Risk Assessment Summary
Annual Review 2024

1. General Information

Date of Assessment: June 25, 2024
Assessed By: Jane Doe
Department: Operations
Location: Main Office, New York, NY

2. Scope of Assessment

This assessment reviews key operational risks affecting the department's performance and staff safety for the 2024 calendar year. Areas of focus include physical security, data protection, and compliance with regulatory standards.

3. Risk Matrix

Risk Description	Likelihood	Impact	Current Controls	Additional Actions
Data breach due to phishing attack	Medium	High	Staff training, email filters	Quarterly refresher training
Physical injury due to equipment malfunction	Low	Medium	Regular equipment inspections	Update maintenance schedule
Non-compliance with new industry regulations	Low	High	Monthly compliance reviews	Appoint compliance officer

4. Summary of Key Findings

- Overall risk profile remains comparable to the previous year, with no significant new exposures identified.
- Operational risks are primarily mitigated through ongoing training and updated compliance procedures.
- Enhanced monitoring is recommended for cyber threats and regulatory changes.

5. Recommendations

- Increase frequency of cybersecurity awareness sessions for all staff.
- Improve documentation of equipment inspections and maintenance.
- Monitor and adapt to any regulatory updates promptly.

Important Notes

- This document is a summary and should be supported by detailed assessments and evidence.
- Risk assessments must be reviewed and updated at least annually or when a major change occurs.
- The participation of relevant stakeholders is crucial for accuracy and comprehensiveness.
- Action items should be tracked and assigned to ensure continual improvement.