

# Implementing Enterprise-Wide Data Classification and Protection



## Client Overview

A global sovereign investment company, managing assets valued at over \$400 billion, operates across multiple geographies with diverse investment portfolios. The organization handles highly sensitive financial data, proprietary investment strategies, and confidential stakeholder information across on-premise and cloud environments, requiring robust data protection and governance frameworks.

## Challenges Faced

The client faced critical data security risks stemming from lack of visibility and control over sensitive information across the enterprise.



### No Data Visibility or Categorization

Corporate data was scattered across multiple on-premise and cloud assets without categorization or inventory.



### Absence of Classification Tools

No tools or systems were in place to identify, categorize, or track sensitive information.



### Unvalidated Information Sharing

No validation mechanisms were available for data shared with internal users or external parties.



### High Risk of Data Leakage

Uncontrolled sharing led to significant exposure of confidential information.



### Compliance and Governance Gaps

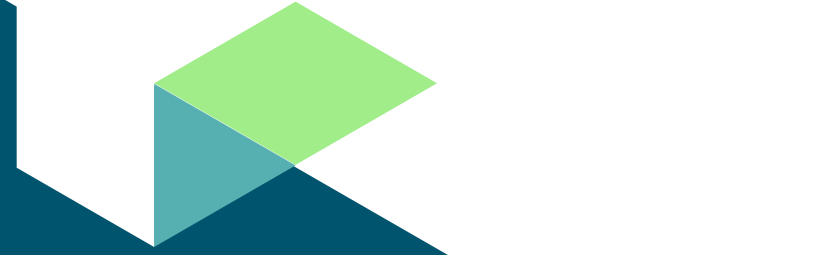
The client was unable to demonstrate data handling controls for regulatory compliance and stakeholder confidence.

## The Solution

Amiseq implemented a comprehensive Data Classification and Protection program through improved data handling policies, deployment of Titus data discovery and classification tools, and integration with in-house applications for monitoring. The solution combined technical implementation with end-user training and enterprise-wide rollout with ongoing support.



Why the Client Chose



Enterprise data  
classification and  
protection program  
expertise

Comprehensive DLP and  
data protection across  
endpoint, network, and  
cloud environments

Regulatory compliance and  
risk mitigation in sensitive  
data environments

Deployment of data  
discovery and classification  
tools at scale

Integration of technical  
implementation with policy  
development and user  
adoption

# Strategy and Implementation



## Improve Data Handling Policies and Procedures

Develop and implement enhanced data handling policies and procedures establishing clear classification and sharing standards.



## Implement Data Discovery and Classification Tools

Deploy Titus for data discovery and classification across enterprise assets.



## Integrate with In-House Applications

Establish integrations with existing applications for analysis, monitoring, and reporting of data handling activities.



## Execute End-User Adoption and Training

Develop and deliver comprehensive adoption plans and training programs educating users on data handling standards.



## Rollout and Support

Deploy tools enterprise-wide and provide ongoing support addressing user issues.

# What Amiseq Delivered



## Complete Data Visibility

Provided a full view of confidential, internal, and general data across the enterprise.



## Automated Classification System

Integrated Titus for automated monitoring and reporting.



## Validated Information Sharing

Implemented real-time checks to ensure only authorized data sharing.



## Enterprise-Wide Adoption

Rolled out organization-wide with embedded standards.

## Conclusion

The client successfully transformed its data security culture from reactive to proactive, establishing enterprise-wide visibility and control over sensitive information.

This program demonstrates Amiseq's capability to deliver complex cybersecurity transformations combining technology implementation, policy development, and organizational change management.

## Strengthen Your Data Security Posture

See how Amiseq can help your organization establish comprehensive data classification and protection programs. Contact us today.

### California, AMISEQ HQ

📍 1551 McCarthy Blvd Suite # 207  
Milpitas CA 95035.

☎ +1 510 509 9888

