Master Thesis Economics & Informatics

Identity and access management in a cloud computing environment

---

Author:
Edwin Sturrus
294763

Supervisors:
Ing. A. A. C. de Visser RE (Erasmus University Rotterdam)
Prof. dr. ir. U. Kaymak (Erasmus University Rotterdam)
Drs. W. S. Chung RE (KPMG IT Advisory)
Ir. ing. J.J.C. Steevens RE (KPMG IT Advisory)

Econometric Institute
Erasmus School of Economics
Erasmus University Rotterdam
4 August 2011

Abstract

Over the past couple of years cloud computing has rapidly grown to a widely accepted IT model. A vast majority of decision makers of organisations in The Netherlands state that cloud computing is the future model of IT. However, security and the trust factor of cloud computing are obstacles for organisations to use cloud computing.

With the growing amount of data and users and stricter rules for organisations for data storage, IAM has become more important. When using cloud computing, data is no longer stored within the organisations owning the data. The current state of IAM does not provide sufficient possibilities to manage this. In this research the differences, risks and controls of IAM in a cloud computing environment are researched.

Acknowledgements

In this chapter I would like to thank everyone that made this thesis possible.

First of all, I would like to thank my girlfriend Sylvia and my parents for keeping me on track at times I lost motivation.

I would like to thank my supervisor Ad de Visser for his efforts in guiding me through this research project. And I would also like to thank everyone else at the Erasmus University Rotterdam who contributed to this thesis.

I would like to thank Mike Chung and Jules Steevens for their efforts and assistance as my supervisors of KPMG. And I would also like to thank my colleagues of the ISC team of KPMG IT Advisory for their help and guidance during my internship.

I would like to thank my interviewees; Arnout Kaaij, Willem de Pater, Sasa Radosevic and Andres Steijaert for sharing their knowledge.

Last but not least, I would like to thank all of my friends and everyone else who supported me throughout these six months of research.

Contents

List of figures

List of tables

1. General introduction

This chapter describes the general introduction of this research. It contains the introduction and relevance of the research subjects, the theoretical background, the research design and structure, the scope of research and the research methodology.

1.1. Introduction

Over the past couple of years cloud computing has rapidly grown from web-based e-mail applications like Hotmail, to software suites like the CRM suite Salesforce.com and the office suite Microsoft Office 365 (Hotmail, 1996) (Salesforce.com, 1999) (Microsoft Office 365, 2011). According to a survey by Chung and Hermans, the view of a vast majority of decision makers of organisations in The Netherlands is that cloud computing is the future model of IT (Chung & Hermans, 2010). According to Birman, Chockler and van Renesse, cloud computing poses very interesting research questions and opportunities (Birman, Chockler, & van Renesse, 2009). Besides that according to Boroujerdi and Nazem: “Cloud Computing reduces both software and hardware maintenance cost.” (Boroujerdi & Nazem, 2009). Organisations using cloud computing can reduce capital expenditure. The cost of hardware, software and services are billed on a utility or subscription bases.

“Although cloud computing offers great user convenience by freeing users from the need to understand processing details, it forces them to trust the cloud service provider (CSP), which worries many users.” (Okuhara, Shiozaki, & Suzuki, 2010).

“Security is the main obstacle for many organisations in their move to the cloud.”(Chung & Hermans, 2010).

Examining previous research, clarifies that cloud computing is a growing phenomenon that provides interesting opportunities for organisations as well as for research purposes. Besides that, security and the trust factor of cloud computing are major obstacles for organisations to use cloud computing. Robust identity and access management (IAM) is one of the requirements to minimise the security concerns of cloud computing (Gopalakrishnan, 2009). With the growing amount of data, users and roles at modern organisations, controlling access to data has become increasingly important. Besides that, the rules and regulations for data storage of organisations have become stricter in recent years (Harauz, Kaufman, & Potter, 2009). This part of security management within originations is relevant for cloud computing. The growing popularity of external data processing and storage raises numerous challenges for organisations that want to extend access governance policies beyond their organisation's firewalls into the cloud, especially for outsourced data management and outsourced services (Ponemon, 2010). When using cloud computing, part of the organisation’s data is no longer stored on devices managed by the organisations owning the data. This increases the risks of unauthorised access and changes the way user management can be performed. Cloud computing has a number of new dimensions that the current state of IAM does not meet (Gopalakrishnan, 2009). These recent developments make the combination of IAM for cloud computing an interesting subject to research. In this research the differences, risks and controls of IAM in a cloud computing environment are researched.

1.2. Theoretical background

1.2.1. Identity and access management

IAM is all about the management of access of identities to data. According to Jøsang and Pope: "An identity is a representation of an entity in a specific application domain." (Jøsang & Pope, 2005). Identities are linked to a set of characteristics that define them within the specific application domain. Examples of characteristics, also called identifiers, are name, date of birth or account id (Günsberg, 2009). An entity can have one or multiple identities within a specific application domain and each identity can have multiple identifiers and must have at least one unique identifier within the specific application domain (Jøsang & Pope, 2005). This unique identifier allows an identity to be recognised (Figure 1).

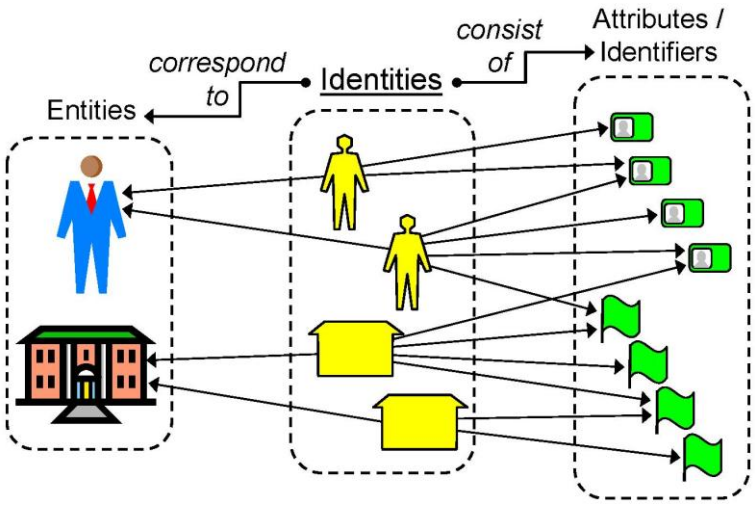

Figure 1: Correspondence between entities, identities and identifiers (Jøsang & Pope, 2005).

According to Lily Bi, IAM is the process of managing who has access to what information and for how long (Bi, 2008). According to Hermans and ter Hart, IAM is the management, processes and supporting system that manages which users (persons, applications and systems) get access to information, IT resources and physical resources and what each user is authorised to do with these resources (Hermans & ter Hart, 2005). The definition of IAM used in this research is based on the two definitions above in relation to the scope of this research (Section 1.4). For this research the following definition of IAM is used.

"The processes and technologies that manage the access of identities to digital resources and what authorisation identities have over these resources."

To get a better overview of IAM, IAM can be divided into several parts. This research uses a model by Mather, Kumaraswamy and Latif (Figure 2).

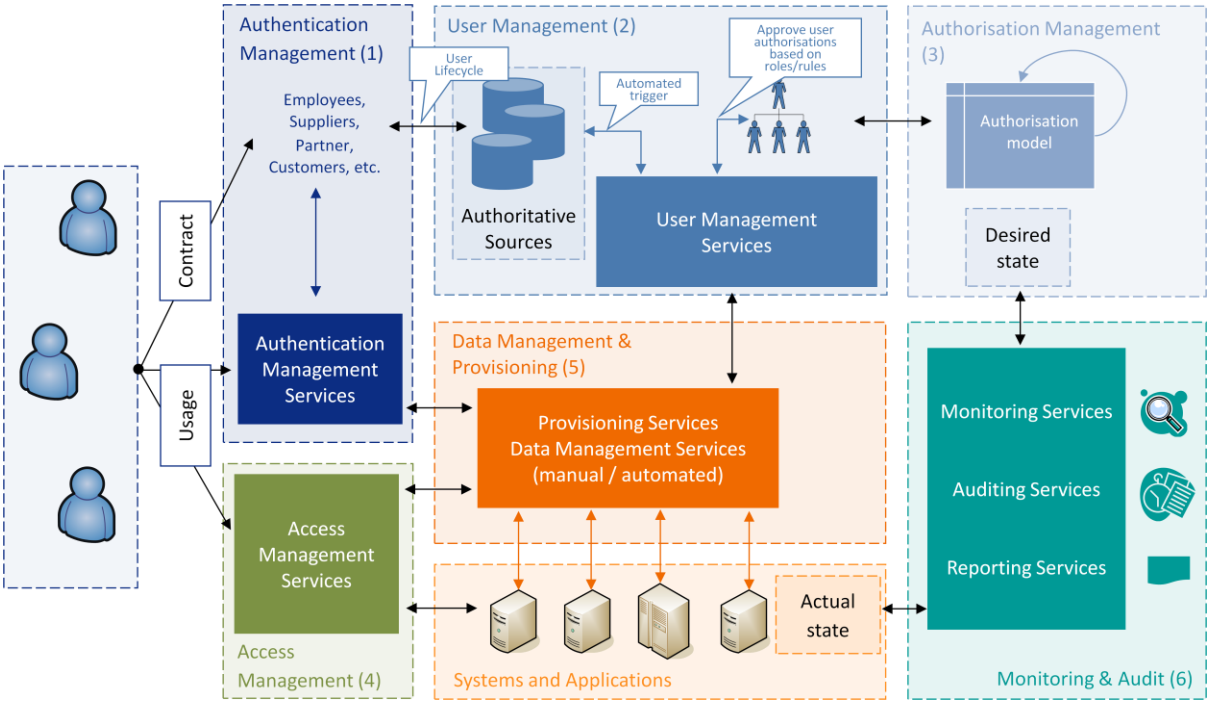

Figure 2: Enterprise IAM functional architecture (Mather, Kumaraswamy, & Latif, 2009).

The following definitions of the different parts of the model by Mather, Kumaraswamy and Latif are used (Figure 2).

- **Authentication management:** Activities for the effective governance and management of the process ensuring that an entity is who or what he claims to be.
- **User management:** Activities for the effective governance and management of identity life cycles.
- **Authorisation management:** Activities for the effective governance and management of the process for determining entitlement rights that decide what resources an entity is permitted to access in accordance with the organisation's policies.
- **Access management:** Enforcement of organisation's policies for access control in response to a request from an entity wanting to access a resource within the organisation.
- **Data management and provisioning:** Management and propagation of identity and data for authorisation to resources.
- **Monitoring and auditing:** Activities for monitoring, auditing and reporting compliance by users regarding access to resources within the organisation based on the organisation's policies.

1.2.2. Cloud computing

For this research the definition by Mell and Grance of the National Institute of Science and Technology is used. Although there is still discussion on maintaining a strict definition of cloud computing, this definition is the most accepted definition in research and organisations in recent years. The definition of cloud computing used in this research is:

"Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources that can be rapidly provisioned and released with minimal management effort or service provider interaction."(Mell & Grance, 2011).

To get a better overview of cloud computing, the model of Mell and Grance is used (Figure 3).

Figure 3: Delivery and deployment models of cloud computing (Mell & Grance, 2011).

The following definitions of the deployment models of the model by Mell and Grance are used (Figure 3).

