cloud security alliance®

Cloud Octagon Model

Model for Improving Accuracy and Completeness of Cloud Computing Risk Assessments

TABLE OF CONTENTS

EXECUTIVE SUMMARY

In the last few years, time to market, cost advantage and operational resiliency among many other factors have fueled the adoption of cloud computing. The research and advisory company Gartner indicates that IT spending on cloud computing services is expected to double to $216 billion by 2020.

The cloud computing market has grown significantly in size and number. Major cloud service providers (CSPs) including Amazon, Microsoft and Google have transformed Infrastructure as a Service (IaaS) and Platform as a Service (PaaS) models making them technically efficient for SaaS providers. Across industries, we are seeing large scale adoption of cloud-based business applications from such providers.

Irrespective of their size, organizations are adopting cloud-based solutions in some form or other, ranging from SaaS applications on the public cloud to hybrid/private PaaS/IaaS solutions. Businesses tailor cloud formations that best suit their workload requirements. Consequently, both the organizational data and its supporting IT infrastructure are moving away from traditional data centers.

Although businesses have succeeded in reducing operational overheads and gained economically by moving to the cloud, concerns around security, compliance, vendor lock-in, data portability, etc. continue to surface. For instance, the Interop ITX research report “2017 State of the Cloud” identifies security and compliance as the key challenges for private and hybrid cloud implementations. Furthermore, as privacy regulations strengthen globally, adherence to stringent controls across industries is desired.

The sheer complexity arising from diversity in the number of cloud-based services, implementation approaches (on premise, dedicated, etc.) and security aspects make cloud security very challenging. Moreover, for large organizations where security aspects such as legal, compliance, Service Level Agreements (SLAs) and privacy are dealt with by separate internal departments, ensuring that all security risks are identified and addressed may seem difficult.

Furthermore, while CSPs undergo strict audits such as Service Organization Control (SOC) meeting regulatory requirements that are specific for the organization can be quite daunting.

This whitepaper aims to draw upon the security challenges in cloud computing environments and suggests a logical approach to deal with security aspects in a holistic way. It introduces a Cloud Octagon model. This model makes it easier for organizations to identify, represent and assess risks in the context of their cloud implementation across multiple actors (Legal, Information Risk Management, Operational Risk Management, Compliance, Architecture, Procurement, Privacy Office, Development teams and Security.

SECURITY CHALLENGES IN CLOUD COMPUTING

International boundaries are blurring and new cloud-based technologies are being introduced at a rapid pace. Both factors contribute to the ever-changing environment in which firms compete. Regarding the aspects of technology and innovation, large firms are continuously subjected to external competition, often from much smaller start-up firms. Thus time to market takes precedence and security is often overlooked. As a result, organizations are exposed to inherent risks and evolving security challenges.

Broadly, these challenges can be grouped into the following categories:

1. Awareness
2. Cloud Strategy
    a. Cloud Service Model, Hosting and Processing
    b. Technology
    c. Contract and SLAs
3. Data Governance, Privacy and Security
4. Assurance

Awareness

Typically, within an organization, departments (such as Legal, Privacy, Compliance, etc.) that are responsible for managing cloud risk operate in silos. This leads to a lack of common understanding. For instance, the Privacy office will address data and privacy concerns. At the same time the Legal department may ensure that the cloud solution meets local legal requirements.

Cloud Strategy

Cloud strategy should address key elements such as service model (IaaS, PaaS and SaaS), data processing, hosting and service requirements. Large organizations often struggle to define a secure cloud strategy, as the requirements (such as processing, hosting and service) are diverse and spread across different functions within organizations.

Furthermore, the technology which enables the cloud computing landscape evolves continuously. This rapid evolution also restricts the smooth portability of applications. The security configuration review of a cloud computing solution are often overlooked. Consequently, the risk profile of the organizations adopting the cloud increases over time.

Data Security

Customers and stakeholders demand that their data (business) information is protected from security breaches.

Some key aspects of cloud computing security such as data ownership, provisioning of digital identities, logical access and encryption of data, etc. are either unknown or unmanaged for the cloud project team. Moreover, seeking the right relevant information from the CSPs is a challenge. Furthermore, regulatory requirements such as geographical location of information needs to be explicitly requested from a SaaS CSP.

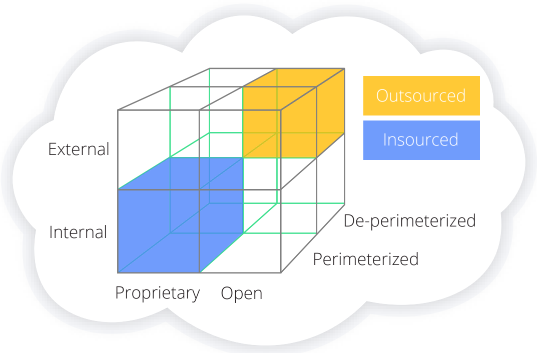
Assurance

To meet local regulatory and compliance requirements, organizations seek assurance of the effectiveness and proper management of information security controls implemented by the CSP Examples are the requirements imposed to CSPs by HIPAA, PCI DSS, etc. In demonstrating the required assurance levels, CSPs often fail in either the scope or the depth of their effort (i.e. unclear and/or insufficient). For example: not all subcontractors are in scope; not all trust criteria are in scope. Small and Medium Sized Business (SMB) CPS offer little assurance. They are ISO 27001 certified at best.

EXISTING APPROACHES

In 2009, Jericho Forum introduced the Cloud Cube Model (CCM).

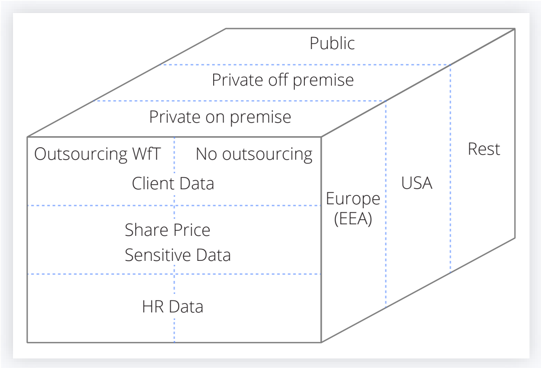
Security aspects are represented by each of the three plus one dimensions defined in the model. For instance, a cloud formation could comprise an external hosting provider and proprietary solution, installed in a perimeterized environment that is managed by an external party (outsourced).



The Jericho Forum Cloud Cube Model

Although the Cloud Cube was a good starting point, in our experience of adopting this model to the financial environment, the author of this paper ran out of dimensions to cover project complexity.

Key security aspects such as data criticality and assurance levels could not be represented. In practice, with evolving security requirements and growing complexity of the organizations, not all aspects of the security requirements could be accommodated in the Jericho Forum Cloud Cube model. HR data, share price sensitive data and client data are all confidentiality critical from a data classification schema perspective. Yet client data is perceived to be more critical than HR data. How do cloud project teams get clarity on this matter?



Cloud Cube in a Large Financial Organization

PROPOSED SOLUTION APPROACH

Businesses can address security risks by implementing the right controls which meet security requirements. In order to secure cloud implementations, requirements which are tailored to offset potential risks, risks need to be identified in the context of the cloud.

These requirements are likely to evolve over time under the influence of changes in technology, providers, regulations, scale, etc. Also, the addition of new cloud services or change in the deployment model, for instance movement from hybrid to public or vice-versa, could necessitate additional security aspects. Moreover, different departments are responsible for dealing with specific security aspects. They look at cloud risk from their perspective or lens.

The evolving nature of cloud implementation and the security (regulatory, compliance, etc.) landscape often results in new security challenges which cannot be represented by a limited set of dimensions in a cube.

The Cloud Octagon Model was developed to support your organizations risk assessment methodology. The model provides practical guidance and structure to all involved risk parties in order to keep up with rapid changes in privacy and data protection laws and regulations and changes in technology and its security implications. Goals of this model are to reduce risks associated with cloud computing, improve the effectiveness of the cloud risk team, improve manageability of the solution and lastly to improve security.

A single Cloud Octagon represents the context for a specific cloud application. For instance, a SaaS based CRM solution. Multiple octagons indicating internal/external departments can be connected together to represent organizational structures. Security aspects which a department is responsible for could be included as well. For instance, the Privacy Office department which concerns with data privacy regulations can be represented by a single Octagon. The security team can create octagons on the topics of SOC report reviews, data center visits, penetration testing, and continuous monitoring.

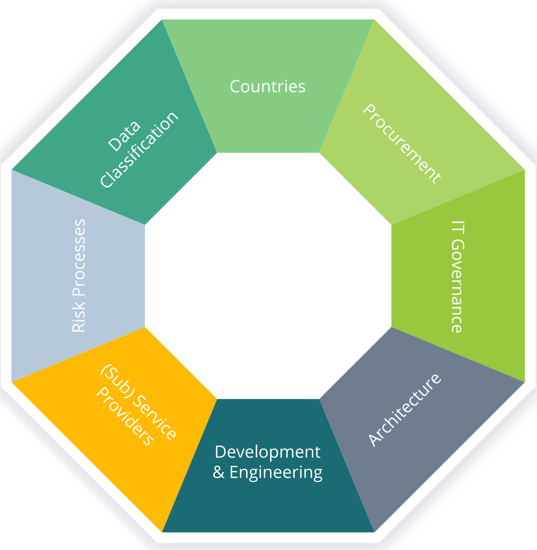


Figure 1 Octagon model

POSITIONING OCTAGON MODEL IN RISK ASSESSMENTS

What if an organization already has procedures and tools for cloud risk assessments or its regulator demands that the risk assessment methodology is supported by international standards? The octagon model can be supplementary to an organization's existing risk assessment methodology. By applying it, risk assessments will be completer and more accurate.

The following tables provide information on how to position the cloud octagon model with ISO 31000. The inner rectangle is covered by the octagon model.

