected from unauthorised changes?
3. How will you be alerted if an authorised changes occur?
4. How comfortable are you that the data feeding the algorithms is reliable (whether open source, structured or unstructured data feeds)?
5. Are all access and operational risks specific to the application and data environment adequate?
6. Is there robust Cyber Security protocols in place to protect the AI solution or data feeds from any internal or external bad actors?

Infrastructure

1. Does management fully understand the risk dependencies across the infrastructure supporting each AI solution?
2. How is this being documented and assessed to ensure a full view of the infrastructure environment exists?
3. How is management providing the board with comfort that each high priority infrastructure risk is being managed?
4. Is the Board/Risk Committee updated at each meeting to address any gaps?
5. Due to the dynamic nature of the IT environment supporting AI solutions, are the risks and assurance adequately reassessed?

Third Party Dependencies

1. Due diligence covers all risk scenarios?
2. How are the 3rd party dependencies being identified and risk assessed?
3. Is there appropriate due diligence in place over the 3rd parties you are collaborating with?
4. Does any risk assessment cover all risk scenarios – There are many with examples being loss of infrastructure, energy reliance, assurance over chip integrity, loss of sensitive datasets, access to intellectual property...)?
5. How are you obtaining comfort from each third party that the specific risk scenarios are being effectively managed?
6. Is the supporting evidence robust and boards aware of any residual risks?

Governance & Regulation

1. Is there a robust understanding of the governance and regulatory frameworks specific to the AI solutions being developed or deployed?
2. Does the board and management have a strong understanding of the risk scenarios that could create a breach in the governance or regulatory requirements??
3. How is the organisation measuring compliance against the frameworks that they need to adhere to?
4. Is the reporting & audit evidence sufficient, if a regulatory requests access to your business to understand how you are managing the requirements?