- **Private cloud:** The cloud infrastructure is operated solely for an organisation. It may be managed by the organisation or a third party. And it may exist either at the infrastructure of the organisation using the cloud services (on-premise) or at the infrastructure of the organisation selling the cloud services (off-premise).
- **Community cloud:** The cloud infrastructure is shared by several organisations and supports a specific community that has shared concerns. It may be managed by the organisations or a third party and may exist on premise or off premise.
- **Public cloud:** The cloud infrastructure is made available to the general public or a large industry group and is owned by an organisation selling cloud services. Multiple users and organisations are using the cloud services from the infrastructure of an organisation selling the cloud services.
- **Hybrid cloud:** The cloud infrastructure is a composition of two or more clouds that remain unique entities but are bound together by standardized or proprietary technology that enables data and application portability.

The following definitions of the delivery models of the model by Mell and Grance are used (Figure 3).

- **Software as a service (SaaS):** The capability provided to the consumer is to use the provider's applications running on a cloud infrastructure. The applications are accessible from various client devices through a thin client interface such as a web browser. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, storage, or even individual application capabilities, with the possible exception of limited user-specific application configuration settings.
- **Platform as a service (PaaS):** The capability provided to the consumer is to deploy onto the cloud infrastructure consumer-created or acquired applications created using programming languages and tools supported by the provider. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, or storage, but has control over the deployed applications and possibly application hosting environment configurations.

- **Infrastructure as a service (IaaS):** The capability provided to the consumer is to provision processing, storage, networks, and other fundamental computing resources where the consumer is able to deploy and run arbitrary software, which can include operating systems and applications. The consumer does not manage or control the underlying cloud infrastructure but has control over operating systems, storage, deployed applications, and possibly limited control of select networking components.

1.3.Research question

Combining the research relevance described in the introduction with the topics described in the technological background; a research objective is defined (Section 1.1) (Section 1.2). The research objective is an overview of the effects of cloud computing on the risks and controls of the processes of IAM.

Using this research objective, a research question is defined. The main research question of this research is:

What are the specific risks and controls of IAM processes in a cloud computing environment?

In order to answer the main research question, the research question is divided into multiple research questions listed below.

- What are the different IAM processes in a traditional IT environment?
- What are the different IAM architectures in a cloud computing environment?
- What are the differences and risks of the IAM processes in a cloud computing environment compared to a traditional IT environment?
- What are the controls to mitigate these risks?

The first research question serves as a general overview of the different processes of IAM in a traditional environment. The second research question serves as an overview of the different IAM architectures in a cloud computing environment. The third research question compares the IAM processes in a cloud computing environment to a traditional IT environment. The fourth research question provides an overview of how these risks of IAM in a cloud computing environment can be controlled. The answers to the above research questions provide the answer to the main research question.

1.4.Scope of research

Both IAM and cloud computing are large subjects. In order to answer the main research question and complete the research objective within the constraints and limitations of this research, this has a pre-defined scope. In this research not all technologies and processes of both cloud computing and IAM are researched.

For scoping IAM, this research uses the model described in the technical background of IAM (Paragraph 1.2.1). The technologies involved in these processes are reviewed on an architectural level. The technologies are not compared on their technical details, but on their general use within the model.

For scoping cloud computing, this research uses the model described in the technical background of cloud computing (Paragraph 1.2.2). According to a survey by Chung and Hermans, SaaS is the most used delivery model of cloud computing and the private cloud (hosted on-premise) the least used deployment model (Chung & Hermans, 2010). The hybrid cloud and community cloud are both deployment levels that combine multiple private and/or public clouds, which makes these deployment levels difficult to research and test (Mell & Grance, 2011). According to research, SaaS is the most interesting delivery model for a wide variety of cloud computing users (Vaquero, Rodero-Merino, Caceres, & Lindner, 2008). Therefore, within the model of Mell and Grance, this research concentrates on the public cloud for the deployment model and on SaaS for the service model (Mell & Grance, 2011). These models are graphically modified to show the scope of this research (Figure 4).

Figure 4: Scope of research (cloud computing).

In the introduction the relevance of IAM in a cloud computing for organisations is described (Section 1.1). Therefore, this research is taken from the point of view of organisations that use or want to use SaaS applications within their organisation. The data is gathered using literature study, interviews and business cases. This research focuses on organisations that are or are trying to manage the identity and access for SaaS applications. This research is limited to the demand for SaaS of organisations; the risks and controls for IAM used by vendors of SaaS are not within the scope of this research.

1.5.Methodology

This research is performed by using qualitative research methods. The research is based on the study of data gathered from scientific literature and expert interviews. The scientific literature is used to research the theory on cloud computing and IAM. The interviews are used to test the application of the theory of cloud computing and IAM in practice.

This research uses a phased approach, the research questions are answered in the pre-defined order (Section 1.3). First, the IAM processes for a traditional IT environment are recognised. Second, the different IAM architectures in a cloud computing environment are recognised. Third, the differences in IAM processes in a cloud computing environment are researched. Interviews and literature study is used to recognise the differences in IAM processes in a cloud computing environment.

These differences are researched for flaws and weaknesses, called the risks (Stoneburger, Goguen, & Feringa, 2002). Interviews and literature study and analyses are used to identify all risks. A modified model of KPMG for cloud computing risks is used to structure the risk research (KPMG, 2010). This model recognises the following business risk dimensions: financial, vendor, regulatory and compliance, data, operational and technology (Figure 5).

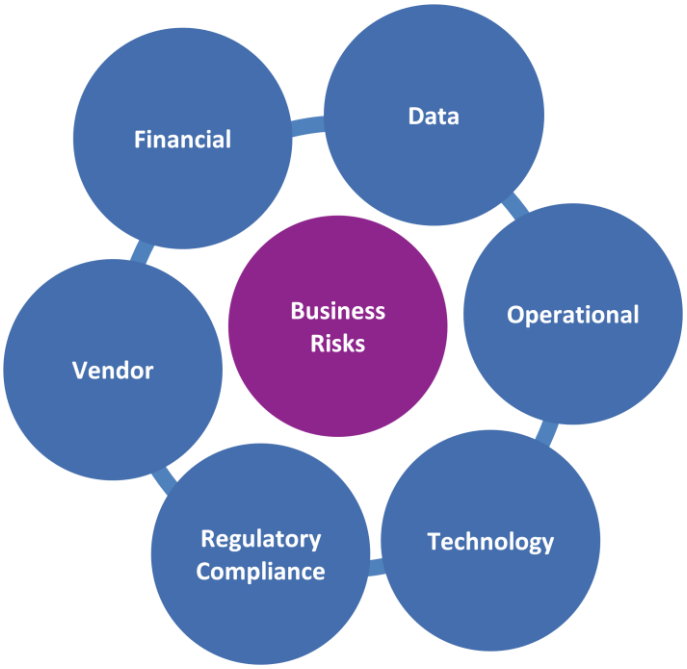

Figure 5: Cloud computing risk dimensions (KPMG, 2010).

This research uses the risk dimensions of this model that are directly applicable to cloud computing and IAM. Financial risks and vendor risks in this model are not directly related to both subjects. Although Vendors risks may affect organisations that are using cloud computing, it is not an IAM risk. Besides that, financial risks are applicable to IAM and cloud computing, but only as an indirect risk caused by other risks. Therefore these two risk dimensions are not taken into account for this research.

The following risk dimensions are researched for IAM in a cloud computing environment: law and regulation, data, technology and operational. Law and regulation risks include all the laws and regulations applicable to the organisation and compliance to them. Data risks include all the security policies and requirements in place to secure the data of the organisation. Technology risks include all risks related to the changes in technology for IAM in a cloud computing environment. Operational risks include all risks associated to the operational management of the organisation.

In order to eliminate, minimize or mitigate the risks, controls can be taken in place or are in place. In order to identify controls for the recognised risks, the COBIT framework is used (ISACA, 2007). COBIT is a widely accepted framework for IT governance and control. Alternatives such as ISO27001 and SAS70 are too detailed for this research and have a less suitable domain structure (NEN, 2005) (AICPA, 1992). The COSO framework does not have its focus on IT, which also makes it less suitable for this research (COSO, 2004).

The four domains of COBIT are “plan and organise”, “acquire and implement”, “deliver and support” and “monitor” (Figure 6). These domains, combined literature study and interviews are used to identify possible controls for each of the recognised risks (Stoneburger, Goguen, & Feringa, 2002).

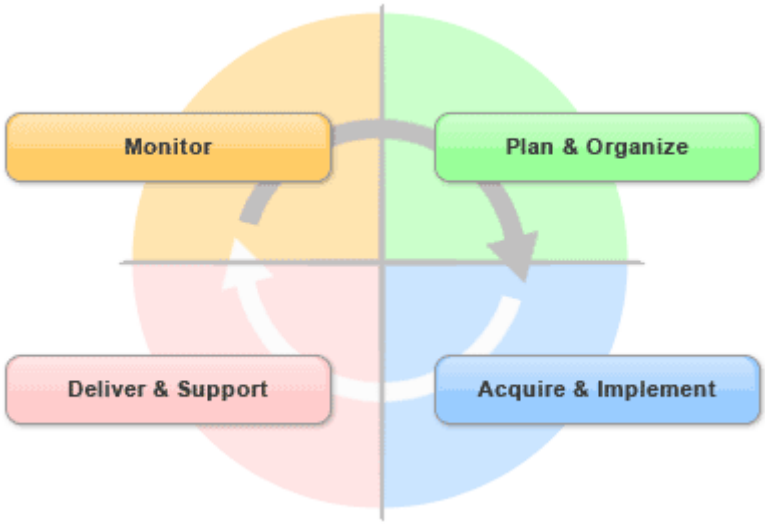

Figure 6: COBIT domains (ISACA, 2007).

The interviews for this research are interviews consisting neutral and open questions. For this research the following categories of relevant interviewees are pre-defined below.

- Architect of an organisation consuming cloud computing.
- Architect of an organisation delivering IAM solutions.
- Architect of an organisation delivering SaaS applications.

At least one interview with an interviewee of each category is required for this research.

The results of this research are tested using cross-validation. In this research the combination of the two research methods (literature study and interviews) and multiple scientific sources are used to perform cross-validation (Shank, 2005). Cross-validation is validating the results of research or answers to a research questions using multiple sources. If multiple sources provide the same answer or same result to the same research question it increases the likelihood of the correctness of the result or answer.

1.6.Research structure

In the second chapter of this research a general overview of the different processes of IAM in a traditional IT environment. In the third chapter the different IAM architectures are examined. In the fourth chapter the differences and risks of IAM processes in a cloud computing environment are compared to a traditional IT environment. In the fifth chapter provides an overview of how these risks of IAM in a cloud computing environment can be controlled. In the final chapter the research provides the answer to the main research question in the conclusions. The last pages of this research contain the used bibliography, figures and tables.

1.7.Summary

In the last couple of years cloud computing has grown to a widely used model of IT and poses very interesting research opportunities (Chung & Hermans, 2010) (Birman, Chockler, & van Renesse, 2009). However, according to research, security and trust limits the growth of cloud computing for organisations (Okuhara, Shiozaki, & Suzuki, 2010). With the growing amount of data and users and stricter rules for organisations for data storage IAM has become more important (Witty, Allan, Enck, & Wagner, 2003). When using cloud computing, data is no longer stored within the organisations owning the data. The current state of IAM does not provide sufficient possibilities to manage this (Gopalakrishnan, 2009). In this research the effects of cloud computing on the risks and controls of the processes of IAM are examined and suggestions for improvements to a current model of IAM are researched (Section 1.2).

The main research question of this research is: “What are the specific risks and controls of IAM processes in a cloud computing environment?” (Section 1.3).