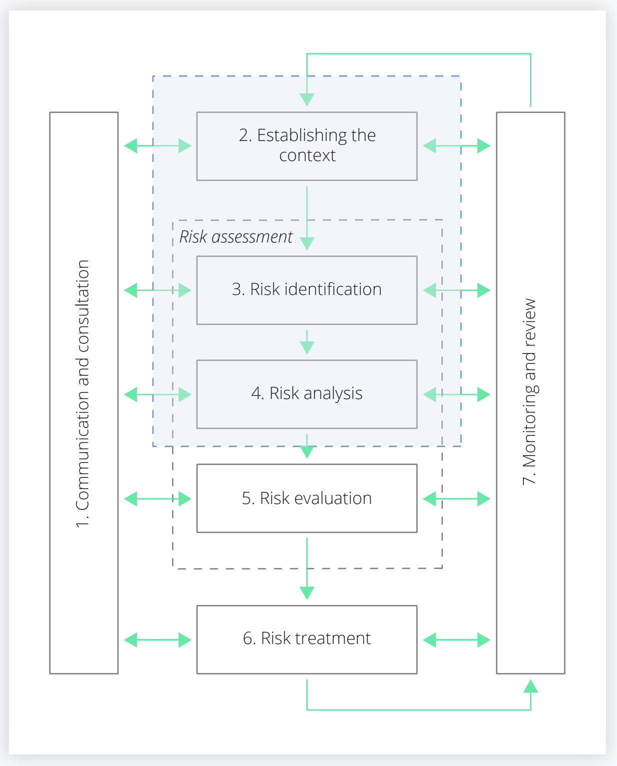


Figure 2 Octagon model is applicable to sections 2, 3, 4

ISO 31000	**Octagon model, questions for the risk team**
2 Establishing context	What is the data classification? In which countries are we hosting & processing data? Sign the CPS contract or will CSP sign the organizations contract? Which security policies and standards apply? Does the design meet architecture requirements? What does the chain of service providers look like? What will be the scope and depth of the risk assessments? What should be the risk team composition?
3 Risk identification	Identification and selection of relevant security controls by taking the results of establishing context into account. In the octagon model this is an iterative process and performed in every phase of the project. By going through the model like if it is a PDCA cycle more insight into risk is gained. Cloud project phases are: RFP; contracting; design & implementation; continuous monitoring. The octagon model does not introduce new risk workshops or tools. It is a mechanism to increase the depth of the risk assessment.
4 Risk analysis	The security controls from the octagon model assist the team in gaining insight into a.o. dependencies. During RFP phase the team learns that the level of assurance offered by the CSP's in the provider chain is limited. Nothing further is done with this information. Colleagues from legal and procurement are not aware. During RFP phase the team learns that the level of assurance offered by the CSP's in the provider chain is limited. After playing the cloud octagon game, the team is aware of the options for site visits and data center visits. They ask their colleagues from legal and procurement to include these controls in the contract negotiation. Once agreed interviews on site at the CSP are conducted and the data center is reviewed from a physical security perspective.

	Here the added value of the octagon model is the extra attention that is paid to the architecture standards and architecture governance. For cloud projects that want to deviate from standards for the sake of speed or innovation, a form review by an Architecture Review Body is made obligatory.
5 Risk evaluation	Not in scope of the octagon model.
6 risk treatment	Not in scope of the octagon model.

In addition to the risk management framework of your organization (e.g. NIST SP 800-37, ISO 31000, ENISA) specific instruments and or requirement sets can be used to support the cloud risk assessment process.

Actor	Type of process	Type of process
Procurement	Procurement	ENISA cloud procurement document
Legal	Contracting	CSA privacy level agreement
Vendor management	Procurement	CSA CAIQ
Privacy Officer	Privacy Impact Assessment	PIA tool
Security 1st line	Risk assessment with focus on IT security	Security requirements from a.o. CSA CCM, ISO 2700x, NIST, your organization's policies
Security 1st line	Risk assessment	Octagon model
Operational Risk Management	Risk assessment	Octagon model
Information Risk Management (2nd line)	Risk assessment	Octagon model
Compliance	Risk assessment	Octagon model
Cloud project members	Risk assessment	Octagon model

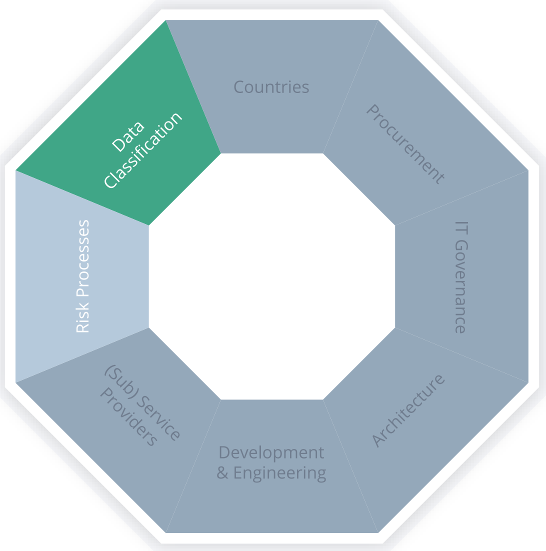
The team marked with the yellow color is a multi-disciplinary team that goes through the octagon model aspects a few times, during the phases of a cloud journey.

OCTAGON MODEL EXPLAINED

In order to provide an innovative solution to a retail customer base existing of millions of customers, a large Dutch bank and a Nordic start-up company agreed to a partnership. One of the results of this partnership was that transaction data from retail customers would be processed and stored in a public cloud environment. In order to determine what risks this introduces to a highly regulated financial institution, the cloud octagon can be used to determine the cloud context and the risk associated to that context as illustrated in an example project.

Core Function, Data Classification

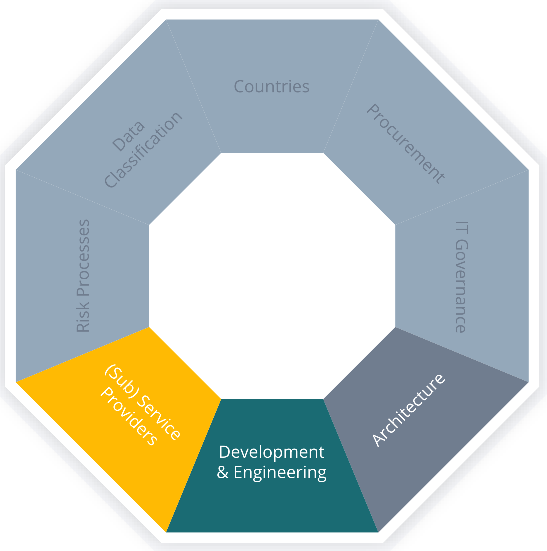
Processing payments for customers is considered one of the core functions of a bank. Data resulting from this core function, transaction data, is the main input needed to deliver the new service. A connection between the back end of the bank and the back end of the start-up needed to be established so that transaction data could be shared real time, granting the start-up access to transaction data. In order to determine the value of the data, it is classified using the CIA triad (confidentiality, integrity and availability). Transaction data was classified as confidentiality and integrity critical; this resulted in business, legal and security requirements that not only apply to the technical aspects of the solution but also cover the governance aspects. Classification of data aided in ensuring the following controls were in place:



- Encryption of critical data in transit
- Agreements on key ownership and management
- Logical access control to restrict access to data
- Identity and access management governance
- Ownership of data

Cloud Service Model, Cloud Deployment Model, Subservice Providers

In order to determine the risk associated with the implementation, the cloud service model, the cloud deployment model and the presence of subservice providers needed to be evaluated. The bank decided to leverage a SaaS solution, which is hosted in a public cloud environment. Due to the partnership element, a customized version of the SaaS solution was designed and co-developed. Responsibilities (e.g. IT operations) are shared between the two parties, which makes it

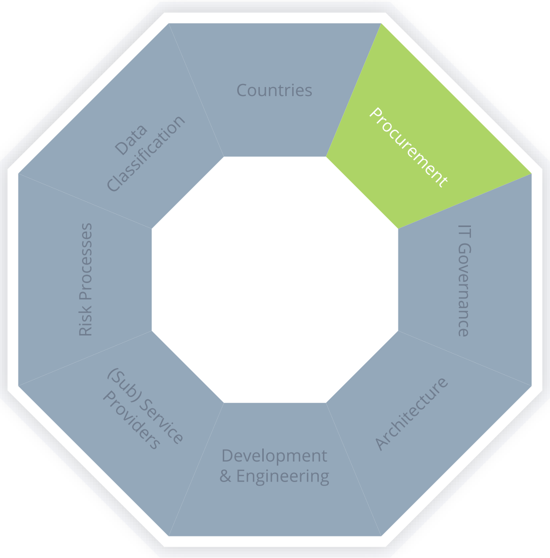


deviate from a standard SaaS solution and thus increases complexity. The bank furthermore has no direct contract with the underlying PaaS solution; thus, assurance must be obtained via the start-up. Evaluating the cloud service model, cloud deployment model and the presence of subservice providers aided in ensuring the following controls were in place:

- Obtaining assurance throughout the chain of providers
- Awareness of shared responsibilities between three different parties
- Awareness of and mitigation in place for malicious insiders
- Evaluation of the lock-in risk
- Due diligence

