Risk Assesment Assets- Country information Database

	ASSET	OWNER	RANKING FOR			TOTALLED	IMPORTANCE
			Confidentiality	Integrity	Availability		
	Information Assets						
1	Country General Information	Admininstrator	1	5	5	11	4
2	Backups	Admininstrator	5	5	1	11	4
3	Historical Records	Admininstrator	1	5	1	7	2
4	Demographics Records	Admininstrator	1	5	1	7	2
5	Geographic Records	Admininstrator	1	5	1	7	2
6	Economy Records	Admininstrator	1	5	1	7	2
	Physical Assets						
1	Platform Servers	Admininstrator	5	5	1	11	4
	Software Assets						
1	Operating System	Admininstrator	5	4	5	14	5
2	Application Portal	Admininstrator	5	4	4	13	4
		Confidentiality	5	For Administrators only			
			1	For public information			
		Integrity	5	Must be 100% numerically accurate or unambiguous			
			1	Will tolerate a wide margin of error			
		Availability	5	Must be available immediately			
			1	Should be available within 1 week			

Risk Management - Country information Database

Initial assessment										Assessment after treatment		
Number	Asset	Owner	Importance of Asset	Risk Events	Probability of occurrence	Risk severity	Exposure or impact	Treatment strategy	Trigger date	Treated probability of occurrence (should be reduced)	Treated risk severity (should be same or less)	Residual risk exposure or impact
Information Assets												
1	Country General Information	Admininstrator	4	Input of inaccurate information	1	1	3%	Prevention: Auditing information regularly, Restrict access to input information, review of information before adding it to the database. Contingency: Have a backup files containing accurate previously reviewed information.	2/4/2022	4	1	12.80%
2	Backups	Admininstrator	4	Loss of backup data	3	5	48%	Prevention: Storage of various backups in two different locations	2/4/2022	1	1	3.20%
3	Historical Records	Admininstrator	2	Modification of records by accident	4	2	13%	Prevention: Storage of various backups in two different locations, audit information regularly, Restrict access to records. Contingency:Recover records from backup	2/4/2022	2	1	3.20%
			2	Loss of records	3	4	19%	Prevention: Storage of various backups in two different locations	2/4/2022	2	1	3.20%
4	Demographics Records	Admininstrator	2	Modification of records by accident	4	2	13%	Prevention: Storage of various backups in two different locations, audit information regularly, Restrict access to records. Contingency:Recover records from backup	2/4/2022	2	1	3.20%
			2	Loss of records	3	4	19%	Prevention: Storage of various backups in two different locations	2/4/2022	2	1	3.20%
5	Geographic Records	Admininstrator	2	Physical damage of records by accident	5	5	40%	Prevention: Storage of various backups in two different locations, audit information regularly, Restrict access to physical records if any. Contingency: Recover records from backup. Acceptance: If there are any maps to be stored in physical form the damage of time cannot be avoided	2/4/2022	4	3	19.20%
			2	Loss of records	3	5	24%	Prevention: Storage of various backups in two different locations	2/4/2022	2	1	3.20%
6	Economy Records	Admininstrator	2	Modification of records by accident	4	2	13%	Prevention: Storage of various backups in two different locations, audit information regularly, Restrict access to records. Contingency:Recover records from backup	2/4/2022	2	1	3.20%
			2	Loss of records	3	4	19%	Prevention: Storage of various backups in two different locations	2/4/2022	2	1	3.20%
Physical Assets												
1	Platform Servers	Admininstrator	4	Hardware Failure	4	5	64%	Prevention: Use fault tolerance techniques like RAID and Cluster technology. Reduction: Frequent backup policy or use private cloud storage.	2/4/2022	2	1	6.40%
			4	Natural disasters	1	3	10%	Prevention: Use fireproof material for infrastructure, Use fire-alarms, Use fire-safety equipment. Transference: Use insurance services for equipment and data. Acceptance: Natural disasters often can't be avoided.	2/4/2022	1	1	3.20%
Software Assets												
1	Operating System	Admininstrator	5	System intrusion	4	3	48%	Prevention: Use an Intrusion Detection System, use auditing done by Operating System	2/4/2022	2	2	16.00%
			5	Malware infection	4	3	48%	Prevention: Conformity to established policies and standards, frequent scan of system for detection of any malware.	2/4/2022	3	2	24.00%
			5	Vulnerabilities	4	3	48%	Reduction: Apply authorized patches as soon as available	2/4/2022	3	2	24.00%
2	Platform Portal	Admininstrator	5	System failure	3	4	48%	Prevention: Usage of adequate configured firewalls and IDS Contigency: Backup data regularly	2/4/2022	3	3	36.00%
						Risk Factor	22%				**Risk Factor**	3%