In this research the following definitions are used for the two main subjects. “IAM is processes and technologies that manage the access of identities to digital and physical resources and what authorisation identities have over these resources.” (Paragraph 1.2.1). “Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources that can be rapidly provisioned and released with minimal management effort or service provider interaction.”(Mell & Grance, 2011).

This research focuses on organisations that are or are trying to manage the identity and access for SaaS applications (Section 1.4). This research uses qualitative research methods to collect, analyse data (Section 1.5).

In the second chapter of this research a general overview of the different processes of IAM. In the next chapters the IAM processes in a cloud computing environment are compared to a traditional IT environment, the changes in risks are analysed and controls are suggested (Section 1.6).

2. IAM processes in a traditional IT environment

This chapter describes the IAM processes of an organisation with a traditional IT environment. The IAM architecture is defined as well as the main IAM processes in practice.

2.1.IAM architecture for a traditional IT environment

For this research the IAM architecture for a traditional IT environment within an organisation is defined. IAM architecture for organisations encompasses several layers of technology, services and processes. At the core of the deployment architecture is a directory service. The directory service is a repository for identities, credentials and user attributes and it interacts with all IAM services (Mather, Kumaraswamy, & Latif, 2009) (KPMG, 2007). The user data store (UDS) feeds the directory service with user data. The UDS can for example be the database of HR within the organisation. Microsoft Active Directory is an example of a directory service (Microsoft Active Directory, 2000). In practice, a user connects to a directory service and after the authentication the user gets the applicable resources provisioned according to his authorisations (Figure 7).

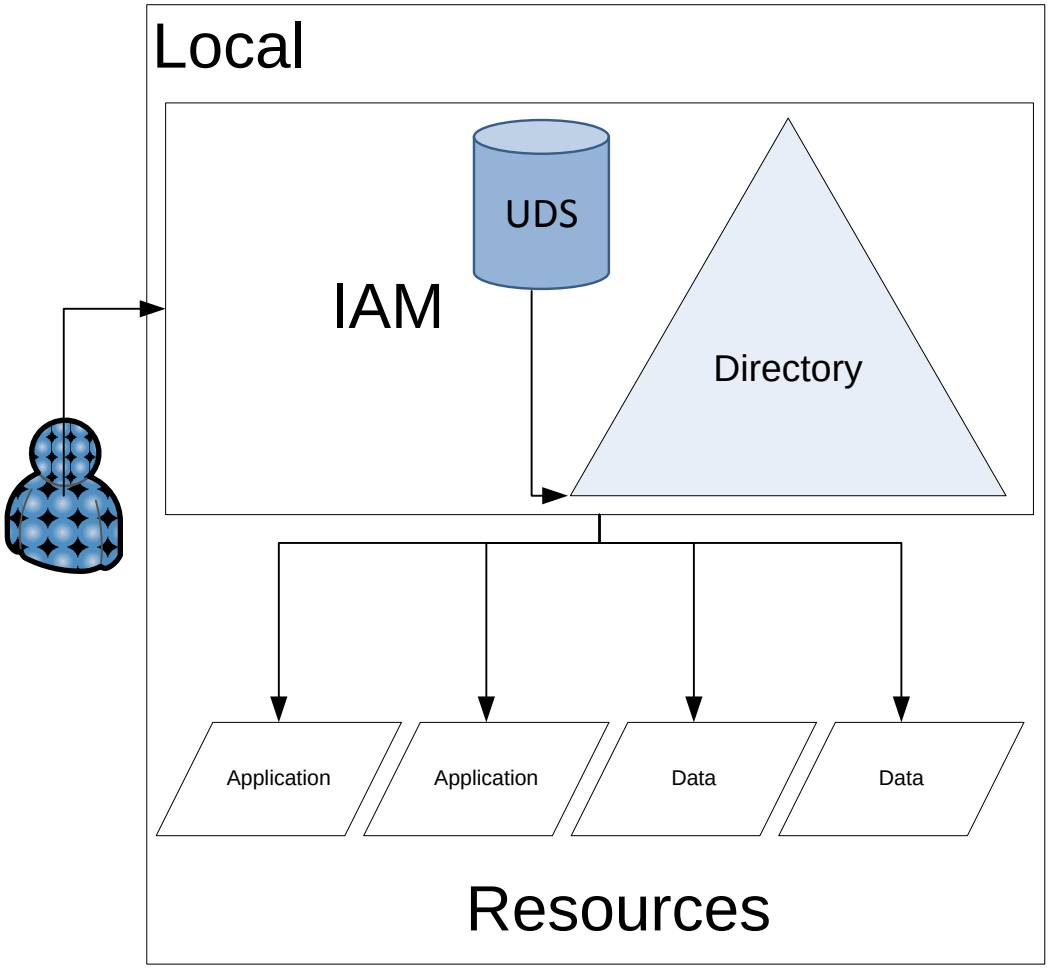

Figure 7: IAM architecture in a traditional IT environment.

2.2.Identity management processes

For managing users and identities a couple of processes are defined (KPMG, 2007). All use-cases apply to the model described previously (Paragraph 1.2.1). The use-cases apply to the same situation (Figure 8). The processes are projected on the pre-defined IAM parts (Figure 2).

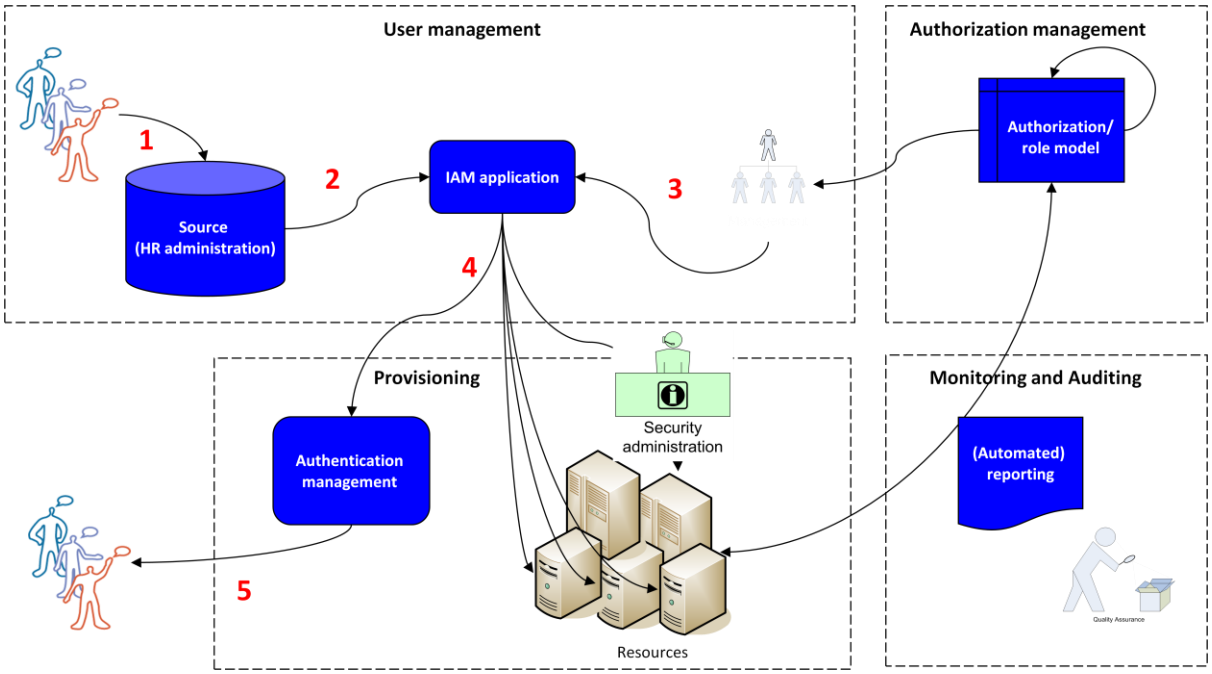

Figure 8: Identity management use-cases.

2.2.1. New employee

When a new employee joins the organisation, he or she requires an account, a role with authorisations and an authentication device. In order to provision the employee with an account, a role and an authentication device the following processes take place.

1 HR administrates new employee to the UDS
2 An automated trigger initiates the role assigning process
3 A manager assigns a role
4 User account and authorisations following the role are created
5 An authentication device is provided to the user

2.2.2. Job rotation

When an employee changes his job, his or her account is modified, role and authorisations are changed and authentication device is updated. In order to provision the employee with a modified account, appropriate authorisations and updated authentication device the following processes take place.

1 HR changes the job of the employee in the UDS
2 An automated trigger initiates the role assigning process
3 A manager assigns a role
4 User account and authorisations following the role are changed
5 A new or modified authentication device is provided to the user

2.2.3. Dismissal of an employee

When an employee leaves the organisation, his or her account is removed, role and authorisations are unassigned and authentication device are withdrawn. In order to remove the account, unassign the role and withdrawn the authentication device the following processes take place.

1 HR dismisses the employee from the UDS
2 An automated trigger initiates the role unassigning process
3 A manager unassigns the role
4 User account and authorisations are dismissed
5 The authentication device is withdrawn from the user

2.3.Access management processes

For managing access of users to resources a couple of processes are defined (KPMG, 2007). All use-cases apply to the model described previously (Paragraph 1.2.1). The use-cases apply to the same situation (Figure 9). The processes are projected on the pre-defined IAM parts (Figure 2).

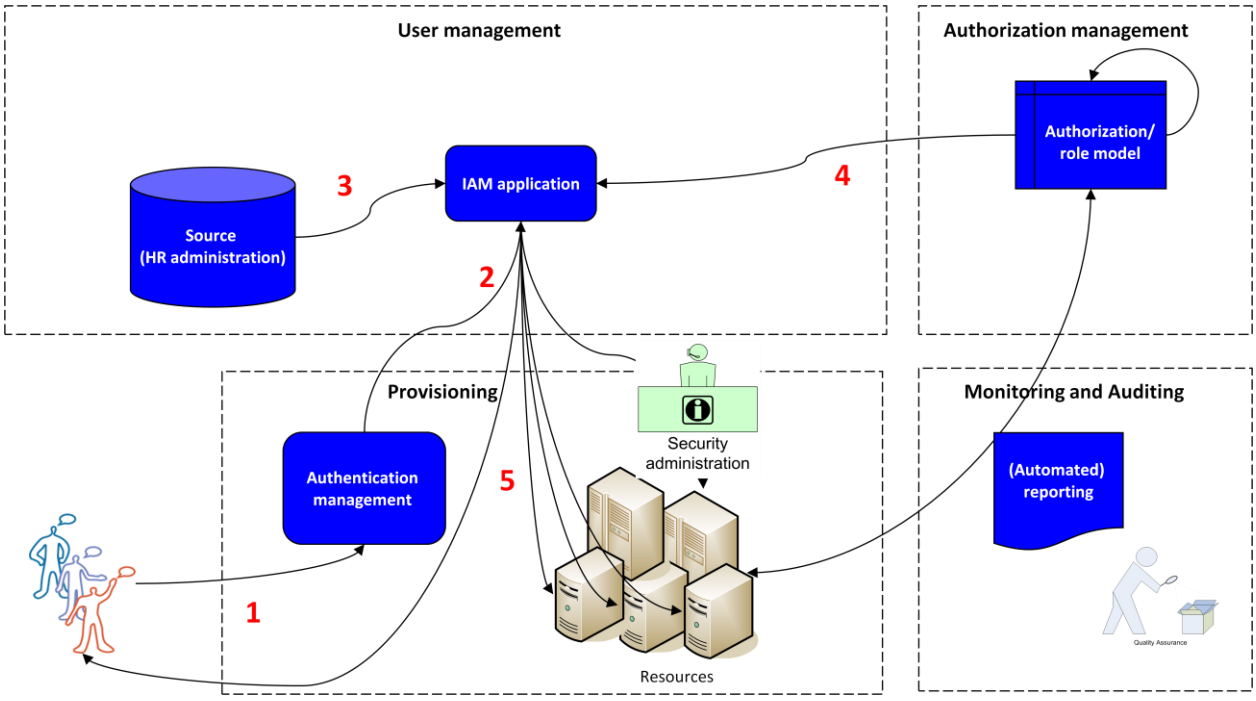

Figure 9: Access management use-cases.