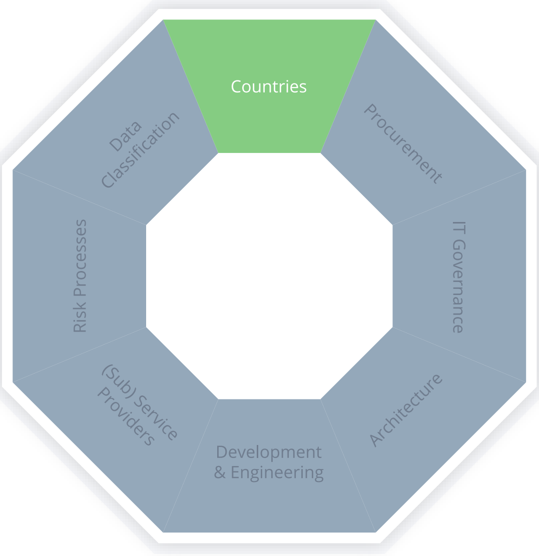
Procurement

One of the facets of the cloud octagon is procurement, which is in place to ensure involvement of applicable risk parties during the procurement process of cloud parties. In the early phases of procurement a Change Risk Assessment workshop was organized to identify possible risks and discuss mitigating controls. Early involvement of the legal department furthermore ensures that contract clauses in the contract are included regarding, for example, the right to audit, assurance reports, permission to conduct penetration testing, obligations in regard to (security) incidents and a sub-service provider clause. Involvement during the procurement phase enabled the bank's security office to conduct an onsite visit on the start-up premise to obtain assurance on its security controls and processes as no assurance reports were available. Contract clauses were included to ensure the start-up would become ISO 27001 certified within an agreed timeframe. Early engagement ensured all risk processes could be followed, which made it possible in an early phase to identify, evaluate and mitigate risks in an effective manner. Making procurement part of the risk assessment methodology for cloud ensured



- Right to audit for the bank and the regulator
- Permission to conduct penetration testing
- Early risk identification and mitigation

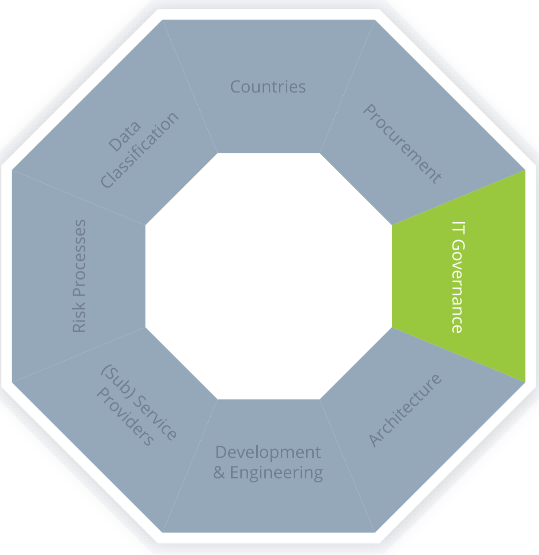
Countries Using, Processing, Hosting



Cloud computing often results in data being used, processed, back upped and hosted in different geographical locations. Geographical spread, especially if this means that data is distributed over multiple continents, introduces challenges for legal, compliance and security. In this particular case, a Dutch bank partnered with a Nordic start-up. This means the data is used and processed within the same continent. In regard to hosting, the start-up leveraged cloud services from Amazon Web Services (AWS) located in Germany. From a legal and compliance perspective this means that all data is used, processed and hosted within Europe and thus European rules and regulations apply. AWS is, however, an American company; therefore, legal had to ensure that customer and transaction data hosted in Germany could not be transferred to the US without the consent of the Bank. Consideration of diverse geographical locations in the risk assessment methodology ensures that

- Data cannot be transferred to another country without consent
- Data in motion shall be protected
- Compliance to laws and regulations in multiple countries

IT, Governance and Security Policies



Outsourcing services to a cloud provider may result in less control over the data for the financial institution. This is especially true in the case of an SaaS service where the service is often fully managed by the cloud provider and the client needs to rely on the existence and effectiveness of adequate IT operations and security policies. Procedures and standards need to be evaluated to ensure there is no conflict between the financial institution and the cloud provider. The start-up company was subjected to a full risk assessment in order to determine whether there was a gap between the requirements set by the bank (and its regulators) and the procedures and standards of the start-up and its subservice provider. Doing so resulted in the following:

- Agreements of roles and responsibilities between the bank and start-up were described in the contract
- Agreements on IT operating procedures including but not limited to access control, change management, patch management, logging and monitoring, incident response, back-up and Disaster Recovery and data deletion upon contract termination

Based on the business scenario described above, it can be concluded that applying the facets of the cloud octagon into the risk assessment process aids in reducing risks associated with cloud computing, improves security and manageability of the solution and ensures a smooth implementation of an innovative, cloud-based solution within a traditional financial institution.

The next section explains how to apply the octagon model in a risk assessment.

RISK ASSESSMENTS

When performing a risk assessment on a cloud computing initiative, a general risk assessment process from your organization is followed. It can be derived from an ISO standard, NIST or for example ISF IRAMv2. It is the cloud change profile part that is specific to the octagon model.

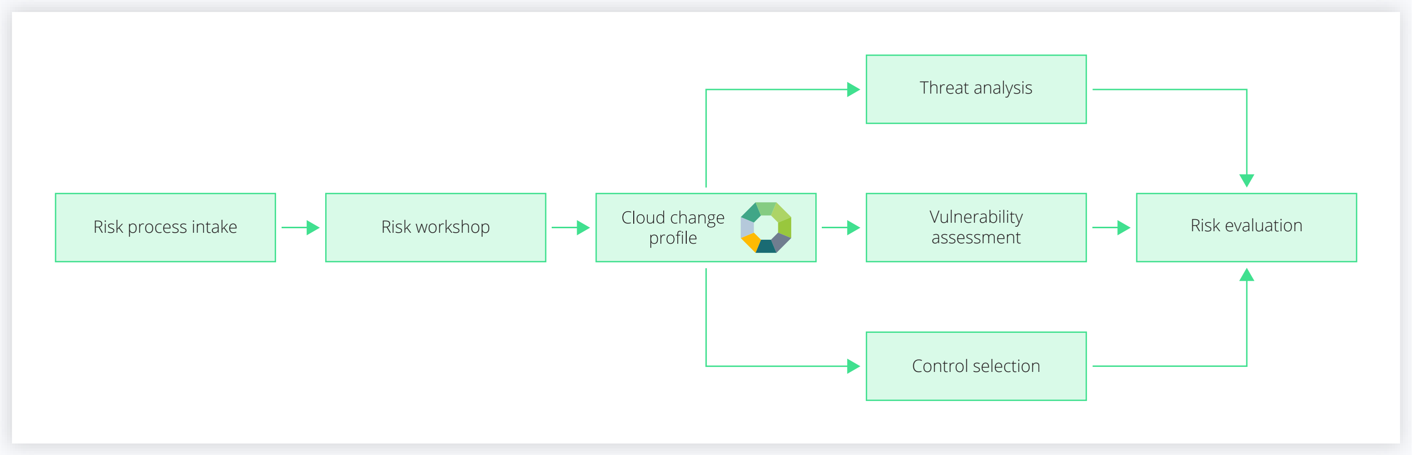


Figure 3 General Risk Assessment Process

Implementing/applying the aspects of the octagon model allows identification of the context or profile of a cloud change. And since projects do not usually know from the beginning exactly which providers and services they are going to use, this process can be repeated in multiple workshops during the cloud journey.

Threat analysis can be performed using Microsoft STRIDE (https://docs.microsoft.com/en-us/azure/security/azure-security-threat-modeling-tool-threats). This is not included in this paper.

The vulnerability assessment and risk evaluation is performed by the organization's security professionals.

Control selection should be automated via cloud change profile or context. Organizations can use their own security library with requirements or the CCM from CSA.

CSA cloud security alliance® Cloud Controls Matrix

The Cloud Security Alliance Cloud Controls Matrix (CCM) is specifically designed to provide fundamental security principles to guide cloud vendors and to assist prospective cloud customers in assessing the overall security risk of a cloud provider. The CSA CCM provides a controls framework that gives detailed understanding of security concepts and principles that are aligned to the Cloud Security Alliance guidance in thirteen domains. The foundations of the Cloud Security Alliance Controls Matrix rest on its customized relationship to other industry-accepted security standards, regulations, and controls frameworks such as the ISO 27001/27002, ISACA COBIT, PCI, NIST, Jericho Forum and NERC CIP, and will augment or provide internal control direction for service organization control reports attestations provided by cloud providers.

As a framework, the CSA CCM provides organizations with the needed structure, detail and clarity relating to information security tailored to the cloud industry. The CSA CCM strengthens existing information security control environments by emphasizing business information security control requirements, reduces and identifies consistent security threats and vulnerabilities in the cloud, provides standardized security and operational risk management, and seeks to normalize security expectations, cloud taxonomy and terminology, and security measures implemented in the cloud.

https://cloudsecurityalliance.org/group/cloud-controls-matrix/

By using the octagon model in combination with CCM, you can do more with the information provided by CSA. You are challenged to look at topics from perspectives other than those of than the provider. You are challenged to look at controls with a more helicopter view. Doing so makes the risk assessment more complete. In addition, linking controls from CCM to octagon topics like procurement or data classification makes risk assessment more accurate.

Let’s look at two example controls from CCM.

DSI-01 data and objects containing data shall be assigned a classification by the data owner based on data type, value, sensitivity, and criticality to the organization.

In the area of data classification the octagon model challenges the team to see if data classifications across application interfaces are aligned. The model makes sure ratings are challenged by experts, signed off and properly documented. This includes taking into account the privacy impact assessment results.

STA-09 Third-party service providers shall demonstrate compliance with information security and confidentiality, access control, service definitions, and delivery-level agreements included in third-party contracts. Third-party reports, records, and services shall undergo audit and review at least annually to govern and maintain compliance with the service delivery agreements.

In the area of service providers the octagon model challenges the team to investigate the entire chain of service providers and the assurance levels offered. The cloud project team looks at providers from a data processing perspective and subsequently decide on relevant controls during the contracting phase of your cloud journey. When organizations are using plus ten SaaS applications to support a particular business process, the octagon model will address the topic of managing landscape complexity.

Not all cloud project teams reach this level of detail in their risk assessments. The controls from the cloud octagon model assists in making the in making the cloud risk assessments more accurate and complete.

