Risk Management Policy - Guidance

Purpose: To provide a guideline for defining and communicating the broad level AAA risks that organization will manage from the perspective of impact to humans, society and environment:

- Integrate the framework into the organization and specifically
- Establishing its risk tolerance/risk appetite for evaluating such AAA risks;
- Identifying metrics and thresholds for meaningful risk impact
- Defining the frequency of assessment
- Establishing oversight and accountability (committees / duly designated experts)
- Integrating Diverse Inputs and Multi Stakeholder Feedback
- Identifying risk logs and risk management documentation
- Identify training, education and awareness
    - For risk managers
    - For C-suite executives
    - For Designers and Developers
    - For the organization broadly

Accountability: The Risk Management Policy shall be created and published by the **Algorithmic Risk Committee**, in consultation with Operational Risk Management (or a Chief Risk Officer). The Risk Management Policy shall be delivered to the Board of Directors.

The **Algorithmic Risk Committee** shall manage the ongoing application of the Risk Management Policy to the system.

Definitions:
Risk Appetite - *is the type and amount of risk that an organization is prepared to accept in pursuit of its strategic objectives and business plan.*

Risk Tolerance - *is the organization's acceptable level of variation in the risk the organization is ready to bear after risk treatment in order to achieve objectives.*

Format: There is no specific format or one size fits all for **Risk Management Policy**. These illustrative examples could be considered as guidance to adapt from including the critical aspects referenced below:

- WHO
- University of Southern Queensland
- Actuaries Risk Policy Template
- Infosys Risk Management Policy
- CDSL Risk Management Policy

Critical aspects of the policy

1. **Identify significant risks (Internal and External)**
    - Examine risks to humans from the perspective of 5 pillars namely **Ethics**, **Bias**, **Privacy**, **Trust** and **Cybersecurity**.
    - In specific, ensure guidance is in place to identifying risks associated with:
        - Evaluating sufficient **Ground Truth** and **Functional Correctness** for **AAA systems** deployment
        - Evaluating fairness metrics and outcomes against established metrics, threshold or laws
        - Evaluating effectiveness of embedding Ethics, Governance or Accountability structures to oversee risks associated with **AAA systems**.
        - Evaluating broad market concerns associated with risk of **AAA Systems** beyond the Company's control significantly reducing demand for its services and harming its business, financial condition and results of operations.
        - Evaluating effectiveness of controls and procedures for compliance with the rights of **Data Subjects**, including communications and access.
        - Evaluating data protection, security risks associated with **AAA systems** and their associated data (including **Data Entry Point attacks**)
        -

2. **Define the governance, accountability and oversight of committees/ designated group of experts**
    - The organization shall match expertise, training, research and knowledge from individuals into multi disciplinary teams sufficient to satisfy the nature of risk in **AAA Systems**
    - The organization shall set up essential committees to ensure adequate segregation of duties, oversight and accountability to enable effective **Risk Input**, **Risk Evaluation** and **Risk Treatment**
    - Establishing focused committees including the **Algorithm Risk Committee** (Overall responsibility for risks contributed by algorithms), an **Ethics Committee** (trained expertise to evaluate ethical risks and instances of **Ethical Choice** associated with AAA systems), **Testing and Evaluation committee** (responsible to examine risks associated **Accuracy, Validity, Reliability, Robustness and Resilience**) and a **Children's Data Oversight Committee** (responsible for examining risks associated with processing of children's data).

3. **Define the Risk Management Process and its integration to ERM**
    - Provide a broader overview of the AI Risk Management process and its integration with Enterprise Risk Management. (Refer FH - AI Risk Management Process for more detailed guidance)

4. **Detail Risk Tolerance and Risk Appetite**
    - Consider Legal & Regulatory, Reputational, Financial, Sustainability, Operational and People & society factors to determine the **Risk Tolerance** and **Risk Appetite.**
    - Calculate the estimated monetary value of legal non-compliance associated with characteristics of the system
    - Committee responsibilities considering the six strategic risks (Economic, Political, Social, Technology, Legal & Regulatory, Environmental, People and Third party) and estimated costs associated with the assumption of risks realized
    - Manner in which the ERM plugs into the six strategic risks and the committees responsible for evaluating them.
    - Any risk above the **Risk Tolerance** is avoided by the organization. Risk tolerances are based on the maximum tolerable level of risk.
    - Risk appetite and **Risk Tolerance** may be expressed as a metric, principle or even a matrix or a rubric.
    - Define the process to establish the **Risk Tolerance** and **Risk Appetite** for each **AAA system** and the Governance to revisit them on a regular periodicity and document the actions on an ongoing basis.
    - **Risk Appetite** and **Risk Tolerance** are essential in risk evaluation, risk treatment and managing residual risk.

5. Frequency of review or reassessment of risks:
    - The committees shall establish a periodicity of reviewing risks and criteria for reassessment of risks. These criteria may include triggers gathered from:
        - **Adverse Impact Reporting System** or similar **Post-Market monitoring mechanisms**
        - Threshold setting and execution of **Systemic Societal Impact Analysis**
        - Continuous monitoring mechanism such as **KPIs for Concept Drift**
        - Procedures to manage catastrophic failures, including assessment of black box data

6. Explain the approach to gathering **Diverse Inputs and Multi Stakeholder Feedback**

- Provide a broader approach towards gathering / involving **Diverse Inputs and Multi-Stakeholders** in the process. Refer
  Diverse Inputs and Multi-Stakeholder Feedback and
  DIMSF - Guideline and template for more detailed guidance

