**Risk Management Framework Policy**

**Risk Identification**

* Risks are identified through **risk assessments, audits, incident reports, and stakeholder feedback**.
* Categories of risks include:
  + **Operational Risks:** Equipment failure, workforce issues, supply chain disruptions.
  + **Cybersecurity Risks:** Data breaches, phishing attacks, malware threats.
  + **Compliance Risks:** Violations of GDPR, HSE regulations, or contractual obligations.
  + **Financial Risks:** Budget overruns, economic instability.

**2. Risk Assessment & Ranking**

Each risk is **evaluated and ranked** based on **likelihood** and **impact**, using a **Risk Matrix (Low, Medium, High, Critical).**

| **Likelihood** | **Impact: Low** | **Impact: Medium** | **Impact: High** | **Impact: Critical** |
| --- | --- | --- | --- | --- |
| **Rare** | Low | Low | Medium | High |
| **Unlikely** | Low | Medium | High | Critical |
| **Possible** | Medium | High | High | Critical |
| **Likely** | High | High | Critical | Critical |
| **Certain** | High | Critical | Critical | Critical |

**3. Risk Response Strategies**

Based on the risk ranking, different **treatment strategies** are applied:

**3.1 Accept the Risk**

* Applied when risks are **low** and mitigation is unnecessary or cost-prohibitive.
* Example: **Minor software glitches that do not affect operations.**

**3.2 Treat (Mitigate) the Risk**

* Implement control measures to **reduce likelihood or impact**.
* Example: **Cybersecurity risks mitigated by multi-factor authentication, firewalls, and regular security updates.**

**3.3 Transfer the Risk**

* Shifting risk to a third party, such as **insurance coverage or outsourcing.**
* Example: **Data breach risks are transferred to a cyber insurance provider.**

**3.4 Terminate the Risk**

* If the risk is too high and cannot be mitigated effectively, the activity is **stopped or modified**.
* Example: **Eliminating high-risk manual cleaning in hazardous environments by automating processes.**

**4. Continuous Monitoring & Review**

* **Risk Reviews:** Conducted regularly to assess changes in risk levels.
* **Incident Tracking:** Logs are maintained to track emerging risks.
* **Regulatory Compliance Checks:** Ensuring risks related to legal and industry standards are managed.

This structured approach ensures risks are proactively managed while maintaining operational efficiency and compliance.