Other instruments from CSA that can be used for risk assessment include the following:

The Consensus Assessments Initiative Questionnaire (CAIQ)
Based upon the CCM, the CAIQ provides a set of Yes/No/NA questions that a cloud consumer and cloud auditor may wish to ask of a cloud provider to ascertain compliance to the CCM and CSA best practices. Nearly all cloud providers have experience with the CAIQ and can often provide a completed copy relatively quickly (although in some cases an NDA is necessary).

https://cloudsecurityalliance.org/group/consensus-assessments/

The CSA security guidance document is the official study guide from the Certificate of Cloud Security Knowledge. This 150+ page document offers guidance on fourteen domains.

https://cloudsecurityalliance.org/group/security-guidance/

The STAR Registry is a publicly accessible website where cloud providers post both self-assessments and third-party audits based upon CSA cloud security standards. By insisting upon cloud provider transparency, CSA's STAR entries deliver a level of detail around security practices previously only available under a non-disclosure agreement (NDA). These entries provide valuable information that enterprises can compare to customer requirements. All major cloud providers and hundreds of others have adopted the STAR program. Enterprises can query the STAR Registry to search for cloud providers they wish to evaluate or procure. If a cloud provider does not appear in the STAR Registry, customers can send the CAIQ to the provider. CSA STAR program offers information about Cloud Service Providers that can be used during the procurement phase of the cloud journey and for continuous monitoring after go live.

https://cloudsecurityalliance.org/star/

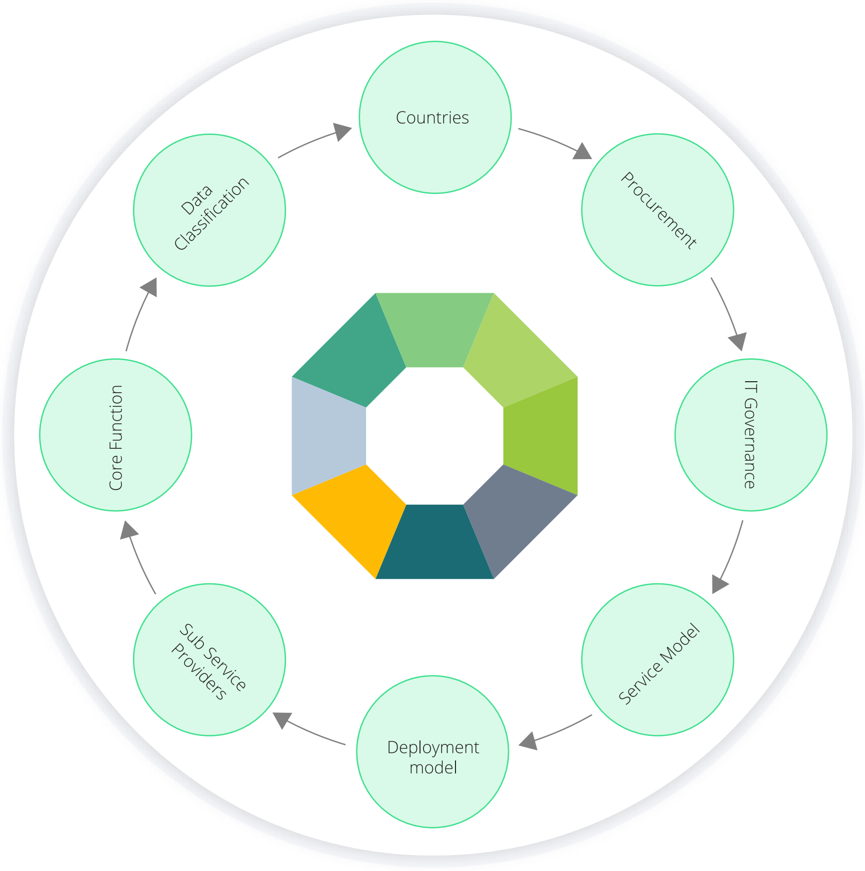


Figure 4 Going through all octagon aspects multiple times improves accuracy and completeness.

In the beginning of the cloud journey a (multi-disciplinary) risk team goes through all octagon aspects, using the information currently available. Later, additional or new information becomes available, for example, a vendor is chosen and contract negotiations begin.) For the second time the team reviews all octagon aspects, and the risk assessment is refined. In a later stage the vendor is contracted, and the implementation is 90% finished. Again, the team applies the model and refines the risk assessment. Multiple teams or disciplines need to be involved in risk assessment workshops, each with a different focus.

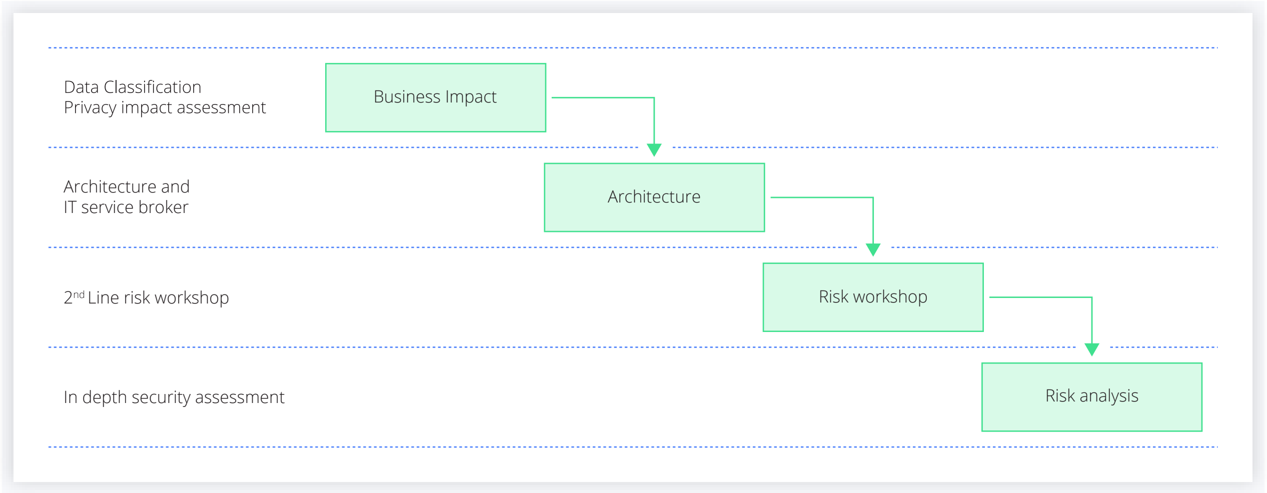


Figure 5 Look at risk from multiple perspectives.

Once the cloud change profile is known, it can be used for security requirements selection.

During a 2nd line risk workshops the European Union for Network and Information Security (ENISA) cloud risks are discussed (a Dutch regulator requirement).

For a Request for Proposal (RFP) on a SaaS application a document with your organization’s security requirements phrased as questions shall be available.

In a cloud team, that is experienced in risk assessments

> - There is a table available with risk ratings for common findings which should always be checked against the particular change scenario of the project that is risk assessed.
> - There is a document explaining the difference between SOC 1 2 3.
> - For reviewing a SOC report, there is a document available with all ISO 27001 controls. All controls are mapped to sections of the SOC report, and if there are any gaps, risks are identified.
> - For site surveys to data centers, there is a physical security checklist.
> - For risk assessments on SMB cloud providers who do not offer SOC2, there is an Excel sheet with security controls as well as a vendor security requirements list.
> - There is a threat profile available created by the risk management team.

For the project team

> - There is a Privacy Impact Assessment website.
> - There is a data classification form.
> - There is a briefing on how to register the cloud application at the corporate cloud governance board, which has to approve usage of the application and report it to the regulator.

What level of assurance is offered across the chain of service providers?

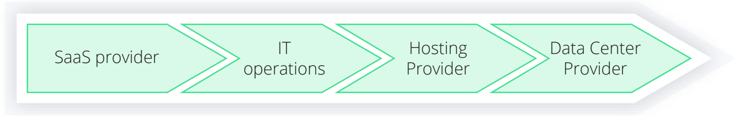


Figure 6 The entire chain of service providers must be investigated.

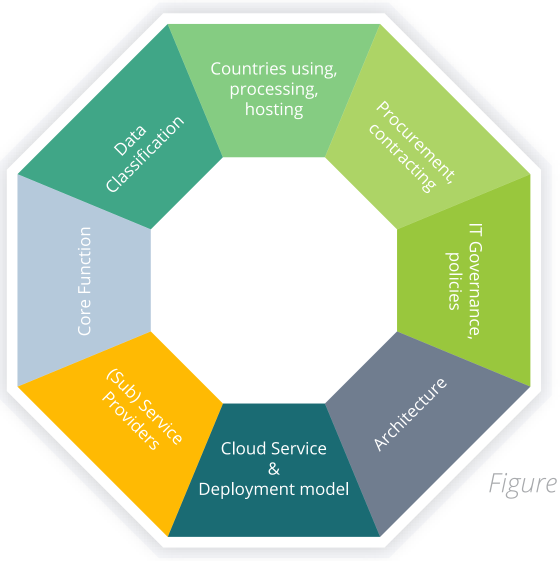


Figure 7 Octagon model

REQUIREMENTS SELECTION

To enable requirements selection the requirements must be labeled or have properties that can be used for selection. The selection is performed using change context variables. Examples of these variables are: the number of sub-contractors; the countries for deployment; the Privacy Impact Assessment score. Depending on the situation of the cloud initiative, some requirements are more relevant than others.

Requirement labels should be designed in such a way that the requirements can be stacked on top of each other. De-duplication after selecting might be needed. This probably means that a spreadsheet with filters does not perform this entire job; an application with a database is more suitable.

