

Report Title: Risk Details

Run Date and Time: 2024-06-28 18:32:10 Pacific Daylight Time

Run by: System Administrator

Table name: sn_risk_risk

Risk

Number:	RK0020610	Active:	false
Inherit from risk statement:	false	State:	Retired
Name:			
Information Technology Asset Management			
Description:			
The organization does not have an updated CMDB that can provide better visibility of information assets across the organization			
Risk Statement:		Entity:	Asset - Computer
Category:	IT	Sync with entity owner:	true
		Calculated score:	2 - Low
Risk relevance:			

Ownership

Owning group:		Owner:	Susan Orwell
---------------	--	--------	--------------

Assessment

Assessment:	NIST CSF Asset Management Assessment
Assessment respondents:	Susan Orwell, Abel Tuter

Scoring

Inherent SLE:	\$2,000,000.00	Residual SLE:	\$500,000.00
Inherent ARO:	5	Residual ARO:	3
Inherent impact:	2 - Low	Residual impact:	1 - Very Low
Inherent likelihood:	5 - Extremely Likely	Residual likelihood:	5 - Extremely Likely
Inherent ALE:	\$10,000,000.00	Residual ALE:	\$1,500,000.00
Inherent score:	3 - Moderate	Residual score:	2 - Low
Calculated ALE:	\$1,500,000.00		
Calculated score:	2 - Low		

Response

Response:	Mitigate
Plan:	
Justification:	
Avoidance steps:	

Insurance contract:	Acceptance state:
Vendor:	Acceptance end date:

Monitoring

Control compliance percentage:	0	Control failure factor:	0
Control non-compliance percentage:	0	Indicator failure factor:	0
		Calculated risk factor:	0

Activity journal

Additional comments:

Related List Title: Assessment instance List

Table name: asmt_assessment_instance

Query Condition: Control/Risk/Requirement = Information Technology Asset Management AND Entity != (empty) AND State = Complete

Sort Order: Number in descending order

1 Assessment instances

▼ Number	Metric type	Due date	State	Assigned to	Percent answered	View responses
AINST0010009	NIST CSF Asset Management Assessment	2024-07-12	Complete	Susan Orwell	100	View Responses

Related List Title: Risk Response Task List

Table name: sn_risk_response_task

Query Condition: Risk = Information Technology Asset Management

Sort Order: Number in ascending order

1 Risk Response Tasks

Name	Plan	Task type	Priority	Assigned to	State
Mitigate Risk of Information Technology Asset Management	1. Conduct a comprehensive inventory of all information assets, including data, documents, and systems. 2. Classify information assets based on their sensitivity and criticality, using a risk-based	Risk Mitigation	3 - Moderate	Susan Orwell	Cancelled

Name	Plan	Task type	Priority	Assigned to	State
	<p>approach (e.g., confidential, internal, public).</p> <p>3. Identify the owners and custodians of each information asset.</p> <p>4. Implement role-based access control (RBAC) to ensure that only authorized personnel have access to sensitive information assets.</p> <p>5. Encrypt all sensitive information assets, both in transit and at rest.</p> <p>6. Establish an incident response plan to promptly respond to information asset-related incidents by designating an incident response team to contain, investigate, and remediate incidents.</p> <p>7. Develop and conduct a regular training program to create awareness in order to educate employees on information asset management best practices.</p> <p>8. Regularly review and update the information asset inventory and classification while continuously monitoring access controls, encryption, and incident response processes.</p> <p>9. Ensure compliance with relevant regulations making sure that our stand on information asset management aligns with industry standards</p>				