Cloud Storage Encryption Vulnerability Checklist

General Information

Project Name	
Cloud Provider	
Date Reviewed	
Reviewer	

Encryption Settings

Checklist Item	Status	Comments
Is data at rest encrypted?		
Is data in transit encrypted?		
Are strong encryption algorithms in use (e.g. AES-256)?		
Are encryption keys rotated regularly?		
Are customer-managed keys (CMK) supported/used?		
Is key management handled securely?		
Is there an audit trail for key access/use?		
Are unmanaged/unencrypted buckets or shares detected and flagged?		

Vulnerability Review

Item	Status	Comments
Unencrypted backup or snapshot detected		
Misconfigured encryption permissions		
Publicly accessible encrypted objects		
Legacy protocols that bypass encryption		
Encryption key stored with data		
No alerting for encryption failures		

Notes / Actions