Requirements

> - That always apply
> - For non-sensitive data
> - For sensitive data
> - For confidentiality critical data
> - For integrity critical data
> - For availability critical data
> - For privacy criteria
> - For material outsourcing
> - For country specific

Every requirement

> - Is phrased as a question for the RFP phase
> - Has a flag identifying the party responsible for implementation
> - Has a flag when relevant for continuous monitoring after go-live

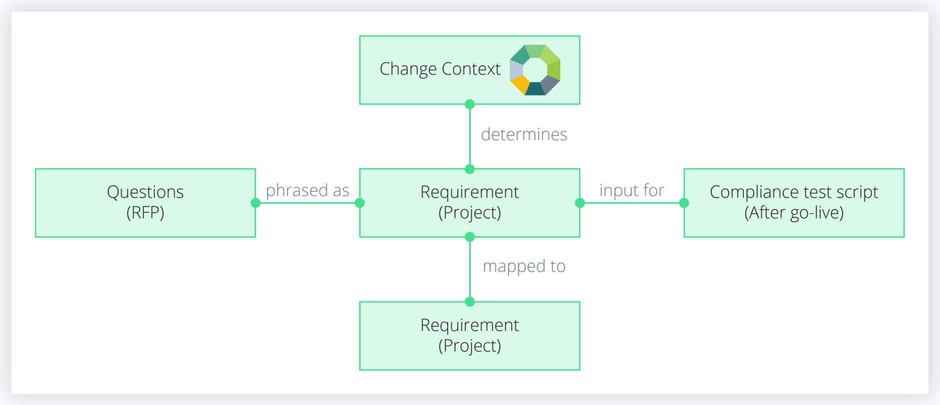


Figure 8 Re-use of Material for Various Purposes

CONTROL SELECTION

The octagon model is based on four years of experience in cloud risk assessments. It is not based on frameworks like ISO 27001 and CobIT. The authors of this paper looked for a model that did not require procurement of a license. The model contains security controls. A summary is presented here. A full list can be found in the appendix.

Data Classification

- A data classification shall be established, preferably for the end state of a project and not for a proof of concept or minimal viable project. The latter occurs more in a PaaS environment.
- A data classification must be challenged by 2nd line experts before approval.
- A data classification must be aligned when creating interfaces to other applications in the back office of your organization. Especially when the cloud application is used as a golden source for other applications to use.
- The recommendations that result from the privacy impact assessment should be addressed in the overall change risk assessment.)

Countries

- For SaaS applications that are deployed globally in an organization, the team must pay attention to where the application is hosted and in which countries the cloud application is processing data and what the possible consequences are from a legal, compliance, privacy, operational risk and or security perspective. Cross border data transfers must be taken into account.
- Local (privacy) requirements should be taken into account as early as the RFP phase of the project.
- Local risk workshops per country of deployment should be conducted, and local security officers should be consulted.

Procurement

- The security team should be well-aligned with the procurement team and involved during RFP and contracting phases.
- A standard set of security questions for RFP must be available.
- A standard cloud contract with security annex and Service Level Agreement must be in place.
- A contract clause for data exit shall be part of the contract.
- A contract clause on the topic of subcontractors shall be part of the contract.
- In case of material outsourcing the contract must include clauses on the topics of right to audit for the organization and right to examine for the regulator.
- During the procurement phase of your the cloud project, any country-specific requirements should be discussed, negotiated, and agreed upon, for example, in the area of (privacy) incident reporting.

IT Governance

- This section is highly dependent on the organization's cloud and security policies and architecture standards. Most cloud (SaaS) projects are driven by business people. In organizations that have transformed to an agile way of working, bridge builders between IT and the business (formerly known as COO) no longer exist. As a consequence cloud projects are steered by people who are unfamiliar with the formal IT changes processes of the organization. Finding an audience for security requirements and getting the message across might not be easy. So in addition to technical security requirements the cloud project team should pay attention to the following:

- In addition to sharing security requirements via email (Office documents or applications like ServiceNow) face-to-face meetings can be held and walk-in sessions with the security team can be organized and hosted.
- Cloud project teams can develop a cloud awareness game based on the control set from the octagon model.
- Sufficient cloud security knowledge must be present in the team conducting the risk assessment. It is worth considering having the colleagues involved in quality review and or document approval to be ISC2 CCSP certified. In addition CSA CCSK is recommended for all participants. Those interested in vendor neutral education can look at the education offerings from Arcitura.

Risk Processes

Risk assessments shall be performed from multiple perspectives, such as operational risk, privacy, compliance, legal and security. This document has a focus on the security risk assessment. In general a risk assessment consists of the following components:

- Preparation
- Information gathering and fieldwork
  - In case the Cloud Service Provider (CSP) offers little assurance, the organization/company might benefit from a site survey. More insight can be gained when interviewing the CSP security officer and asking for a demonstration of the security control implementation.
- Security requirements engineering
  - Requirements are based on data classification, PIA results and context.
- Security consultancy (risk mitigation)
- Risk identification, rating and formal acceptance
- Teams should be trained on how to review SOC assurance reports. When reviewing a SOC audit report, the team should verify if the trust criteria in scope are aligned with the data classification.
- The team should discuss and agree on requirements for continuous monitoring after go live.

Architecture

- In the authors opinion all cloud journeys should start with talking to the architects, starting with the topic of re-use before build before buy. It is possible that the architecture function has a broker role and gives advice on which cloud to use, based on workload characteristics. In addition architects can be asked for advice on application integration and perimeter security.
- Verification of architecture standards must be done at the beginning of a project.
- A cloud project team must be knowledgeable on architecture standards.
- Architect involvement must be documented for the benefit of the cloud governance body.
- Solution Architecture document must be documented and approved.

Chain of Service Providers

- A SaaS application is, in most cases, delivered by a chain of service providers. This chain of providers must be investigated and reviewed, starting in the procurement phase. Who are the parties involved and what level of assurance is offered?
- Are subcontractors in scope of SOC reports? If not, investigate further.
- Are subcontractors addressed in contracts? Is this verified in case of SME providers hosting on clouds like Azure and AWS?

Development & Engineering

- Not within the scope for SaaS and therefore not described in detail.

Bringing it all together

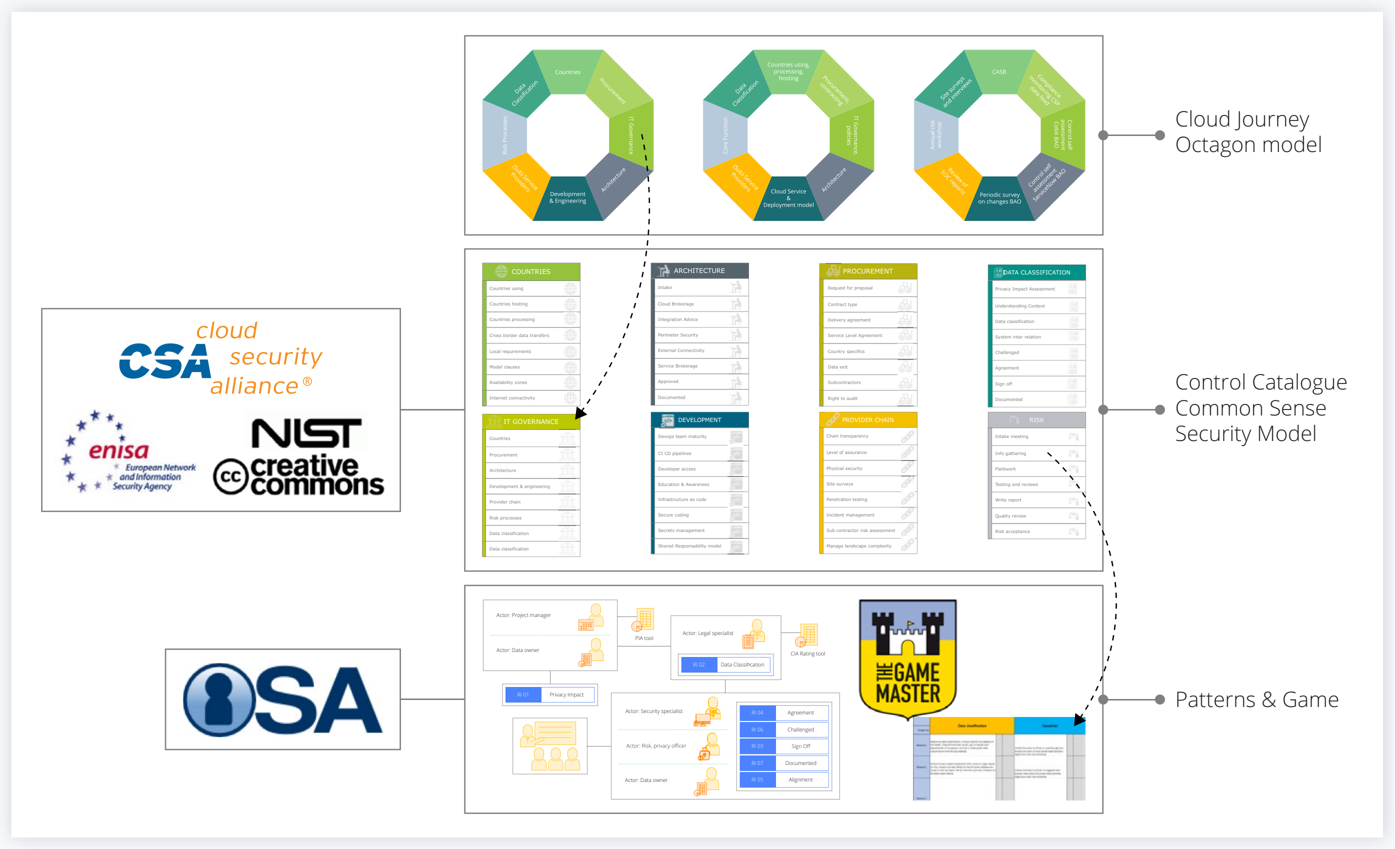


Figure 9 Complete Overview of the Concept

SUPPORTING PATTERNS

The author has developed a number of patterns that can support a cloud risk assessment. Following the patterns and associated controls helps to do a more thorough and complete job.