2.3.1. User access to resources

When an employee attempts to access resources within an organisation, the employee has to prove that he or she is who he or she claims to be. If the identity of the employee is validated correct, the authorisations of the employee are validated for access rights to the resource. If the employee has the right role and authorisations to be allowed access to the resource, the requested resource is provisioned. If the validation of identity or authorisation fails, the employee receives an error message. In order to provide the employee access to the requested resource, the following processes take place.

- User attempts to access resources, provides it's credentials
- An automated trigger initiates the access management process
- The user credentials are verified in the UDS
- The user authorisations for the resource are verified
- The user gets the resources provisioned or get an error message

2.4.Summary

In this chapter the IAM architecture of a traditional IT environment is defined (Figure 7). IAM encompasses several layers of technology, services and processes. In the core of the IAM architecture is a directory service, a repository for identities, credentials and user attributes.

The defined identity management processes are: adding a new employee, job rotation of an employee and dismissal of an employee. Besides that there is an access management process that allows or denies users access to resources. These four processes are used in the next chapters to research in a cloud computing environment.

3. Different IAM architectures in a cloud computing environment

This chapter describes the different IAM architectures in a cloud computing environment compared to a traditional IT environment.

3.1. Cloud computing environment

In this chapter the IAM architecture for a cloud computing environment within an organisation is researched. The main difference with a traditional IT environment is that a part of the resources is provided by the CSP (Figure 7). In the cloud computing environment an organisation can have one or multiple resources provided by a CSP or multiple CSP's.

A single cloud computing environment for IAM cannot be defined. There are several options to manage identities and access in a cloud computing environment. According to research of Blakley; the identity can be brought to the cloud, the identity can be in the cloud or the identity can be delivered from the cloud (Blakley, 2009). In other words, when the user attempts to access a resource, the user can provide his identity to a CSP, the user can store his identity in the UDS of a CSP or the user has his identity provided by a CSP (Figure 10) (Figure 11) (Figure 12).

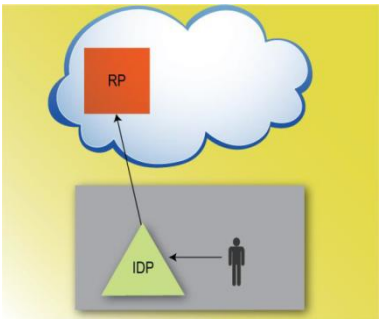

Figure 10: Identity to the cloud (Blakley, 2009).

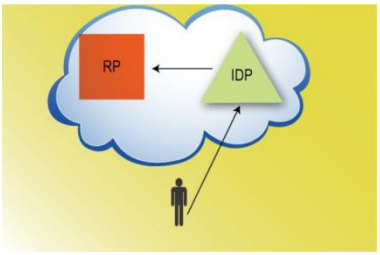

Figure 11: Identity in the cloud (Blakley, 2009).

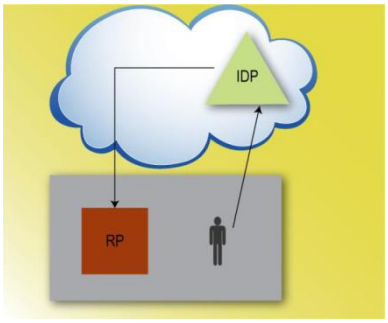

Figure 12: Identity from the cloud (Blakley, 2009).

According to research of Goulding et. al; IAM can be up to the cloud, inside the cloud or delivered from the cloud (Goulding, Broberg, & Gardiner, 2010). In other words, local IAM can be connected to the cloud, IAM can be taken care of by the CSP or IAM can be delivered as a service from the cloud (Figure 13) (Figure 14) (Figure 15).

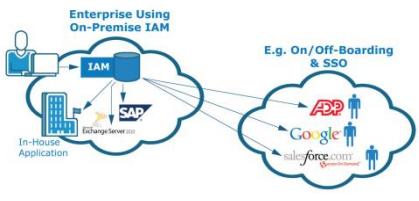

Figure 13: IAM up to the cloud (Goulding, Broberg, & Gardiner, 2010).

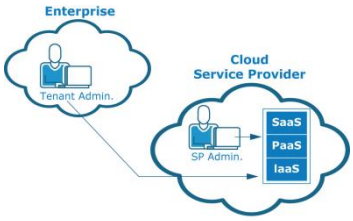

Figure 14: IAM inside the cloud (Goulding, Broberg, & Gardiner, 2010).

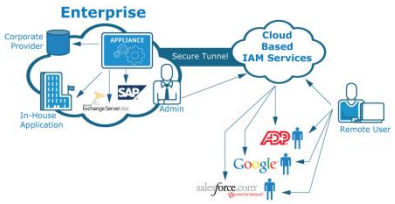

Figure 15: IAM delivered from the cloud (Goulding, Broberg, & Gardiner, 2010).

According to research of Huang et. al; identity federation should be used to manage identities and access in a cloud environment (Huang, Wang, Liu, & Xu, 2010). According to research of Cser et. al and Frank Villavicencio IAM; IAM can be delivered as a service to manage a cloud environment (Cser, Balaouras, & Hayes, 2010) (Villavicencio, 2010).

There is some overlap in the cloud computing environments for IAM that are researched. IAM delivered as a service from the cloud is similar to the identity in the cloud model of Bob Blakley and the IAM delivered from the cloud of J. Tony Goulding et. al. Another similarity can be noticed in the identity up to the cloud environment of Bob Blakley and the IAM up to the cloud environment of J. Tony Goulding et. al. This research recognises four models to manage IAM in a cloud computing environment suitable for the scope of this research: A traditional model, trust relationship model, identity service provider model and all in the cloud model. These models are validated in the interviews as well. In the following sections the models are described in detail.

3.2.Traditional model

In the traditional model the organisation hosts, manages and controls its own on-premise IAM covering all IAM processes. Users can access the local resources, such as data and applications using local authentication. The users are stored in a UDS, for example the human resources (HR) database, which feeds a directory (Figure 16). For accessing cloud computing resources, a separate account is created in the directory of the CSP for each authorized user. For all CSP's a separate account for each user must be created.

When an employee enters the organisation, gets a role change or leaves the organisation, an additional action to add or remove the identity to the CSP is required. There are software packages on the market to automatically propagate user accounts and changes to the CSP's, for example Oracle Identity Manager (OIM) (de Pater, 2011). OIM allows an organisation to automatically create user accounts at the UDS of the CSP's, were the new employee requires access to. This is done by using standard or custom-made connectors based on the API's of the CSP's. Besides that, single sign-on (SSO) services can be used to lower the amount of identities a user owns. SSO allows users to use a single identity to authenticate for multiple services.

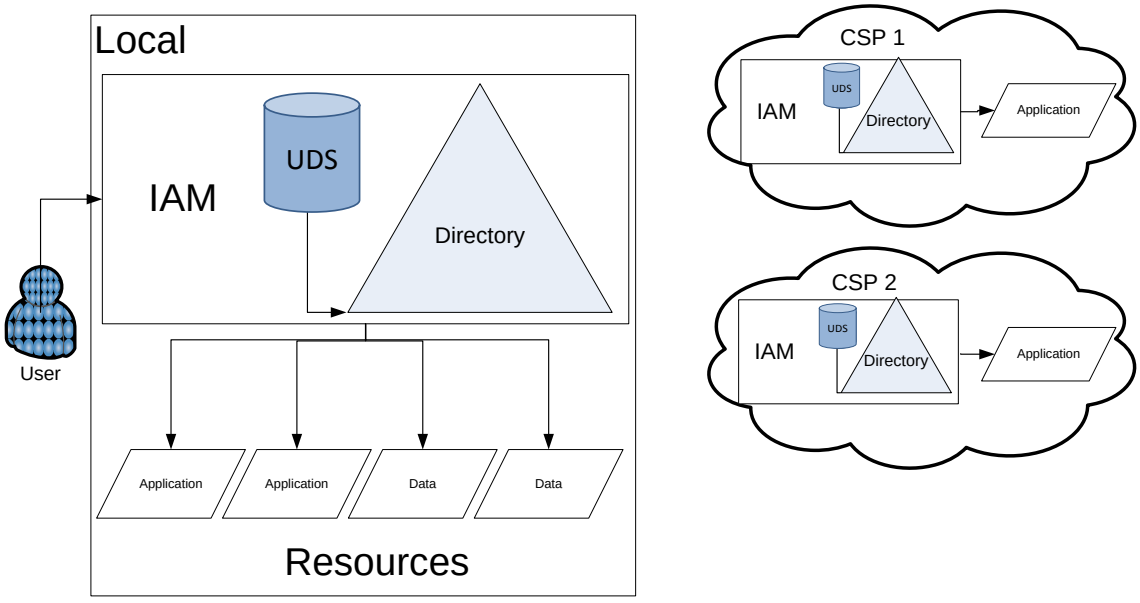

Figure 16: Traditional model for cloud computing environment.

Ahold, an international supermarket organisation, uses the traditional model to manage e-mail and calendar services from the cloud (Kaaij, 2011). Ahold decided to switch Lotus Notes e-mail and calendar applications for the cloud services of Google, Google Mail and Google Calendar, in 2010 (Google Apps, 2006).

3.3.Trusted relationship model

In the trusted relationship model the organisation hosts, manages and controls its on-premise IAM software which covers all IAM processes. Users can access the on-premise resources, such as data and software using local authentication. The users are stored in the UDS which feeds the local directory (Figure 17). When a part of the organisations' resources moves to the cloud, both parties establish a trusted relationship on both of their IAM systems and processes.

When a user is authenticated within the local on-premise IAM system it can use on-premise as well as off-premise resources, such as cloud services, according to his authorizations. The CSP trusts the IAM of its client and allows its users to access the offered services. For each different CSP a separate trusted relationship is established. Account duplication is not needed in this model; the local IAM solutions are synchronized. In this model, the organisation may continue to utilize its existing methods for enforcing access control over user access activities.

