Risk Management Plan For Marriott International

RISK	RISK CATEGORY	PROBABILITY OF RISK 1 – 3	IMPACT 1 – 3	PI SCORE Prob x Impact	EXPECTED RESULT | NO ACTION	RESPONSE OWNER	RESPONSE DESCRIPTION
External system breach	System	2	3	**6**	Shut down systems, Leading to data breaches, Service disruptions, Potential damage to the organisation's reputation	Head of IT	Shut down systems, inform employees, deny all access to systems, recovery from backups and system regeneration.
Unauthorised Access	System	2	3	**6**	Data breach, Loss of customer trust, Financial and reputational damage	IT Security Team	**Identify**: Regularly audit user access rights. **Assess**: Conduct periodic reviews of access logs. **Control**: Implement multi-factor authentication. **Monitor**: Continuously monitor access logs. **Report**: Provide regular reports on access control status.
Data Classification and Handling	Data	2	2	**4**	Unintentional exposure of sensitive information, Compromised customer data	Data Privacy Officer	**Identify**: Implement a data classification policy. **Assess**: Conduct regular audits of data handling practices. **Control**: Enforce encryption for sensitive data. **Monitor**: Monitor data access patterns. **Report**: Provide reports on data classification and handling compliance.
Physical and Environmental Security	Hardware	1	3	**3**	Potential physical damage to data centers, Disruption of services	Facilities Management	**Identify**: Check CCTV footage, **Assess:** Identify the vulnerabilities in physical security. **Control**: Strengthen physical security measures. **Monitor**: Regularly assess environmental controls. **Report**: Provide reports on the status of physical and environmental security.
Inadequate Incident Response	System	2	2	**4**	Delayed detection and response to security incidents, Increased impact and scope of security breaches	Incident Response Team	**Identify**: Regularly update the incident response plan. **Assess**: Conduct drills to test the plan's effectiveness. **Control**: Ensure clear communication channels during incidents. **Monitor**: Continuously update the incident response plan. **Report**: Provide reports on incident response drills and improvements.
Non-compliance with Data Protection Laws	Data	3	3	**9**	Legal actions, Financial penalties and fines, and reputational damage	Legal and Compliance Team	**Identify**: Regularly review and update policies for compliance. **Assess**: Conduct regular compliance audits. **Control**: Implement changes to align with data protection laws. **Monitor**: Continuously monitor changes in data protection laws. **Report**: Provide reports on compliance status and actions taken.
Network Vulnerability	Network	2	2	**4**	Unauthorised access and data interception, Compromised network integrity	Network Security Team	**Identify**: Regularly scan and assess network vulnerabilities. **Assess**: Conduct penetration testing on network defenses. **Control**: Implement and update firewall rules and intrusion detection systems. **Monitor**: Continuously monitor network traffic for anomalies. **Report**: Provide reports on network security assessments and incidents.
Insecure Handling of Hard Documents	Hard Documents	1	2	**2**	Unauthorised access to physical documents, Loss or theft of sensitive information	Document Management Team	**Identify**: Implement secure storage and access controls for hard documents. **Assess**: Regularly audit physical document access logs. **Control**: Restrict physical access to document storage areas. **Monitor**: Periodically review access logs for unusual activity. **Report**: Provide reports on the security status of hard document storage.

PROBABILITY 1 – 3 KEY
1
2
3

IMPACT 1 – 3 KEY
1
2
3