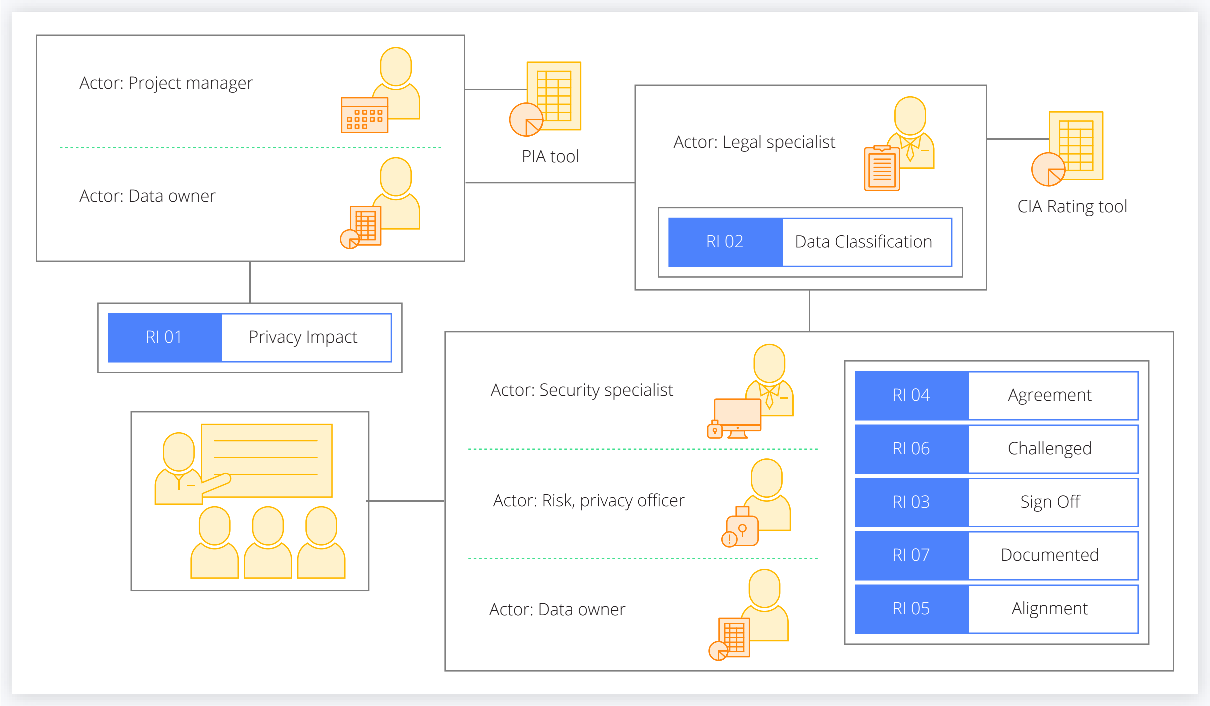


Figure 10 Pattern for Data Classification.

Example of Controls from Octagon Model

- RI01 Privacy Impact Assessment
  Performance of a Privacy Impact Assessment (PIA) using the tooling provided by the Privacy Office. When the impact score is high, the issues should be addressed in a risk workshop.
- RI02 Data Classification
  Classification of the data processed by the cloud application. Determination of the possible impact on the aspects of Confidentiality, Integrity and Availability.
- RI 03 Data Owner Sign Off
  Assurance that the data owner signs off on the agreed data classification

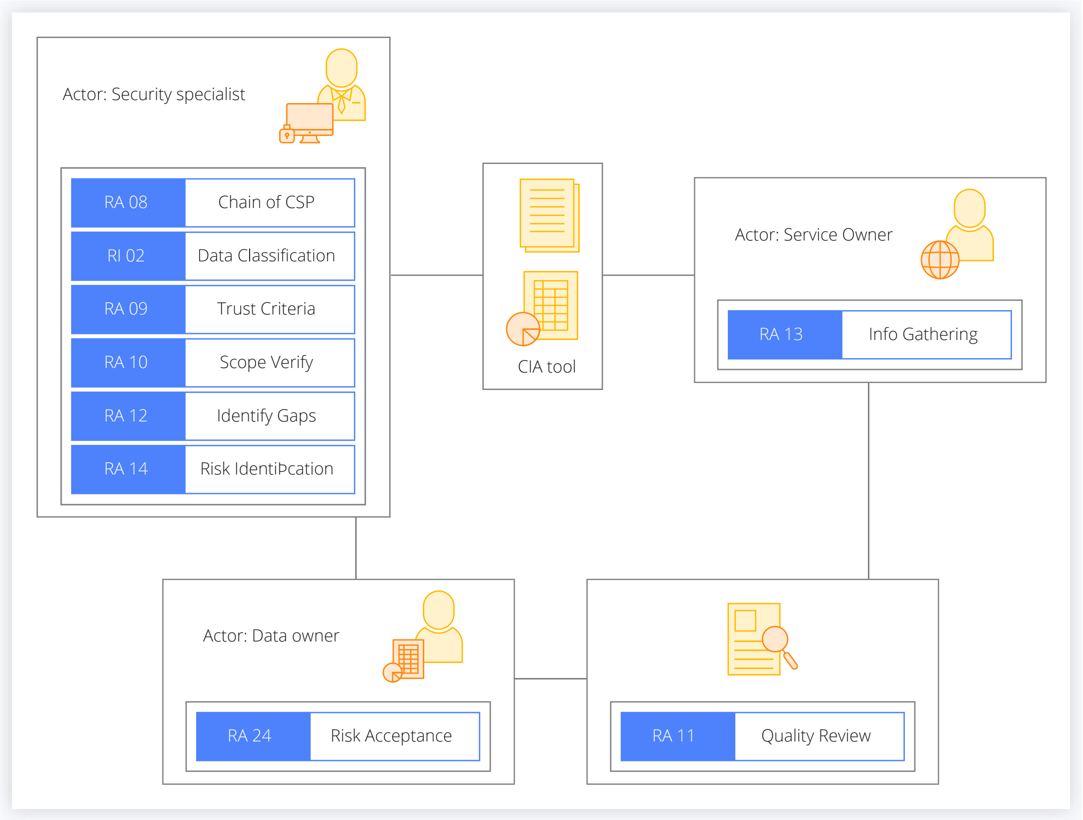


Figure 11 Pattern for SOC Report Review

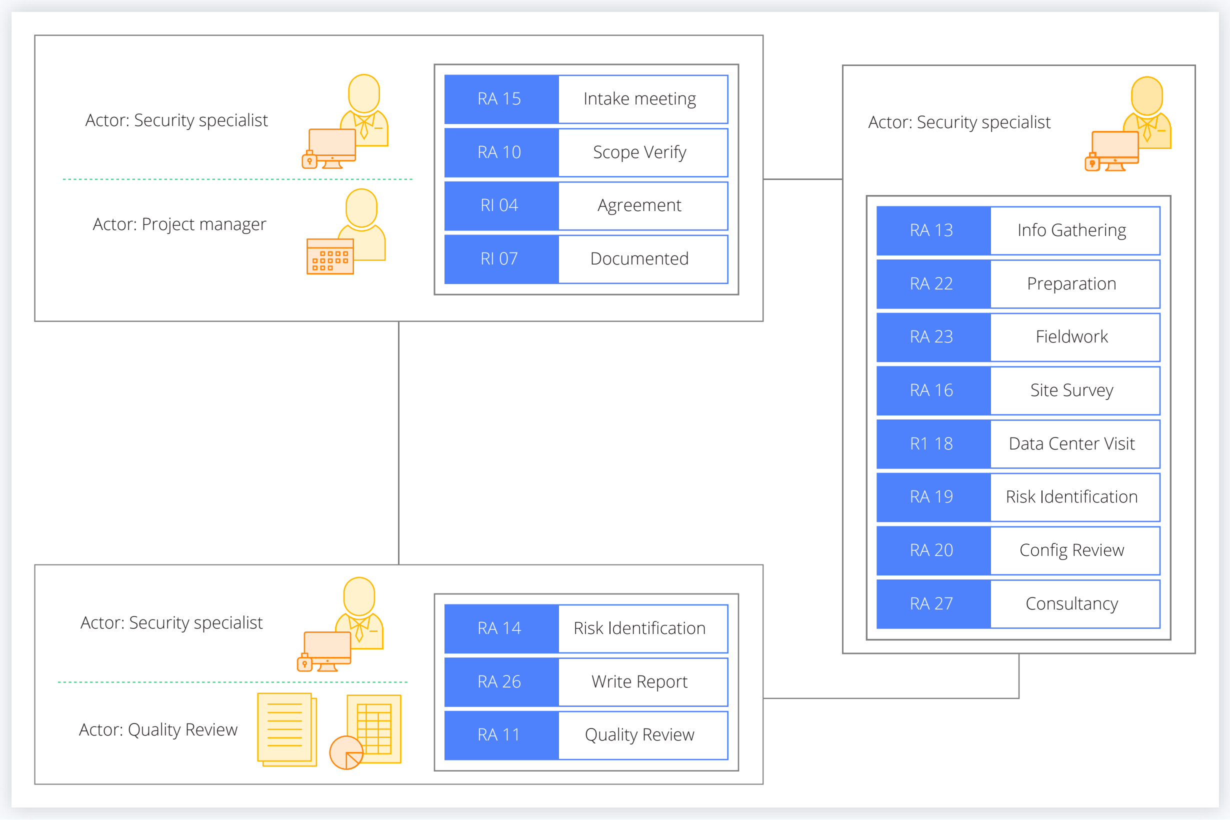


Figure 12 Pattern for Risk Assessment

WHAT HAPPENS AFTER GO-LIVE?

Risk Phase Shift

Does your organization keep track of all the changes that are happening in a critical SaaS application after approval and go-live? For example. An implementation of SaaS application that offers a suite of functionality to support ITIL processes. The first implementation starts with the Configuration Management Database (CMDB). No encryption and two factor authentication (2FA) are implemented at that time. In the two years after that additional SaaS modules are procured and implemented. Without going back to your cloud governing body for approval. Additional data sets are loaded. Additional user groups are added. Three years later this SaaS implementation is completely different than the one that was approved the first year. Encryption and 2FA are still missing. The overall risk rating has probably gone up from low to high or medium to high.

Even when your organization's security policy prescribes periodic review on compliance. It prescribes risk assessments for large IT changes. Yet all these SaaS modules changes stay under the radar. An octagon model specific to the topic of continuous monitoring might help to improve this situation.