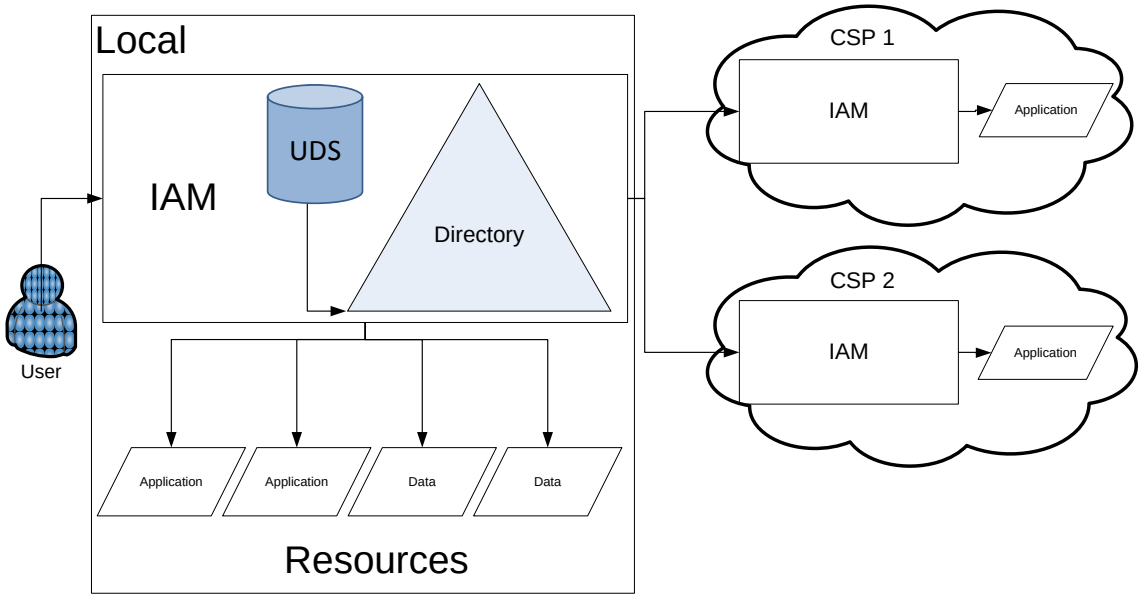

Figure 17: Trusted relationship model for cloud computing environment.

3.4.Identity service provider model

In the identity service provider model the organisation hosts, manages and controls its on-premise IAM software which covers all IAM processes. Users can access the on-premise resources, such as data and software using local authentication. The users are stored in a UDS which feeds the local directory (Figure 18).

When a part of the organisations' resources moves to the cloud, an identity service provider (IdSP) is introduced. An IdSP is a provider of identity services, such as authentication of a user. Examples of organisations that provide identity services are DigiD, FaceBook or SURFnet. SURFfederatie is an authentication and authorisation service from SURFnet (Steijaert, 2011). It allows the verification of an identity. SURFfederatie is used by 160 organisations in The Netherlands and has over one million users. SURFfederatie is focussed on organisations in the education branch. In practice the CSP and organisation using the cloud service both have a trust relationship with SURFnet. When a user attempts to access the cloud resource, SURFnet verifies the identity of the user with the UDS of its organisation.

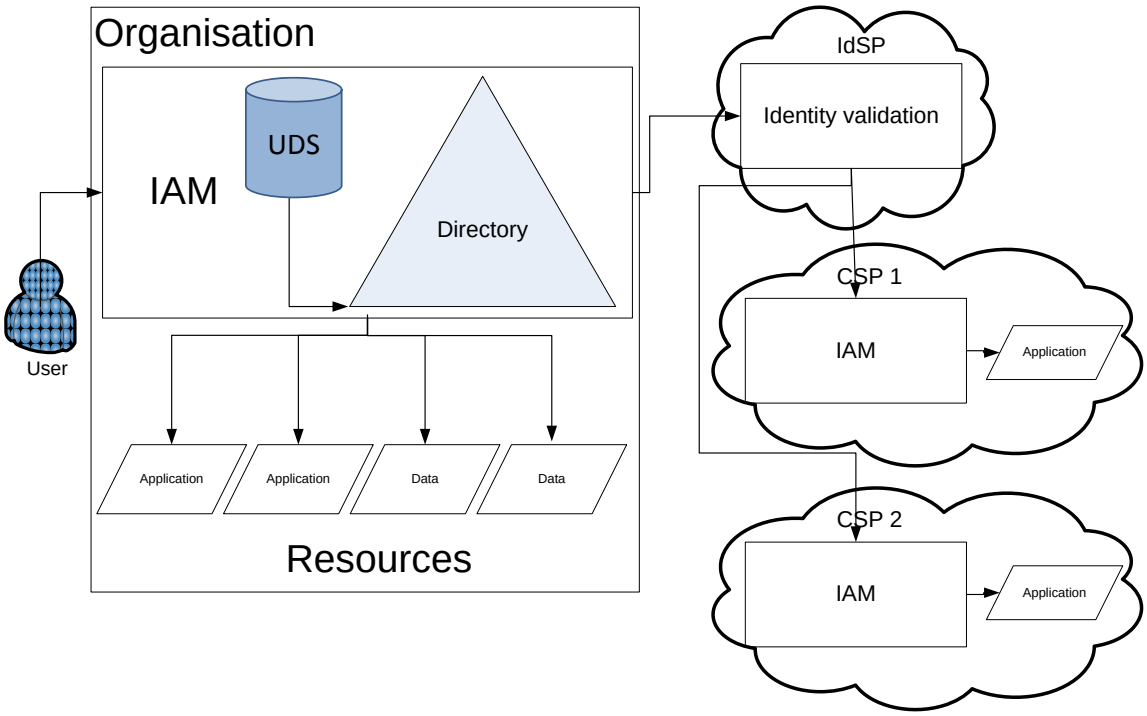

Figure 18: Identity service provider model for cloud computing environment.

There are software packages available to combine the local IAM software with an IdSP, an example is Microsoft Active Directory Federation Services (Radosevic, 2011). Microsoft Active Directory Federation Services is able to use an IdSP within the authentication processes. This IdSP is used to verify the identity of the user trying to access a resource.

3.5.All in the cloud model

In the all in the cloud model the organisation fully delegates the IAM system and processes to a CSP. The CSP delivers IAM as a service to the organisation. In this model, there is no local IAM or directory in place. The CSP fully hosts and manages the IAM of the consuming organisation. The CSP stores the users in a UDS, authenticates users, and authorizes authenticated users to resources (Figure 19). Users authenticate with the cloud IAM service to access on-premise as well as off-premise resources. Monitoring and audit are the responsibility of the provider of IAM services. However, the organisation using the IAM service remains accountable.

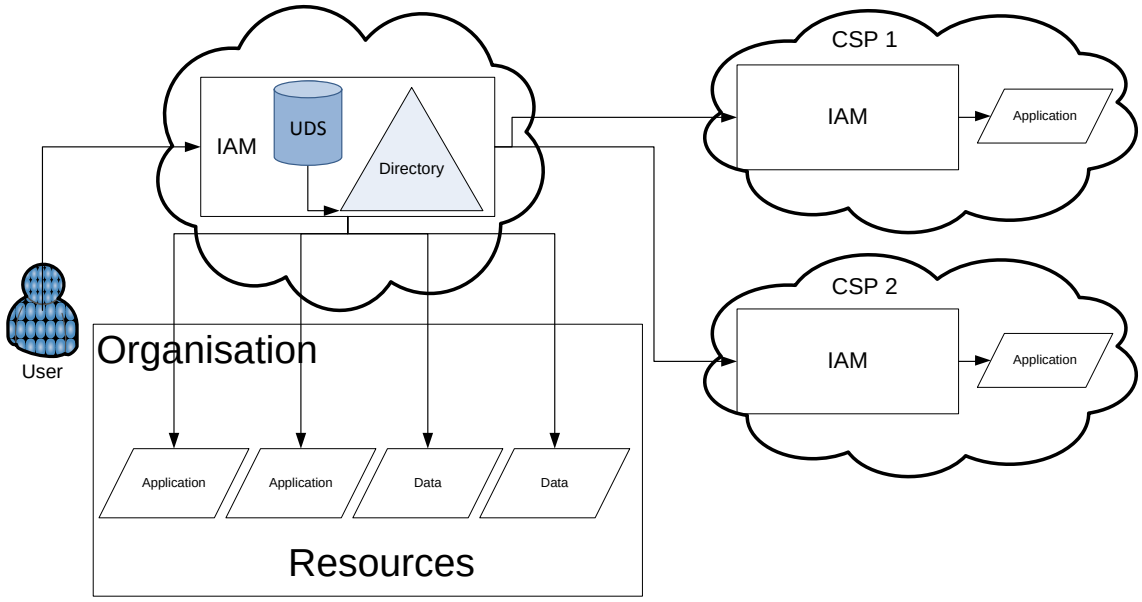

Figure 19: All in the cloud model for cloud computing environment.

According to Gregg Kreizman, the market of organisations offering IAM as a service remains small and volatile (Kreizman, 2011). Currently there are no signs of a large scale adaptation (de Pater, 2011) (Radosevic, 2011). However, on a smaller scale there are organisations entering this market. CloudID is an example of an organisation delivering cloud IAM services (CloudID, 2010).

3.6.Summary

In this chapter the different architectures for using IAM in a cloud computing environment are researched. The first option is the traditional model. In this model the organisation manages his own on-premise IAM processes and connects them to the CSP. All users have to be added to, changed in or removed from the UDS of the CSP or CSP's providing the cloud services. In the trusted relationship model, the CSP trust and uses the IAM of the organisation using the cloud services. The users are stored in the UDS of their organisation and can connect to the cloud services using local authentication. In the identity service provider model, a third party is introduced to validate the identity of a user. Users are stored in the UDS of their organisation and when connection to a cloud service the IdSP validates the identity of the user. In the all in the cloud model the organisation fully delegates IAM to a CSP. Users use the cloud IAM service to access on-premise as well as off-premise services. In the following table an overview of the differences between the models is provided (Table 1).

	Traditional model	Trusted relation-ship model	Identity service provider model	All in the cloud model
Location of the UDS	On-premise and off-premise	On-premise	On-premise	Off-premise
Account duplication	Yes	No	No	No
Location of authentication	On-premise and off-premise	On-premise	On-premise and off-premise	Off-premise
Level of control of IAM	High	Medium	Medium	Low

Table 1: Differences between IAM models for a cloud computing environment.

In the next chapter the changes and risks of IAM processes in a cloud computing environment are researched.

4. IAM processes in a cloud computing environment

In this chapter the changes and risks of the parts of IAM in a cloud computing environment compared to traditional IT environment are researched.

4.1. Changes to IAM

In the traditional IT environment, users have to be added, changed or removed from a system and these users can access their authorised resources (Chapter 2). The general processes of adding, changing or removing an employee do not change in a cloud computing environment. Users still must be added to a system to be able to access resources. Even if this system is located at a CSP, the users must be recognised by the system in order to access its authorised resources. Simple said, the record of the employee still changes in a HR system, a manager still assigns or dismisses a role and the authentication device is still provided to or retracted from the employee. However, depending on the model chosen, parts of IAM are not managed by the organisation itself (Chapter 3). The same applies to access management. A user still has to provide the authentication device and is granted or denied access to the requested resources on the authorisations. However, for each model chosen, parts of IAM are not managed by the organisation itself (Chapter 3).

Even if the IAM processes or parts of the IAM processes are not managed, the organisation is always accountable for their IAM processes (Jansen & Grance, 2011). Therefore it is essential to know which organisation controls (parts) of the IAM processes. In the following sections the changes and risks per part of IAM are examined. The IAM model, described previously, is used to define the different parts of IAM (Paragraph 1.2.1). For all these parts of IAM the, previously described, cloud computing models are compared to the traditional IT environment (Section 2.1) (Chapter 3). The differences are examined in the amount of control (low, medium or high) that an organisation has over that specific part of IAM using a specific cloud computing model. The more control the organisation has over its IAM the less impact a risk has and the easier it can be mitigated. For example, if the organisation uses on-premise authentication to access its resources it can easily modify the authentication mechanisms if they are insecure. However, if the organisation uses off-premise authentication the organisation is not in control of changes made to the authentication mechanisms. After examining the differences for each cloud computing model compared to the traditional IT environment, the risks are examined. The following risk dimensions are researched: Laws and Regulation, Data, Technology and Operational (Section 1.5). The risks are researched for each part of IAM. The impact of the risk is dependent on whether the organisation using the cloud services or the CSP owns a specific part of IAM. If the organisation is the owner of a part of IAM, its level of control is higher and the impact of the risk is lower. If the CSP is the owner of a part of IAM, the level of control of the organisation using the cloud services is lower and the impact of the risk is higher.

