



CLOUD SERVICE RISK MANAGEMENT (CSRM)

The rate of newly available cloud services and cloud service providers has increased significantly over the past few years and this new capability has brought about tremendous business efficiencies and cost reduction benefits.

However, as organisations start making use of and growing their cloud services platform, and as these services become more readily available within the organisation, there is a certain level of information risk that may be introduced into the environment. These include the risk of information breaches and loss of organisational information.

We provide a holistic cloud risk management service to help you identify and manage your cloud risks, either at the point of making a decision to use a cloud service provider, for existing cloud service providers or even identifying cloud services being used that you may not be aware of. We partner with leading cloud access security brokers to analyze your cloud network traffic and identify the cloud services in use.

WITH THIS INFORMATION, WE CAN ASSIST YOU WITH IDENTIFYING THE RISKS POSED TO YOUR ORGANISATION AND WITH OUR EXPERTISE ASSIST YOU IN MANAGING THESE RISKS.

Our approach to managing your cloud service risks encompasses the following:

- Identifying cloud services most suitable to your risk appetite, in instances where you are looking to expand your cloud service platform and introduce new cloud services;
- Identifying unknown cloud services being used that process organisational information;
- Identifying information that is being shared with and processed by approved and unapproved cloud service providers; and
- Managing the risks associated with approved and unapproved cloud service providers through formally defined governance models and policies.

Result? Your organisation is aware of the cloud services being used, the information that is being processed and stored within these cloud services and the risks associated with these cloud services. In addition, your organisation has the ability to actively manage cloud service risks and ensure compliance to information regulations and organisational policies.

Contact Mobius Consulting:
info@mobiusconsulting.mu
www.mobiusconsulting.mu

THE MOBIUS ADVANTAGE

EXPERTISE

- Knowledge within the cloud services domain;
- Partnerships with leading Cloud Access Security Broker (CASB) service providers;
- Information governance and security;
- Information risk management; and
- Dynamic consultants with:
 - Certification in Risk and Information Systems Control (CRISC)
 - Certification in Information Security Manager (CISM)
 - Certification in European privacy law (CIPP/E)

APPROACH

- Holistic: big picture thinking ensures an integrated and comprehensive assessment in line with enterprise and third-party risk management
- Risk-based: ensures solutions, including governance models and policies, are created based on your unique risk landscape
- Sustainable: ensures processes are defined and implemented to allow for continuous monitoring and management of risks

RESULTS

- Awareness of your cloud service landscape
- Awareness of what information is processed within cloud services
- Awareness of the risks associated with cloud service providers
- A sustainable approach to managing your organizations cloud service risk, which leads to:
 - Improved information security;
 - Increased regulatory compliance; and
 - Information risk reduction

CLOUD SERVICE RISK MANAGEMENT (CSRM) APPROACH



PHASE ONE CLOUD SERVICE RISK ASSESSMENT

- Identify all cloud services currently in use
- Determine the risk rating of cloud services using the cloud confidence index
- Document and report on the cloud services identified



PHASE TWO ADVANCED CLOUD SERVICE RISK ASSESSMENT

- Perform detailed analysis of the type of information being transferred and processed on the identified cloud services



PHASE THREE DEVELOP CLOUD SERVICE GOVERNANCE

- Develop an organisational specific cloud governance framework to manage the risk exposure of integrating cloud services in the organisation
- Develop cloud service policies such as cloud information transfer policy, cloud information access control policy and data leakage prevention policy
- Define cloud service management standards



PHASE FOUR REMEDiate AND IMPLEMENT

- Implement the governance framework, policies and processes through awareness and training of affected employees
- Implement cloud service management standards through configuration of these standards on a centralised cloud access security broker



PHASE FIVE CONTINUOUS MONITORING AND MANAGEMENT OF CLOUD SERVICE RISKS

- Continuously monitor and identify unsanctioned cloud applications
- Manage and report on identified cloud service risks



>> Let us help you identify, remediate and manage your cloud service risk.