**Reference projects**

**PROJECT 1**

**Cloud discovery**

A large multinational suspected that the enterprise trade-off of a variety of cloud services was not only a consequence of the lack of flexibility with the need for highly correlated business processes, but also the lack of control over security, compliance and the corresponding risk of using them.

The results of this assessment demonstrate that a number of high-risk services were adopted by employees with limited visibility to data being stored and processed. An additional concern expressed by the business partner was the increasing security of cloud services and the potential for misused information in those services.

The client requested our support to ensure that their cloud provider could align cloud adoption with business needs, legal and technical security requirements and the risk of cloud services would be adequately managed.

KPMG performed a risk assessment by using their own framework mapping to risk and control measures, and an additional benefit of this framework was to ensure that the risks of cloud services were better understood. As a result, the client was able to gain visibility into the overall scope and potential risk associated with adoption of new cloud services.

As a result, the client was able to gain visibility into the overall scope and potential risk associated with adoption of new cloud services.

**PROJECT 2**

**Cloud risk assessment**

For an oil & gas client, KPMG is performing a large remediation programme aimed to align the company’s multi-cloud deployment with security and privacy standards. The client was also identified that employees were using personal cloud solutions for the same purposes. For which the client requested our support to ensure that their cloud provider could align cloud adoption with business needs, legal and technical security requirements and ensure that the use of cloud solutions would be adequately managed.

KPMG performed a risk assessment by using their own framework mapping to risk and control measures, and an additional benefit of this framework was to ensure that the risks of cloud services were better understood. As a result, the client was able to gain visibility into the overall scope and potential risk associated with adoption of new cloud services.

As a result, the client was able to gain visibility into the overall scope and potential risk associated with adoption of new cloud services.

**PROJECT 3**

**Risk management platform**

For an oil & gas client, KPMG is developing a strategy for transferring to cloud-based email, storage and collaboration services. For cost reduction and increased efficiency, KPMG performed a risk assessment by using their own framework mapping to risk and control measures, and an additional benefit of this framework was to ensure that the risks of cloud services were better understood. As a result, the client was able to gain visibility into the overall scope and potential risk associated with adoption of new cloud services.

**Why KPMG?**

KPMG can support your organisation in adopting cloud services with appropriate levels of security and governance, and address the full cloud journey, starting with cloud services identification and risk assessments, towards cloud governance, security and compliance transformation.

Our cyber security approach is based on the principle of capability building and service delivery, which is an integrated approach to developing the capability of a company to respond to and mitigate security threats.

The information contained herein is of a general nature and is not intended to address the circumstances of any particular individual or entity unless otherwise stated. Although we endeavor to provide accurate and timely information, there can be no assurance that such information is accurate or complete, or that a particular recommendation is suitable for a particular individual or entity. We do not undertake any obligation to update any information contained herein. The content provided in this document is for informational purposes only and is not intended to provide legal, accounting, tax, or other professional advice. The content does not constitute a representation of any specific KPMG service or service offering.© 2017 KPMG Advisory N.V., registered with the trade register in the Netherlands under number 33263682, is a member firm of the KPMG network of independent member firms affiliated with KPMG International Cooperative (“KPMG International”), a Swiss entity. All rights reserved. The KPMG name and logo are registered trademarks of KPMG International. For more information on KPMG International, visit kpmg.com/aboutkpmg.

**Contact us**

For more information on our cloud security services, please contact one of our professionals or visit us at kpmg.com/GlobalSecurity.

**Ban Kruutzen**

Partner

+31 20 656 7137

ban.kruutzen@kpmg.nl

**Edwin Sturrus**

Manager

+31 20 656 7248

edwin.sturrus@kpmg.nl

**Olga Kulikova**

Senior Consultant

+31 20 656 7137

olga.kulikova@kpmg.nl

**KPMG can support your organisation in adopting cloud services with appropriate levels of security and governance, and address the full cloud journey, starting with cloud services identification and risk assessments, towards cloud governance, security and compliance transformation.**
Cloud Security Journey

1 Discover
You can’t manage what you can’t see. With that in mind, you first need to know whether your employees or contractors are already using cloud services with or without your consent.

Start by identifying all cloud services in use by your employees and contractors.

KPMG SERVICE: CLOUD DISCOVERY

2 Define
Cloud does not require complex governance, but it does require clear rules: Do your employees know when they can use cloud services for personal purposes, or what they should be aware of when storing business data in cloud solutions? Does your IT staff understand how to connect the cloud to their on-premise systems and how to enable secure access management?

Continue by adapting your existing IT policies and end-user code of conduct to make them cloud ready.