4.2. Authentication management

Authentication management is one of the key parts of IAM that are frequently not managed by the organisation that uses cloud services. Looking at the previously described models, authentication mostly takes place in the cloud (Chapter 3). Most CSP's use their own authentication mechanism for user to access the cloud services. Examples of cloud services using their own authentication mechanisms are SalesForce, Microsoft Office 365 and Google Apps (Salesforce.com, 1999)(Microsoft Office 365, 2011) (Google Apps, 2006).

In the traditional model the authentication generally takes place at the CSP. For example in the case of Ahold, when a user attempts to access Google Apps from outside the Ahold network by using the internet, the authentication takes place at the website of Google (Kaaij, 2011) (Google Apps, 2006). The trusted relationship model is an exception in this matter and does allow users to use local authentication to gain access to the cloud services. However, this is a more a theoretical option. Local authentication forces the user to make a connection to the organisation, before being able to access the cloud services. This reduces the flexibility, since the user cannot access the cloud service without connecting to the organisation first. In the identity service provider model, authentication can take place at the IdSP or the CSP, in both scenarios the organisation using the cloud services is not in control of the authentication process. In the all in the cloud model authentication management, as well as all other parts of IAM, are completely off-premise and in the cloud. Therefore the organisation using cloud services is not in control of authentication management.

	Level of control
Traditional model	Low
Trusted relationship model	High
Identity service provider model	Medium
All in the cloud model	Low

Table 2: Level of control of authentication management.

Not being in control of authentication management can introduce multiple risks for the organisation. First of all, the organisation may have to comply with certain security regulations such as the ISO 27002 standard (NEN, 2007). If the authentication mechanisms of the CSP do not comply with certain standards, the organisation using the cloud services might not be able to comply to their applicable standards either. Besides the laws and regulations, the organisations may have certain requirements for data storage in place. These specific security requirements for authentication can be different than those of the CSP, for example password strength and password storage. If the CSP does not meet the required security level for authentication, data theft or loss can become a risk to the organisation (Chang & Choi, 2011). Other possibilities are technology risks for authentication management. Authentication mechanisms of the CSP can be different than the organisation using the cloud services. Ahold had the issue that the authentication website of Google allowed users to stay logged in after closing a browser session (Kaaij, 2011) (Google Apps, 2006). The standard Google Apps authentication website has this option available, this problem is solved (Figure 20) (Figure 21).

Figure 20: Google Apps old situation (Kaaij, 2011).

Figure 21: Google Apps new situation (Kaaij, 2011).

Besides that, the local SSO may use different standards than the CSP; incompatibility can be a risk as well as a general inconvenience for usability. Last but not least, if the CSP has control of authentication, it can change the authentication mechanisms and requirements. The organisation using the cloud service is not in control of these changes, which is a risk for the organisation. For example, the CSP could decide to change the password policy to something less secure than the requirements of the organisation. To sum it up, the following risks are applicable to authentication management for the different models of a cloud computing environment (Table 3).

Law and regulation risks • Noncompliance with security regulations
Data risks • Data theft or loss due to different security requirements for authentication
Technology risks • Incompatible authentication mechanisms • Incompatible SSO
Operational risks • Unable to manage changes to authentication mechanisms

Table 3: Authentication management risks.

4.3.User management

After analysing user management processes in a cloud computing environment the following changes are discovered. In a traditional IT environment users are modified by the organisation itself within their local UDS. In a cloud computing environment the users can be modified, depending on the model that is used, in the UDS of the CSP. In the traditional model the organisation has to add, change and remove users within the UDS of the CSP. In the trust relationship model this difference is not applicable, since the CSP makes uses of the organisation's local UDS. In the identity service provider model the users are authenticated by the IdSP using the organisation's local UDS, the users do not have to be stored in the UDS of the CSP. In the all in the cloud model, the users are stored in the UDS of the CSP providing the IAM services. In the traditional model and all in the cloud model, the users are stored outside the organisation; this leaves the control in the hands of the CSP and not the organisation owning the data. The main difference for user management when using cloud services is the loss of control over the UDS, containing user information.

	Level of control
Traditional model	Low
Trusted relationship model	High
Identity service provider model	High
All in the cloud model	Low

Table 4: Level of control of user management.

Not being in control of all user data makes it difficult to comply with local laws and regulations for personal information (Wet Bescherming Persoonsgegevens, 2000). In case the CSP is located in a region with different laws and regulations in place, the organisation might not comply with the local laws and regulations. An example is that in some regions the law prohibits the transportation of personal information to other countries.

Another risk to the organisation is the possibility of different requirements for data security, which can result in a data breach. If the synchronisation of user data is insecure, confidential or personal information can be read or even modified by unauthorised users (Huynh, 2011). Incompatible technology can be another risk to the organisation. If the CSP does not support the mechanisms to store and update user data that the organisation uses, the service will be difficult to deploy (de Pater, 2011). Besides that, not being in control of user management makes it very difficult to verify if an update to the user data is successful. For example, whether or not dismissing an employee results in a successful removal of this employee in the UDS of the CSP. It is essential that both directories stay synchronised, to ensure that only authorised users have access to the cloud services. Last but not least, the organisation using the cloud services has no control over the changes made to user management by the CSP. For example, the CSP can decide to store users differently, which can make it incompatible and/or incompliant with the organisation using the cloud services, but also much more difficult to maintain (de Pater, 2011). To sum it up, the following risks are applicable to user management in a cloud computing environment (Table 5).

Law and regulation risks • Noncompliance with local laws and regulations for personal information
Data risks • Loss or theft of user data due to incompatible data security requirements
Technology risks • Incompatible technology to update or store user data
Operational risks • Unable to verify successful update of UDS • No control over changes made to user management by CSP

Table 5: User management risks.

4.4.Authorisation management

In all of cloud architectures described in the previous chapter, the organisation using the cloud services decides to which resources the users have authorisations for (Chapter 3). However, the main difference for authorisation management when using cloud services, are the differences in authorisation models of both CSP and the organisation using the cloud services. For example, if the organisation has implemented a role-based access control (RBAC) model to manage authorisations and the CSP does not support this, it is difficult to synchronise authorisations of users (Chang & Choi, 2011).

	Level of control
Traditional model	High
Trusted relationship model	High
Identity service provider model	High
All in the cloud model	High

Table 6: Level of control of authorisation management.

Not being able to synchronise the authorisations of users, makes it impossible to ensure that users only access the authorised resources and perform the authorised actions on them. For example, user can have access to a cloud based service to view his monthly salary. However, the user may not see salaries of other employees. His manager is allowed to see the salaries of other employees; the CSP has to be able to manage these authorisations the same way as the organisation using the cloud service. Incorrect authorisation management can lead to incompliance with laws and regulations.

For example, unauthorised access to personal information of people can conflict with the applicable laws (Wet Bescherming Persoonsgegevens, 2000). Besides that, the security requirements for data cannot be met if data is accessed, removed or modified unauthorised. Another risk to the organisation is that it cannot manually check the authorisations for errors at the CSP. The organisations using the cloud service is ultimately accountable for the authorisations of its users, but the CSP has control, or at least partly control, over the processes involved. Last but not least, the organisation using the cloud services is unable to verify if the authorisations of its users is properly followed by the CSP. To sum it up, the following risks are applicable to authorisation management in a cloud computing environment (Table 7).

Law and regulation risks • Noncompliance with laws and regulations if the authorisations cannot be synchronised
Data risks • Unauthorised data modifications if the authorisation cannot be synchronised
Technology risks
Operational risks • Unable to verify the authorisations for errors • Unable to verify successful execution of authorisations

Table 7: Authorisation management risks.

4.5.Access management

In all of cloud architectures described in the previous chapter, the main different for access management is that the organisation using the cloud services is not in control of the enforcement of their security policies for the services of the CSP (Chapter 3). The CSP ultimately controls the access to their services. Besides that, in order to access to public cloud services an Internet connection instead of a local network connection is used. Managing the local network is a lot easier than managing the Internet, since the local network they are fully managed by the organisation itself. The Internet is a public network that can be accessed by anyone with any compatible device.

	Level of control
Traditional model	Low
Trusted relationship model	Low
Identity service provider model	Low
All in the cloud model	Low

Table 8: Level of control of access management.

The combination of loss of control over access management and the cloud service being accessed over a public network, proposes a couple of risks to the organisation using the cloud services. First of all, if data is not adequately protected, anyone using the Internet can access the data of the organisation using the cloud services. This data can be protected by laws or regulations, which would make the organisation incompliant. For example, personal information of humans is protected by law (Wet Bescherming Persoonsgegevens, 2000). Besides access over the Internet, the data of the organisation using the cloud services is hosted at the servers of the CSP. If the data is not adequately protected, the hardware containing the data can be physically stolen (Jansen & Grance, 2011).

Another risk is the dependency of the Internet, if the connections to the CSP fails, the cloud services can no longer be accessed by the organisation. Last but not least, the fact that data is not stored and managed by the organisation using the cloud services makes it very difficult to verify who has or had access to this data. To sum it up, the following risks are applicable to access management in a cloud computing environment (Table 9).

Law and regulation risks • Virtual as well as physical access to data protected by laws or regulations
Data risks • Virtual as well as physical access to organisation's data in general
Technology risks • Failure of an Internet connection stops access to the cloud services
Operational risks • Unable to verify who has or had access to data

Table 9: Access management risks.

4.6. Data management and provisioning

There are a couple of differences in data management and provisioning in a cloud computing environment. In the traditional model and all in the cloud model, user accounts have to be provisioned and deprovisioned at UDS of the CSP (Chapter 3). In the trust relationship model and identity service provider model the users remain stored in the local UDS of the organisation using the cloud services, provisioning and deprovisioning is controlled by the organisation itself. In all IAM architectures in a cloud computing environment data of the organisation using the cloud services is stored at the servers of the CSP. The organisation using the cloud services is not in control of this data.

	Level of control
Traditional model	Low
Trusted relationship model	Medium
Identity service provider model	Medium
All in the cloud model	Low

Table 10: Level of control of authentication management.

The provisioning and deprovisioning of user accounts has to be performed fast and properly. The risk of using incompatible technologies or incorrect deprovisioning is that unauthorised users can keep access to the cloud services after dismissal. This can make the organisation using the cloud services incompliant with laws and regulations and put the data at risk of being stolen or lost. Besides that, data stored in a cloud environment is no longer managed by the organisation owning the data. Requirements for removal and encryption might not be implemented according to the security standards and regulations (Carlin & Curran, 2011). For example, confidential e-mail requires to be securely removed. The organisation is unable to verify if this process takes place and if the e-mail is not backed up or stored elsewhere in the network. Same applies to encryption, if data requires certain encryption strength, the organisation owning the data cannot verify if the CSP uses this encryption on the data, especially if it is backed up or spread among multiple servers.

The risk of incorrect data management is the loss of data or unauthorised access to the data of the organisation using the cloud service (Huynh, 2011). Besides that, some data has to stay in the country of origin in order to comply with local laws and regulations. A technology risk of the organisation using the cloud services occurs when the provisioning process of user accounts fails. For example, if the technology is incompatible the organisation using the cloud services might not be able to provision user accounts to the CSP. In this case, authorised users will not be able to access their resources. Last but not least, the organisation can not verify the quality of data management and provisioning of the CSP and whether or not the CSP performs changes to this part of IAM. To sum it up, the following risks are applicable to data management and provisioning in a cloud computing environment (Table 11).