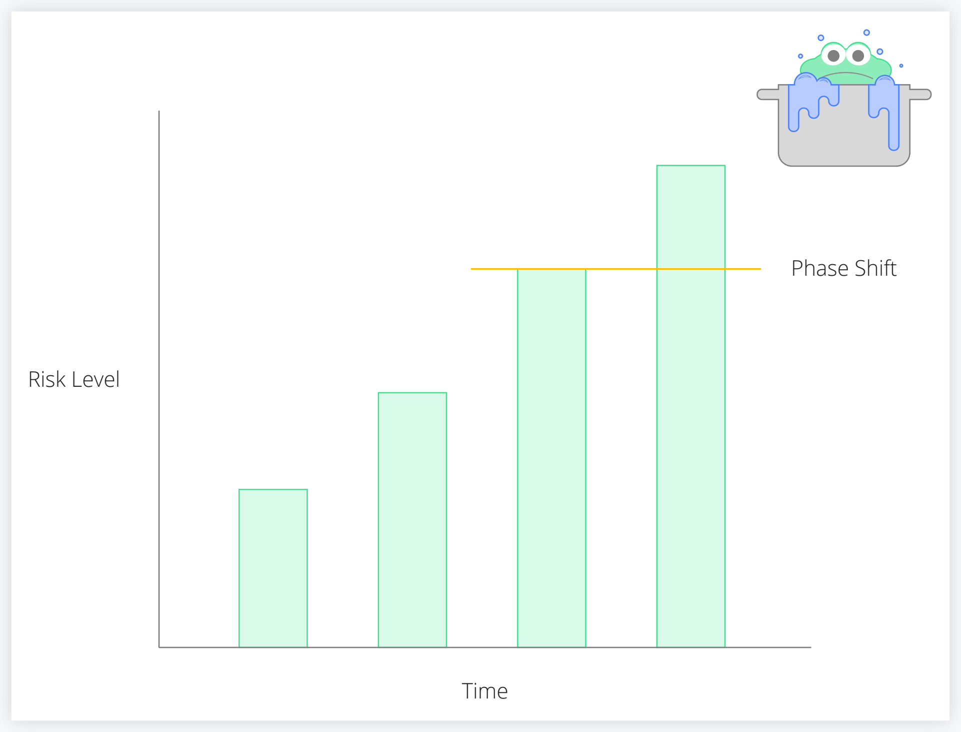
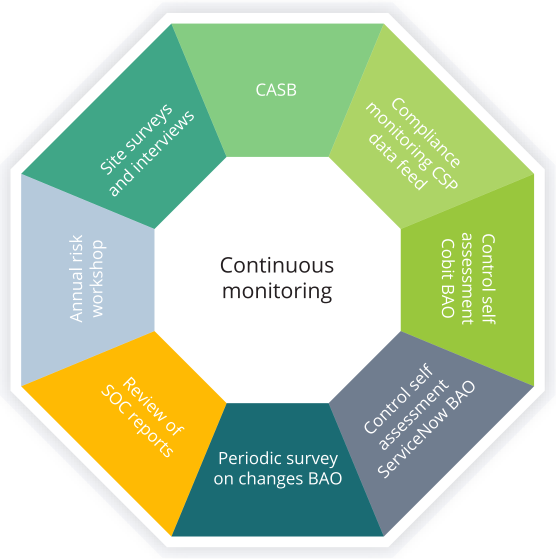


Figure 13 Risk Phase Shift

CONTINUOUS MONITORING


Continuous monitoring
CASB
Compliance monitoring CSP data feed
Control self assessment Cobit BAO
Control self assessment ServiceNow BAO
Periodic survey on changes BAO
Review of SOC reports
Annual risk workshop
Site surveys and interviews

Who looks after the risk following go-live of a cloud application? Annual review of SOC reports is recommended. Continuous auditing and monitoring are needed. Depending on the risk management framework (not part of octagon model) of the organization, there are a number of options for continuous monitoring. These can be technical or procedural.

Technical Monitoring

- With a Cloud Security Access Broker
- Monitoring cloud usage (security activity) with SIEM tooling (can be cloud native)
- Vulnerability detection
- Penetration testing

Procedural Monitoring

- Periodic review of (SOC) assurance reports
- Periodic risk assessment workshop with 2nd line experts
  - First line is IT security team, Second line is Information Security Risk Management, Operational Risk Management, Compliance etc. Third line is group audit.
- Security self-assessment by business application owner
- An audit by internal audit

The European Security Certification Framework (EU-SEC) strives to address the security, privacy and transparency challenges associated with the greater externalization of IT to cloud services. EU-SEC will create a certification framework under which existing certification and assurance schemes can co-exist. Furthermore, it will feature a tailored architecture and provide a set of tools to improve the efficiency and effectiveness of current assurance schemes targeting security, governance, risks management and compliance in the cloud. It will be tested and validated in pilots involving industrial partners.

https://www.sec-cert.eu/eu-sec/certification_framework

AWARENESS AND EDUCATION

Classroom Training and Certification

Working on cloud risk assessments requires a substantial amount of cloud knowledge. An organization’s core risk team should participate in training and certification like these:

CCSK™
Certificate of
Cloud Security Knowledge

CCSP™ Certified Cloud Security Professional

Arcitura®
the IT education company

AWARENESS GAME

In addition to structured education and certification programs, learning about cloud security while playing a game is a great way to get the message across.

One of the initiatives to raise awareness of cloud computing security among the 2nd line experts is to develop and produce a game board version of the octagon model. The game was developed with help from thegamemaster.nl. By playing the game, participants will learn what the relevant topics are to discuss during a risk workshop.

To play the game, the players choose one of the available cases, ranging from easy to hard. A roll of the dice takes the players to one of the octagon aspects. Every aspect has action cards from the Octagon Security Control Set. The players discuss all cards and by doing so learn about cloud computing risk and security. They choose the card that is the most relevant for the case they are working on. Every action card takes time to execute. After about one hour, between ten to fifteen action cards are chosen and it’s time to calculate the number of points, using the case solution description. When playing with one game board, the players who scores fifteen or more points wins; when playing with multiple boards, the team with the most points wins.

While playing the game and discussing the action cards (security controls), the team learns about the required depth of a risk assessment and in what areas something extra needs to be done in order to improve completeness and accuracy.

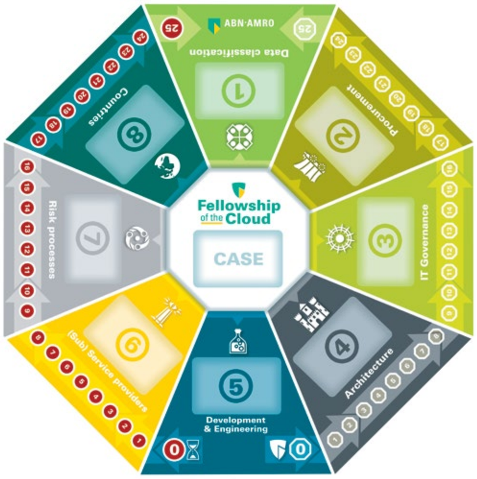


Figure 16 Awareness Game Board Layout

Figure 17 Awareness Game Box Design

REFERENCES AND CREDITS

References

Naydenov, R., Liveri, D., Dupre, L., Chalvatzi, E., (2015). Secure Use of Cloud Computing in the Finance Sector. European Union Agency For Network And Information Security Gartner Says by 2020 "Cloud Shift" Will Affect More Than $1 Trillion in IT Spending - http://www.gartner.com/newsroom/id/3384720

Credits

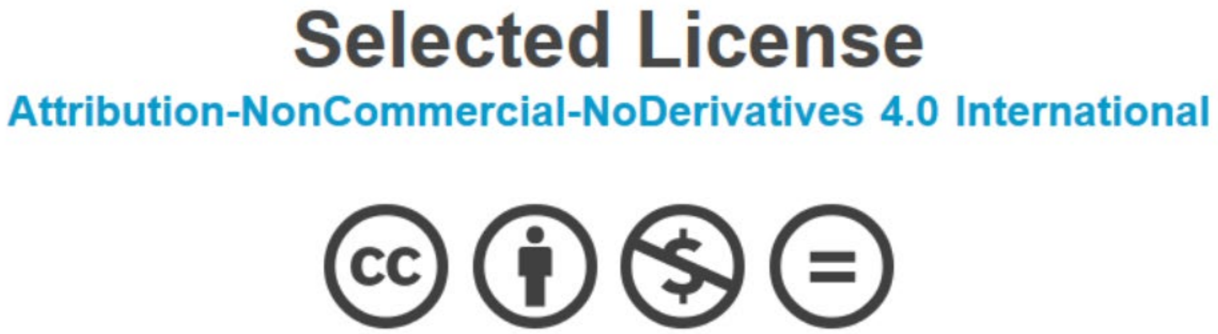
This whitepaper is an outcome of an approach conceptualized and implemented by the Cloud Security Group within the Information Security Services department, Corporate Information Security Office (CISO), ABN AMRO Bank NV.

- Lead author
    - Jim de Haas
- Contributors from ABN AMRO
    - Cheyenne Seur
    - Alok Saxena
    - Biswajt Behera
    - Timo Muller

Peer reviewed by CSA Financial Services Stakeholder Platform members and CSA community. Special thanks to Brian D. Becker, Damir Savanovic, Michael Roza, Olivier Caleff, Steven Genders and Vince Campitelli.

OCTAGON MODEL CONTROL SET

This information is shared under this Creative Commons license



Data classification

Privacy Impact Assessment

Perform a Privacy Impact Assessment (PIA) using the tooling provided by the Privacy Office. When the impact score is high, please address the issues in a risk workshop.

Data Classification

Classify the data processed by your cloud application. Determine the possible impact on the aspects of Confidentiality, Integrity and Availability.

Data classification must be challenged

The draft CIA rating created by the business application owner must be challenged by 2nd line experts. This will improve the quality of the classification.

Data classification must be agreed upon

The CIA rating created by the business application owner must be agreed upon by 2nd line experts.

