Risk Management Framework

1. **Identifying Risks**:

   The first stage is to identify hidden dangers. Here are some major risk categories to consider:

   - Operational risks include technological glitches, software defects, exchange malfunctions, and infrastructure breakdowns, which can disrupt trading operations and result in losses.
   - Financial Risks: Price manipulation, counterparty risk, market volatility, and unfavourable fees may expose you to losses and reduce your financial returns.
   - Technological risks include scalability issues, data breaches, cybersecurity weaknesses, and emerging blockchain technologies.

2. **Measuring Risk Exposure:**

   Identifying the potential impact of these risks is critical for making informed decisions. Here are some typical methods:

   - Qualitative Scoring: Rate the potential impacts and likelihood of occurrence of a risk, then rank mitigation options based on the ratings.
   - Quantitative Methods: Use methods such as Value at Risk (VaR) to estimate the potential loss your portfolio may experience under specific market situations.

3. **Mitigation Strategies:**

   Now that you're aware of the risks, it's time to plan your protection! The following are some important Mitigation Strategies:

   a. Market risk:
   - Diversification: Spread funds across multiple assets and marketplaces to avoid concentration risk.
   - Stop-Loss mechanisms: Use automated stop-loss mechanisms to limit losses during volatile market circumstances.
   - Monitoring and Alerts: Use real-time monitoring tools to keep track of market circumstances and set up alerts for important price changes.

   b. Operational Risks:
   - Smart Contract Audits: Hire third-party organisations to perform periodic smart contract audits.
   - Implement redundant systems and backup mechanisms to reduce technological hazards.
   - Operational Protocols: Create and enforce explicit operational protocols to reduce execution errors.

c. <u>Compliance risks</u>:

- Regulatory Compliance staff: Establish a specialised staff to monitor and enforce compliance with changing regulations.
- Internal audits should be conducted on a regular basis to examine and update compliance procedures.

4. Reporting:

Create thorough reports outlining all risk management operations, including as risk assessments, mitigation plans, and monitoring findings. These reports should be available for internal review and external auditing.