Law and regulation risks • Incompliance with laws and regulations about security requirements of data storage • Unauthorised access to data protected by laws and regulations • Noncompliance with laws and regulations about the location of data
Data risks • Unauthorised access to data or loss of data due to incorrect deprovisioning • Unauthorised access to data or loss of data due to different data security requirements
Technology risks • Unable to access authorised resources due to incorrect provisioning
Operational risks • Unable to verify quality of data management and provisioning • Unable to manage changes to data management and provisioning

Table 11: Data management and provisioning risks.

4.7.Monitoring and auditing

In all IAM architectures in a cloud computing environment, data of the organisation using the cloud services is stored at the servers of the CSP (Chapter 3). Besides that, processes of the organisation using the cloud services are not fully controlled by the organisation itself. The CSP controls a part of the IAM processes involved in all of the cloud architectures. This results in a lack of control of monitoring and auditing processes and data. In the traditional IT environment the organisation can monitor and audit its own systems and network. When using cloud services the organisation does no longer have control over this part of IAM, since it is dependent on the CSP to which extend it can monitor and audit the cloud services that are used.

	Level of control
Traditional model	Low
Trusted relationship model	Low
Identity service provider model	Low
All in the cloud model	Low

Table 12: Level of control of authentication management.

First of all, a part of a regulation applicable to the organisation using the cloud services can be to audit his processes, system and network periodically (NEN, 2007). However, the organisation cannot audit the CSP, which runs a part of the IAM processes and stores a part of the data. In this case the organisation using the cloud services is incompliant with the regulations. Besides that, not being able to monitor and audit cloud services makes it difficult to detect unauthorised access to data (Jansen & Grance, 2011). Unauthorised access to data can lead to data theft or loss. Another risk involved is that in case of a technical problem with a cloud service, the cause of this problem cannot be easily found by using monitoring. The organisation using the cloud service is dependent on the CSP to monitor and fix the problem adequately. Last but not least, the organisation using the cloud services is not in control of the quality and frequency of monitoring, logging and auditing in general. To sum it up, the following risks are applicable to monitoring and auditing in a cloud computing environment (Table 13).

Laws and Regulation risks
• Noncompliance with regulations if the CSP cannot be audited
Data risks
• Data theft or data loss due to undetected unauthorised access to data
Technology risks
• Unable to solve a technical problem due to inability to monitor cloud services
Operational risks
• Unable to control the quality and frequency of monitoring, logging and auditing

Table 13: Monitoring and auditing risks.

4.8.Risks per dimension

Research to the risks of the different parts of IAM in a cloud computing environment resulted in a set of risks for each of the parts of IAM. The risks dimensions are used to structure the risk research for each part of IAM. In order to get an overview of all the applicable risks for IAM in a cloud computing environment, the risks are merged for each risk dimension (Section 1.5).

4.8.1. Law and regulation risks

Research to law and regulation risks results the risk of incompliance to laws and regulations. These risks are specified below for the applicable laws and regulations for IAM in a cloud computing environment.

Noncompliance with applicable laws on personal information
Noncompliance with applicable laws on location of data
Noncompliance with applicable auditing regulations
Noncompliance with applicable regulations on security requirements

Table 14: Law and regulation risks.

4.8.2. Data risks

Merging the results of research to data risks results in the risks of data theft or data loss. These risks are specified below for the different factors that cause these risks.

Loss or theft of data due to insecure authentication
Loss or theft of data due to incompatible authorisation management
Loss or theft of data due to physical access to hardware containing data
Loss or theft of data due incorrect deprovisioning
Loss or theft of data due to different data security requirements
Loss or theft of data due to lack of monitoring and auditing capabilities

Table 15: Data risks.

4.8.3. Technology risks

The following technology risks are found after merging the research to the different parts of IAM in a cloud computing environment.

Incompatible authentication mechanisms
Incompatible SSO
Incompatible technology to update or store user data
Failure of an Internet connection stops access to the cloud services
Unable to access cloud services due to incorrect provisioning
Unable to solve a technical problem due to inability to monitor cloud services

Table 16: Technology risks.

4.8.4. Operational risks

Merging the results to operational risks for IAM in a cloud computing environment results in the inability of the organisation using cloud services to manage, control and verify parts of IAM. The risks are specified below for the different factors that cause these risks.

Unable to manage control changes to processes
Unable to verify successful updates of user accounts
Unable to verify the authorisations for errors
Unable to verify successful execution of authorisations
Unable to verify who has or had access to data
Unable to verify quality of data management and provisioning
Unable to control the quality and frequency of monitoring, logging and auditing

Table 17: Operational risks.

4.9.Summary

In this chapter the changes and risks of the parts of IAM in a cloud computing environment are researched. The IAM processes of adding, changing or removing an employee do not change in a cloud computing environment compared to a traditional IT environment. This also applies for the process of users gaining access to resources in a cloud computing environment. However, parts of IAM are not managed by the organisation using the cloud services. This results in several risks for the organisation. The most important risks are noncompliance to laws and regulations, loss or theft of data, incompatible technology, technology failure and the inability to verify and control changes to IAM. The impact of the risks is dependent on the level of control of a part of IAM using a specific cloud computing model. In the next chapter controls to mitigate risks of IAM in a cloud computing environment are researched.

5. IAM controls in a cloud computing environment

In this chapter controls to mitigate the risks described in the previous chapter are researched.

5.1. COBIT

COBIT is a framework for IT governance and control (ISACA, 2007). The COBIT framework is used to identify controls for the previously described IAM risks of using cloud computing (Section 1.5) (Chapter 4). The four domains of COBIT are “plan and organise”, “acquire and implement”, “deliver and support” and “monitor” (Figure 6).

The domains of COBIT are modified to become more suitable for IAM in a cloud computing environment. The “plan and organise” domain has been renamed to selection, since this research does not focus on the decision whether or not to use cloud computing. This research focuses on how to use IAM in a cloud computing environment. This involved a thorough selection of the most appropriate CSP and cloud computing model described previously (Chapter 3). All other processes involved with planning and organising an investment in or implementation of cloud computing are not relevant for this research. The “acquire and implement” and “deliver and support” have been combined and renamed to agreements. The implementation and delivery of cloud computing within the organisation is dependent on the agreements made with the CSP. Cloud computing is frequently not implemented within the organisation using the cloud services. The cloud services are delivered and maintained by the CSP. The monitoring domain is the last domain of this model. It contains the monitoring and auditing controls.

5.2. Selection

If an organisation is planning to move certain parts of IT to the cloud, it has to carefully select the CSP (and IdSP when using the identity service provider model) (NEN, 2007). The selection procedures have to include whether or not the selectable CSP’s comply with the applicable laws and regulations (Wet Bescherming Persoonsgegevens, 2000). For example, in case the CSP is unable to store the data of the organisation using the cloud services within the region that is forced by law, the CSP might not be the best option to deliver cloud services to the organisation. Besides that, the data security requirements have to be analysed. If the CSP does not use security requirements for data that meet the standards of the organisation using the cloud services, it might not be the best option. For example, if the CSP uses less secure authentication mechanisms or a limited authorisation model compared to the organisation using the cloud services, the data security requirements of the CSP might not be sufficient. Also the technology used by the CSP has to be reviewed for compatibility with the organisation. Additional analyses for compatibility as well as capacity, for example the capacity of the internet connection, can be required as well depending on the cloud services. Last but not least, the organisation using the cloud services has to verify if they are able to manage all parts of IAM. For example, if authentication takes places at the CSP, it cannot be managed by the organisation using the cloud services. In that case, the organisation should have the ability to verify the authentication for errors for example by auditing the CSP. This applies to all parts of IAM; if the CSP cannot be monitored or audited it might not be an option for the organisation in case this is a selection requirement.

5.3.Agreements

Strong agreements governed by a service level agreement (SLA) should be made with the CSP. The SLA should include details about compliance to laws and regulations and the use of data security requirements (NEN, 2007). For example, if the organisation has data encryption as a security requirement for its data, it has to be governed by an SLA that the CSP uses the same security requirements (Brunette & Mogull, 2009). Another example is the case of Ahold (Section 3.2). As part of the SLA, Ahold agreed with Google that the data of Ahold would only be located on servers within Europe or the United States of America (Kaaij, 2011). Besides that, information on technology and operation processes should be made. For example, in case the authentication takes places at the website of the CSP, the CSP should not be allowed to change the authentication mechanisms without informing the organisation using the cloud services beforehand. This would allow the organisation to stay compatible and verify the authentication mechanisms for compliance to security standards. Another example is including the right to audit the CSP in the SLA when using cloud services. This allows the organisation to audit essential IAM processes.

5.4.Monitoring

Another control that should be in place is monitoring and periodically auditing the CSP's of the cloud services that are used. Using the right to audit allows organisation to verify all applicable aspects of IAM in a cloud computing environment (NEN, 2007). For example, this way the organisation can verify if the CSP is compliant to the applicable laws and regulations and uses appropriate data security requirements. Periodically auditing the CSP by either the organisation using the cloud services or an independent third party is essential to assure compliance (Brunette & Mogull, 2009). Auditing can also help to find the causes of technology issues. Last but not least, periodical auditing allows the organisation to stay in control of the parts of IAM. It allows them to verify changes to the mechanisms and errors made during IAM processes. This is an essential control to remain in control of the risks of IAM in a cloud computing environment.

5.5.Control model

The previously described control domains can be arranged and used in every phase of an implementation involving IAM and cloud computing. It starts with a selection procedure for the appropriate CSP delivering the cloud services, followed by making agreements with the chosen CSP and after implementation, the CSP should be monitoring and audited periodically. For all those control domains the organisation using the cloud services should verify compliance to laws and regulations, data security requirements, technology compatibility and capability and operational control in general (Figure 22).

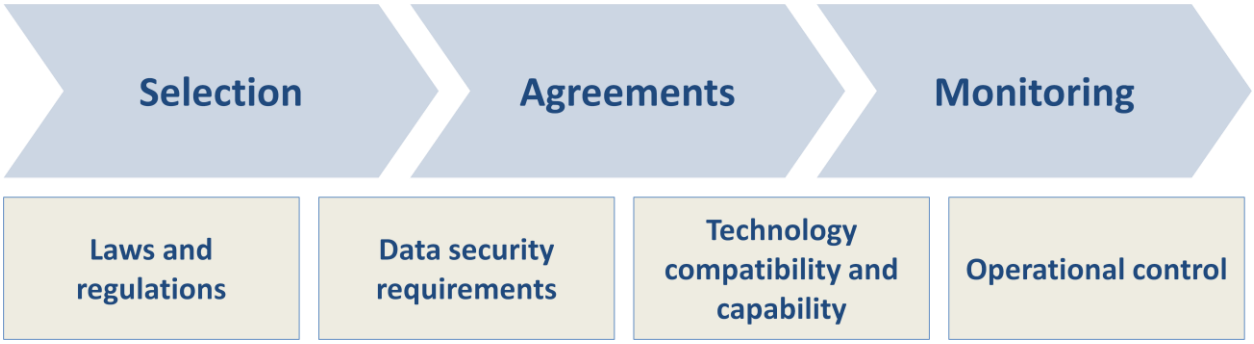

Figure 22: Controls for IAM in a cloud computing environment.