KPMG SERVICE: CLOUD GOVERNANCE FRAMEWORK

3 Assess
Cloud services come in greater numbers than your traditional IT suppliers. This requires assessing whether existing or planned use of the cloud fits in with your organisation’s risk appetite.

Continue by assessing the identified or planned cloud services against your policies and define the required actions.

KPMG SERVICE: CLOUD RISK ASSESSMENT & VENDOR COMPARISON

4 Deploy
The issues identified during the assessment stage must be addressed. This includes actions to improve protection measures, such as access control, but also actions to ensure effective detection & response integration with the cloud provider.

Continue by deploying your remediation actions to implement a secure cloud architecture.

KPMG SERVICE: CLOUD SECURITY ARCHITECTURE

5 Automate
Cloud adoption processes lend themselves well to automation. This increases process performance and compliance, while reducing costs.

Finish your journey by locking in the benefits through automation.

KPMG SERVICE: CLOUD ADOPTION TOOLKIT & RISK MANAGEMENT PLATFORM

The evolving landscape of cloud services is a promising development for organisations that seek to digitise their processes. If IT and security staff do not proactively enable the organisation to benefit from these developments, we see the amount of shadow IT growing and the associated risks increasing.

The good news is that the use of cloud services can actually help organisations to become more secure and to better comply with regulations, as long as the adoption of cloud follows an orderly path, as depicted on the left.

The ultimate stage of the cloud journey involves automation of the cloud adoption processes, to stay in control of the quickly changing IT landscape, providing maximum transparency with minimal manual effort.

Whether you are at the start of the cloud journey, or approaching the ultimate stages, KPMG is ready to help you to take the next step in a practical and effective manner, to increase your organisation’s security by using cloud services.
PROJECT 1
Cloud discovery

A large multinational suspected that the employees traded stock on a variety of cloud-based tools, which could result in a huge risk to the reputation and integrity of its share price. To ascertain this, KPMG performed an in-depth discovery and assessment of the entity’s cloud activities, identified the corresponding risk of using it.

The results of this assessment demonstrated that a number of high-risk services were in place by employees with large volumes of data being handled by uncontrolled, unmonitored, and unauthenticated cloud services. The objective was to discover cloud services that were of high risk without the knowledge of the IT organisation and steered towards the most trusted cloud solution instead. As a result, the client was able to gain visibility in the overall scope of cloud services, the risks associated with adoption of new cloud services, and the corresponding risk of using them.

PROJECT 2
Cloud risk assessment

For an oil & gas client, KPMG performed a large remediation programme where the client requested to monitor their cloud-based shadow IT services, which process organisation and which the business has purchased or developed. KPMG also recommended that manual interventions by IT staff were considered to be the least secure on-premises solution, which resulted in some possible changes to the cloud governance, security, and compliance processes.

KPMG performed a risk assessment by using their own framework mapping to cloud standards and best practices, such as CSA, HITRUST, NIST, and ISO. A number of high risks were identified in an assessment prior to deploying the cloud solution. After doing so, KPMG identified that the use of cloud services would not be able to adequately manage the risk. KPMG proposed a solution for full automation of the cloud in the risk assessment, which can be run on secure web gateway and cloud access security broker. Further supplemented by the KPMG SOFY Digital Risk Platform. The platform was able to manage the associated risk analysis and remediating processes.

KPMG then performed the follow-up automation of the cloud discovery and identification of the risks associated with the cloud adoption processes. The volume of shadow IT today is such that manual interventions by IT staff are considered to be the least secure on-premises solution. This resulted in some possible changes to the cloud governance, security, and compliance processes.

PROJECT 3
Risk management platform

A client in the financial sector, who had previously adopted a Cloud Access Security Broker (CASB) business case, wished to reduce the amount of enterprise-ready solutions. In addition, to steer employees towards a Cloud Access Security Broker (CASB) business case, a number of high risks were identified in an assessment prior to deploying the cloud solution. After doing so, KPMG performed a risk assessment by using their own framework mapping to cloud standards and best practices, such as CSA, HITRUST, NIST, and ISO. A number of high risks were identified in an assessment prior to deploying the cloud solution.

As a result of the risk treatment prior to adopting the cloud solution, a number of high risks were identified that required proactive measures, such as ENISA, NIST, ISO, and Business Risk management. The results of this assessment demonstrated that a number of high-risk services were in place by employees with large volumes of data being handled by uncontrolled, unmonitored, and unauthenticated cloud services.

KPMG proposed a solution for full automation of the cloud solution, which can be run on secure web gateway and cloud access security broker. Further supplemented by the KPMG SOFY Digital Risk Platform. The platform was able to manage the associated risk analysis and remediating processes.