SIT Department Risk Matrix

Risk	Likelihood	Impact	Existing Controls	Proposed Mitigation
System Outage	Medium	High	Basic backup and recovery	Test disaster recovery plan quarterly
Data Breach	Low	High	Firewalls, limited access control	Implement multi-factor authentication (MFA)
Hardware Failure	High	Medium	Regular maintenance	Upgrade aging hardware and use proactive monitoring
Insufficient Incident Response	Medium	High	Basic response plan, not tested	Conduct incident response drills regularly

SIT Risk Control Measures Overview

Control Measure	Description	Departmental Coverage	Frequency of Review	
Firewall Protection	Protects network from unauthorized access	SIT Department	Monthly	
Data Backup	Regular backups of critical data	All Departments	Weekly	
Access Control (RBAC)	Restricts data access based on roles	SIT, HR, Finance	Quarterly	
Incident Response Plan	Guides response in case of a cyber incident	SIT Department	Bi-Annual	

SIT Proposed Action Plan for SIT Risk Mitigation

Action	Responsible Team	Timeline		
Implement multi-factor authentication (MFA)	IT Security Team	Q1 2025		

Test and update disaster recovery plan	IT Department	Q2 2025		
Replace aging IT hardware	IT Infrastructure Team	Ongoing (2025)		
Conduct incident response drills	IT & Compliance Teams	Bi-Annual (2025)		