Data classification must be aligned

When the cloud application has interfaces with other applications, make sure that the CIA ratings of those applications are aligned. The requirements of the application with the highest CIA rating must be met.

Be aware of crown jewels applications.

Some applications have business impact critical, which is one level above high. Please be aware that these might not be visible in your data classification schema immediately. When your cloud is approved for critical data, does this mean it is also approved for so called crown jewels applications?

Countries

Model Clauses

Once you have identified the countries using, processing and hosting determine the need for using model clauses from a legal perspective.

Countries hosting

Determine in which countries the cloud application is hosted and what the possible consequences are from a legal, compliance, privacy, operational risk and or security perspective.

Countries processing

Determine in which countries the cloud application is processing data and what the possible consequences are from a legal, compliance, privacy, operational risk and or security perspective.

Cross border data transfers

Determine is any cross border data transfers occur and what the possible consequences are from a legal, compliance, privacy, operational risk and or security perspective.

Local Requirements

Once you have identified the countries using, processing and hosting determine what local requirements must be addressed from a legal, compliance, privacy, operational risk and or security perspective.

Procurement

Request for proposal

During the procurement phase of your cloud project discuss, negotiate and agree on the security requirements in scope.

Determine and agree on contract version

During the procurement phase of your cloud project discuss, negotiate and agree on which contract to sign.

Determine and agree on delivery agreement

During the procurement phase of your cloud project discuss, negotiate and agree on the details in a so called delivery agreement.

Determine and agree on Service Level Agreement

During the procurement phase of your cloud project discuss, negotiate and agree on the service level agreement.

Determine and agree on Data exit

During the procurement phase of your cloud project discuss, negotiate and agree on your data exit strategy, including a test plan for it.

Determine and agree on Subcontractors

During the procurement phase of your cloud project discuss, negotiate and agree on which subcontractors are used and how requirements are met in contracts.

Determine and agree on Country specific requirements

During the procurement phase of your cloud project discuss, negotiate and agree on any country specific requirements. For example in the area of incident reporting.

Determine and agree on Right to audit for your Organization

During the procurement phase of your cloud project discuss, negotiate and agree on the right to audit for your Organization.

Determine and agree on Right to examine for your regulator

During the procurement phase of your cloud project discuss, negotiate and agree on the right of examine for the regulator.

Level of Assurance

When critical data is processed, the highest level of assurance by the CSP must be offered. Review if the information provided is complete, recent and in line with your data classification. Pay extra attention to the topic of assurance during contract negotiations.

IT Governance

Cloud knowledge

You realise that performing a cloud computing risk assessment requires substantial cloud security knowledge. You decide to invest in education. Part of your team goes to general cloud security education, whereas others are attending more specialized training.

Portability

Make sure you meet requirements in the area of portability. This means you are able to migrate your application and data to a different provider. Your CSP must support or meet your requirements in this area. Please investigate as early as the RFP phase.

Cloud policy check

You Organization has a cloud security policy with a number of rules. For every policy rule, you verify compliance and document it. Non-compliance is addressed by further investigation, risk acceptance or risk mitigation.

Strategy for encryption

Your Organization has developed and published a strategy for encryption in the cloud. It covers things like allowed algorithms, bring your own key, key management and use of Hardware Security Modules.

Data leakage prevention

Ask the CSP to implement controls for data leakage prevention. Enabling timely detection or even prevention of data leakage by employees working at the SaaS provider.

Single Sing On

Ask the CSP to implement Single Sign for end users or internal staff. Enabling you to meet the architecture standards of your Organization.

Two-factor Authentication

Ask the CSP to implement two-factor authentication for application users, for systems where critical data is processed.

Web application firewall

Ask the CPS to implement a Web Application Firewall (WAF) using the best practice or ruleset from OWASP. A WAF protects the application against common attacks such as SQL injection.

IAM event monitoring

CSP must provide automatic, continuous, actual and real-time information on users and their access rights to Organizations Identity & Access Management. If this cannot be provided, all users and user privileges must be provisioned using Single Sign-On methods with ‘Federation’ as the preferred option.

Privacy breach reporting

The supplier must have systems in place to monitor for privacy breaches and notify tenants expeditiously if a privacy event may have impacted their data. Contract shall specify what constitutes a privacy breach.

Continuous monitoring

Does your organisation have a framework or methodology for continuous monitoring of cloud services after go live. Please look at this from the perspectives of procurement, vendor management and security.

Risk processes

Chain of Service Providers

Organisation shall take account of the risks associated with chain outsourcing where the outsourcing service provider subcontracts elements of the service to other providers. Outsourcing institution should agree to chain outsourcing only if the subcontractor will also fully comply with obligations existing between outsourcing institution and outsourcing service provider.

Trust Criteria Check

When reviewing a SOC audit report verify if the trust criteria in scope are aligned with the data classification. For any misaligned raise a risk.

Risk assessment information gathering

Gather information for a risk assessments and verify if relevant security requirements are met. Talk to Subject Matter Experts, review documentation and system configuration.

Risk Identification

For any security requirements that are not met a risk must be raised, taking mitigating controls and company context into account. Risk labeling is done using the Organizations risk rating procedure.

CSP Site Survey

In case the Cloud Service Provider (CSP) offers little assurance you might benefit from a site survey. During a site survey, you visit the main office of the provider and acquire information via interviews, demos and observations.

Security Consultancy

Offer security consultancy during all phases of the project, from RFP to implementation and continuous monitoring.

Application stack Configuration review

Perform a risk assessments by reviewing the configuration. See for yourself that security controls are implemented.

Security Requirements engineering

After determining the context of the cloud change select all relevant security requirements and present them to the project and the CSP.

Risk assessment preparation

Prepare your risk assessment by identifying the chain of service providers, identifying your major stakeholders, technology in scope, relevant security policies, standards and requirements.

Risk assessment fieldwork

Conduct the fieldwork for your risk assessment and over a period of time talk to subject matter experts. Validate any findings or observations by acquiring a second opinion on the matter. Check if the information provided covers all security requirements in scope.

Architecture

Architecture Intake

Perform an intake meeting with an architect of the domain where the cloud application is implemented. Discuss topics like reuse before buy before build. Determine the possible impact on your current application landscape and decide if there is a need for a detailed architecture design or definition document.

Architecture Cloud Brokerage

Perform an intake meeting with your Organisations cloud broker. Present your workload characteristics and determine which cloud offering best suits your needs. This is about your workload placement strategy

Architecture Integration Advice

Talk to your architects and explain your requirements in the area of integrating services like fraud monitoring, security monitoring, encryption and identity management.

Architecture Perimeter Security

Talk to your architects and discuss your requirements in the area of perimeter security. Familiarize yourself with the applicable policies and standards in this area.

Architecture Approved Design Documented

Make sure the formal approval of the architecture design document is documented.

Architecture Design Approved

Make sure the architecture definition document is approved in the right approval board, at the right level. Thus making sure that management supports the architecture choices made.

Central IT or not? Depending on your organization’s IT strategy you allow for local IT responsibility or not. Is your IaaS offering suitable for consumption by your foreign offices and daughter companies? Does the chosen architecture and setup support this? Please take into account different policy needs per tenant (business unit).

Alignment with Future State Architectures Are the IaaS PaaS features that you are approving and making available for your devops teams aligned with your architects Future State Architecture documents? Are they aligned with your strategy as well, in the area of portability for example.

Providers

Chain transparency

Before signing the contract the security team investigates the parties involved in the total chain of service providers. The assurance level offered per vendor is determined. Associated risks for any gaps are raised.

System integration

Cloud system and service management must be integrated into existing run and change processes. To ensure that Organization is in control of its systems and data IT must maintain an integrated view of all processes managing IT-solutions, including the cloud-solutions.

Site Survey data centre

During a site survey of a data centre you verify the physical security. You review the terrain and the building from roof to basement. Review is done from both a technical and procedural point of view.

Penetration testing

The SaaS application is tested for security vulnerabilities before every major release. The same applies for applications deployed on Organizations IaaS PaaS cloud. Findings from testing are included in an GRC or risk management application.

Sub-contractor risk assessment

The main cloud provider must perform annual risk assessments on their sub-contractors. Evidence of risk assessment and risk management must be available for the customers of the CSP.

Manage landscape complexity

When complex or large business processes are supported by a substantial SaaS landscape, it is key that the complexity of the landscape is managed. For example by putting one of the vendors in charge.

Security Monitoring

Your management team has requested that the SaaS service is monitored on continuous basis, by the corporate security team. Ask the CSP to provide an event log stream for this.

Development & Engineering

Devops team maturity

You development team needs a certain maturity level before it is allowed to deploy systems to production. Especially in the areas of security and ops work. Also, consider how to implement application support in the evenings and weekend, should your availability rating require so.

CI CD pipelines

Your devops teams must use the available Continuous Integration and Continuous Delivery pipelines and make sure they program in the languages that are supported by those pipelines. Part of the governance process is verifying that they do so. Secure coding verification is included in the pipeline.

Developer access

Developer access to systems is controlled and monitored. An Identity and Access Management architecture and design is created and implemented. Taking into account requirements in the areas of segregation of duty.

Infrastructure as code

All cloud stacks must be created, deployed and changed via infrastructure as code templates. Devops teams go to training for Cloudformation and or ARM templates.

Secure coding

Secure coding is key to security. Code quality is verified by the devops teams themselves. The process is fully automated. Devops teams are trained in secure coding. There is a Center of Expertise secure coding established.

Secrets management

Devops teams must manage credentials, API keys and other secrets through their lifecycle. From creation to rotation. Additional software for secrets management is used.

Shared Responsibility Model

Responsibilities in an IaaS PaaS cloud are divided between the provider, the cloud resource administrator and the devops team. For every service, the responsibilities for the devops team are described. This is done for both Run and Change.

Monitoring for security compliance

What kind of monitoring dashboards are available for your devops teams? Is the data quality of these dashboards sufficient? Is the ops team taking its responsibility for becoming and staying compliant?