5.6.Summary

In this chapter the controls to mitigate the risks of IAM in a cloud computing environment are researched. The organisation using the cloud services should consider the following control domains to manage the risks. First of all they should make a thorough selection for the CSP that is going to deliver the cloud services. After that, solid agreements governed by an SLA should be made with the selected CSP. Last but not least, the CSP delivering the cloud services has to be monitoring and audited periodically to test for compliance. For all these controls the organisation using the cloud services should take the following aspects into account: compliance to laws and regulations, data security requirements, technology compatibility and capability and operational control in general (Figure 22).

6. Concluding remarks

6.1. Conclusion

In the last couple of years cloud computing has grown to a widely accepted IT model. However, security and the trust factor of cloud computing are obstacles for organisations to use cloud computing. With the growing amount of data and users and stricter rules for organisations for data storage IAM has become more important. When using cloud computing, data is no longer stored within the organisations owning the data. The current state of IAM does not provide sufficient possibilities to manage this. This qualitative research is focused on organisations that are or are trying to manage the identity and access for SaaS applications. This research studied the effects of cloud computing on the risks and controls of the processes of IAM. The main research question of this research is: "What are the specific risks and controls of IAM processes in a cloud computing environment?".

This research defines the four architecture models to use IAM in a cloud computing environment. The first architecture is the traditional model. In this model the organisation manages his own on-premise IAM processes and connects them to the CSP. All users have to be added to, changed in or removed from the UDS of the CSP or CSP's providing the cloud services. In the trusted relationship model, the CSP trust and uses the IAM of the organisation using the cloud services. The users are stored in the UDS of their organisation and can connect to the cloud services using local authentication. In the identity service provider model, a third party is introduced to validate the identity of a user. Users are stored in the UDS of their organisation and when connection to a cloud service the IdSP validates the identity of the user. In the all in the cloud model the organisation fully delegates IAM to a CSP. Users use the cloud IAM service to access on-premise as well as off-premise services.

Depending on the architecture used, parts of IAM are not managed by the organisation using the cloud services. This causes risks for the organisation. The most important risks are noncompliance to laws and regulations, loss or theft of data, incompatible technology, technology failure and the inability to verify and control changes to IAM. The impact of the risks is dependent on the level of control of a part of IAM. Depending on which IAM architecture is used, the impact of a risk can be more or less severe.

The organisation using the cloud services should consider the following control domains to manage the risks: selection, agreements and monitoring. For all these control domains the organisation using the cloud services should take these risk dimensions into account: laws and regulations risks, data risks, technology risks and capability and operational risks. The first step for the organisation is to make a selection of the CSP that is going to deliver the cloud services. After that agreements, governed by an SLA, should be made with the selected CSP. Last but not least, the CSP delivering the cloud services has to be monitored and audited periodically to test for compliance.

6.2.Future research

This research focuses on IAM as an important security factor for cloud computing within organisations. However, IAM is not the “Holy Grail” of IT security. There is room for research to other security aspects of cloud computing, especially within organisations. Besides that, this research only takes the organisations that use cloud services into account. There is room for research to security of other types of cloud computing consumers and CSP’s.

This research only takes the public deployment model of cloud computing into account. It has not been researched whether or not the private, community or hybrid variants of cloud computing have the same impact on the risks and controls of IAM. Public cloud computing is considered to be the “most extreme” deployment model of cloud computing, since the data of the organisation is fully trusted to the CSP. Additional research to IAM for other deployment models is necessary. Besides that, this research focuses on SaaS as a delivery model of cloud computing. Although there is quite some overlap with PaaS and IaaS, the results of this research cannot be directly linked to these delivery models of cloud computing. Additional research to these alternative models is essential.

This research contains four IAM architectures for a cloud computing environment. Research is required in order to select the most suitable architecture for a specific organisation.

7. Abbreviations

The following abbreviations are used in this research.

CSP	Cloud service provider
HR	Human resources
IaaS	Infrastructure as a service
IAM	Identity and access management
IdSP	Identity service provider
IT	Information technology
PaaS	Platform as a service
RBAC	Role-based access control
SaaS	Software as a service
SLA	Service level agreement
SSO	Single sign-on
UDS	User data store
CSP	Cloud service provider

8. References

AICPA. (1992). *Statement on Auditing Standards No. 70.*

Bi, L. (2008). Identity and access: How to protect your business. *Journal of Corporate Accounting & Finance , 19* (5), 9-13.

Birman, K., Chockler, G., & van Renesse, R. (2009). Toward a cloud computing research agenda. *SIGACT News , 40* (2), 68-80.

Blakley, B. (2009). *The Business of Identity Services.* Midvale, United States of America: Burton Group.

Boroujerdi, M. M., & Nazem, S. (2009). Cloud Computing: Changing Cogitation about. *World Academy of Science, Engineering and Technology , 58*, 1112-1116.

Brunette, G., & Mogull, R. (2009). *Security Guidance for Critical Areas of Focus in Cloud Computing V2.1.* Cloud Security Alliance.

Carlin, S., & Curran, K. (2011). Cloud Computing Security. *International Journal of Ambient Computing and Intelligence , 3* (1), 38-46.

Chang, H., & Choi, E. (2011). User Authentication in Cloud Computing. *Communications in Computer and Information Science , 151*, 338-342.

Chung, W. S., & Hermans, J. (2010). *From Hype to Future: KPMG's 2010 Cloud Computing Survey.* IT Advisory. Amstelveen, The Netherlands: KPMG Advisory.

CloudID. (2010). Retrieved 5 30, 2011, from http://www.cloudid.nl/

COSO. (2004). *Enterprise Risk Management – Integrated Framework.*

Cser, A., Balaouras, S., & Hayes, N. M. (2010). *Are You Ready For Cloud-Based IAM?* Cambridge, United States of America: Forrester Research.

de Pater, W. (2011, 2 23). Solution Architect Identity & Access Management at Oracle Nederland BV. (E. Sturrus, Interviewer) De Meern, The Netherlands.

Google Apps. (2006). Retrieved 5 3, 2011, from http://www.google.com/apps/

Gopalakrishnan, A. (2009). Cloud Computing Identity Management. *SETLabs Briefings , 7* (7), 45-54.

Goulding, J. T., Broberg, J., & Gardiner, M. (2010). *Identity and Access Management for the Cloud: CA's Strategy and Vision.* Islandia, United States of America: CA Technologies.

Günsberg, W. A. (2009). *Federated Identity Management: The auditor's perspective.* Master Thesis, VU University Amsterdam, Amsterdam.

Harauz, J., Kaufman, L. M., & Potter, B. (2009). Data security in the world of cloud computing. *Security & Privacy, IEEE , 7* (4), 61 - 64.

Hermans, J., & ter Hart, J. (2005). Identity & Access Management: operational excellence of 'in control'? *Compact Magazine , 2005* (3), pp. 47-53.

Hotmail. (1996). Retrieved 1 7, 2011, from http://www.hotmail.com/

Huang, H. Y., Wang, B., Liu, X. X., & Xu, M. J. (2010). Identity Federation Broker for Service Cloud. *International Conference on Service Sciences* (pp. 115-120). Los Alamitos, United States of America: IEEE Computer Society.

Huynh, I. (2011). *Top Six Security Questions Every CIO Should Ask a Cloud Vendor.* Cloud Security Alliance.

ISACA. (2007). *COBIT Framework for IT Governance and Control 4.1.*

Jansen, W., & Grance, T. (2011). *Guidelines on Security and Privacy in Public Cloud Computing.* Information Technology Laboratory. Gaithersburg, United States of America: National Institute of Standards and Technology.

Jøsang, A., & Pope, S. (2005). User Centric Identity Management. *AusCERT Asia Pacific Information Technology Security Conference.* Brisbane, Australia: AusCERT.

Kaaij, A. (2011, 2 17). Architect Architecture & Planning at Ahold IM Europe. (E. Sturrus, Interviewer) Zaandam, The Netherlands.

KPMG. (2010). *Cloud Computing Risks: Current Insights.* KPMG International.

KPMG. (2007). *IAM Methodology.* KPMG International.

Kreizman, G. (2011). *IAMaaS Adoption Is Increasing.* Stamford, United States of America: Gartner.

Mather, T., Kumaraswamy, S., & Latif, S. (2009). *Cloud Security and Privacy: An Enterprise Perspective on Risk and Compliance.* Sebastopol, United States of America: O'Reilly Media, Inc.

Mell, P., & Grance, T. (2011). *The NIST Definition of Cloud Computing.* Information Technology Laboratory. Gaithersburg, United States of America: National Institute of Standards and Technology.

Microsoft Active Directory. (2000). Retrieved 1 2011, 14, from http://www.microsoft.com/windowsserver2008/en/us/ad-main.aspx

Microsoft Office 365. (2011). Retrieved 4 18, 2011, from http://office365.microsoft.com/

NEN. (2005). *NEN-ISO/IEC 27001: Informatietechnologie - Beveiligingstechnieken - Managementsystemen voor informatiebeveiliging - Eisen.* Delft, The Netherlands: Nederlands Normalisatie-instituut.

NEN. (2007). *NEN-ISO/IEC 27002: Code voor informatiebeveiliging.* Delft, The Netherlands: Nederlands Normalisatie-instituut.

Okuhara, M., Shiozaki, T., & Suzuki, T. (2010). Security Architectures for Cloud Computing. *Fujitsu scientific and technical journal , 46* (4), 397-402.

Ponemon, L. (2010). *2010 Access Governance Trends Survey.* Traverse City, United States of America: Ponemon Institute.

Radosevic, S. (2011, 3 16). Security Technology Specialist at Microsoft Nederland BV. (E. Sturrus, Interviewer) Amstelveen, The Netherlands.

Salesforce.com. (1999). Retrieved 1 7, 2011, from http://www.salesforce.com/

Shank, G. D. (2005). *Qualitative Research: A Personal Skills Approach (2nd Edition).* Upper Saddle River, United States of America: Prentice Hall.

Steijaert, A. (2011, 4 6). Program Manager & IT Advisor at SURFnet. (E. Sturrus, Interviewer) Amstelveen, The Netherlands.

Stoneburger, G., Goguen, A., & Feringa, A. (2002). *Risk Management Guide for Information Technology Systems.* Information Technology Laboratory. Gaithersburg, United States of America: National Institute of Standards and Technology.

Vaquero, L. M., Rodero-Merino, L., Caceres, J., & Lindner, M. (2008). A break in the clouds: towards a cloud definition. *ACM SIGCOMM Computer Communication Review , 39* (1), 50-55.

Villavicencio, F. (2010). *Approaches to IDaaS for Enterprise Identity Management.* New York, United States of America: Identropy.

Wet Bescherming Persoonsgegevens. (2000).

Witty, R. J., Allan, A., Enck, J., & Wagner, R. (2003). Identity and access management defined. *Gartner Research Note SPA-21-3430* .

9. Interviews

The following interviews are used in this research.

Name	Arnout Kaaij
Organisation	Ahold IM Europe
Function	Architect Architecture & Planning
Date	17 February 2011
Location	Zaandam, The Netherlands
Reference	(Kaaij, 2011)

Name	Willem de Pater
Organisation	Oracle Nederland BV
Function	Solution Architect Identity & Access Management
Date	23 February 2011
Location	De Meern, The Netherlands
Reference	(de Pater, 2011)

Name	Sasa Radosevic
Organisation	Microsoft Nederland BV
Function	Security Technology Specialist
Date	16 March 2011
Location	Amstelveen, The Netherlands
Reference	(Radosevic, 2011)

Name	Andres Steijaert
Organisation	SURFnet
Function	Program Manager & IT Advisor
Date	6 April 2011
Location	Amstelveen, The Netherlands
Reference	(Steijaert, 2011)