Improving the boarding process of external insiders in large organisations

The Philips case

Master thesis

Peter Keeris

UNIVERSITY OF TWENTE.

PHILIPS

UNIVERSITY OF TWENTE.

PHILIPS

Improving the boarding process of external insiders in large organisations

Velp, September 8, 2014

Author

Name:	P.J.C. (Peter) Keeris
Student number:	S0121401
E-mail:	p.j.c.keeris@alumnus.utwente.nl

University of Twente

Master:	Business Information Technology
Faculty:	School of Management and Governance / Electrical Engineering, Mathematics and Computer Science
PO box	217, 7500 AE, Enschede
Website:	www.utwente.nl

Royal Philips N.V.

Department:	Philips IT Delivery
Competence group:	Security & Authorizations
Location:	High tech campus, Eindhoven
PO Box	77900, 1070 MX, Amsterdam
Website:	www.philips.nl

Graduation Committee

Jos van Hillegersberg	University of Twente, School of Management and Governance
Klaas Sikkel	University of Twente, Electrical Engineering, Mathematics and Computer Science
Stefan Pados	Philips, IT Delivery (Competence Manager SAP GRC Access Control)
Paul Keltjens	Philips, IT Delivery (Director Security & Authorizations)

Management Summary

Large organisations who outsource big parts of their IT need to be able to quickly onboard the outsourced workers (external insiders) to the IT systems which are required to do the job. Identity and access management systems are being used to execute this process. This is however not easy because organisations tend to be precautious when giving external insiders access to their systems and because it is a process involving two or more organisations and often multiple organisational units. This research presents an approach for organisations to identify barriers and design an improved onboarding process. To validate the approach, it was applied at Philips which resulted in a high level solution for Philips to improve their boarding process. The approach was built and improved iteratively, based on the experiences of the Philips case. The approach consists of six steps:

Step 1: Analyse the organisation
The first step of the approach is the analysis of the organisation. This step is divided into three parts which can be executed simultaneously:

- Identify the context of the organisation, this is done by taking the context variables (section 2.1) and match them with the situation of the organisation;
- Analyse the current boarding process of the organisation by examining internal documents, attending meetings about this subject and interviewing employees and partners who are part of the boarding process;
- Identify the goals of the organisation that should be reached by adopting the improvements. Goals could for instance be to increase the speed of the boarding process, reduce costs, increase security or increase user satisfaction.

Step 2: Identify issues
The second step is to use the analysis from step one to identify issues regarding the boarding process. This can be issues related to the goals set by the organisation as well as issues that were identified with the boarding process analysis.

Step 3: Design an improved boarding process
The next step is to design the improved boarding process. This process is not limited to the design of one solution, but multiple scenarios could be designed that fit within the existing architecture of the organisation. The IAM techniques, which were identified in section 2.2 and 2.3, can be used to solve the issues of step two. In this step, the barriers for implementation of identity and access management (section 2.4) should also be addressed by analysing how the organisation will deal with them. Any issue in step two that can form a barrier to the implementation of identity and access management, should also be added to the barrier list (making it a dynamic list).

Step 4: Develop recommendations for implementation of the boarding process
In step four, the designs of the improved boarding process will be used to develop recommendations for the organisation to implement the boarding process by making a business case. In this business case, all different scenarios will be compared with their own costs, risks and benefits. Also a net return on investment allows the organisation to compare between different projects. Finally, the preferred solution from the business case is worked out in more detail to serve implementation.

Step 5: Implement
The next step contains the implementation of the preferred solution from the business case. All the involved employees and partners should be briefed about the new boarding process in advance. Then,

an appropriate change management process should be initiated which is in line with the organisation's policy on implementing new business processes.

Step 6: Evaluate
In the final step, the new boarding process is evaluated to verify whether all goals were reached, all issues were solved and no new issues arose. This evaluation could be used as input for new improvements by applying the approach again from step one.

The validity of this research is limited because not all steps were applied at the Philips case. Further research is needed for an ex-post evaluation of the approach. Such an evaluation should make clear whether all goals were reached and all issues were solved. Once this is successful, the scope could be widened to all Philips IT partners and non-IT partners. The approach becomes more reliable if it is applied and evaluated in more cases. It would also be interesting for further research to apply this approach on a small or medium sized organisation that builds its first identity and access management system.

Preface

This Thesis is the final step in my Master studies Business Information Technology. When I started at Philips on the High Tech Campus in Eindhoven, it was unclear what would exactly be my assignment. All I was told is that the boarding process was inefficient and it was my task to find out what was wrong with it, why it was wrong and how to improve it. To get me started, my supervisors at Philips invited me to dozens of meetings and gave me a list of people to talk with about the boarding process. This gave me a great experience to see from the inside how a big multi-national organisation works. From there I was able to get all the needed information to map the boarding situation of Philips IT and use it as a case validation for this research.

Of course I would not have been able to successfully finish this Thesis without certain people who have supported me during my research. First, I would like to thank Jos van Hillegersberg. Your expertise has taught me a lot and you were always able to point me in the right direction when I had hit a roadblock. Unfortunately Pascal van Eck had to leave my graduation committee due to his new job, but nevertheless I want to thank you for the great feedback you gave me. Also your comparison of IT onboarding and soldiers in World War I really helped me think outside the box. Fortunate, Klaas Sikkel was willing to replace Pascal in my graduation committee, thank you for that. Another great mentor to me was Stefan Pados, my direct supervisor at Philips. You were always available to me for when I had questions and we had great laughs during our lunches. I also want to thank Paul Keltjens, my other supervisor at Philips for your great insights. Of course I am also very grateful to all other people at Philips who helped me get information for my research. As last, I would like to thank my family and friends for all the support and encouragements I received.

Glossary

- **Application Developers (AD):** Partner resources who work on the development of (new) applications.
- **Application Managed Services (AMS):** Partner resources who work on the maintenance of applications.
- **Boarding tool:** Internal Philips tool which handles onboarding, offboarding and changeboarding requests. It sends out e-mails to all involved parties who need to take action in this process. It also registers the feedback these parties give.
- **Business Analyst (BA):** Employee who is part of a project team translating Business requirements into IT solutions. The BA is a counterpart of the business representation for functional requirements.
- **Competence group Security & Authorization (CG S&A or S&A):** The competence group within IT delivery which is involved with giving a resource SAP access.
- **Clarity:** System in which employees and time-hired resources can register their working hours.
- **CODE account:** Common Office Desktop Environment is the name of the Philips accounts. There are CODE1 and CODE2 accounts. CODE2 is very limited, intended for partners who just need access to a SharePoint file for example.
- **Competence group:** Within Philips IT delivery, there are sixteen specialized groups, with staff enabled to work on global projects and support operational services throughout Philips.
- **Enterprise Management Infrastructure (EMI):** A multi-functional global framework that supports deployment of management of desktop infrastructure based on CODE. EMI has the role of active directory and domain controller based on Microsoft Windows server.
- **External insiders:** individuals that are not trusted and have (some) authorized access over the organisation's assets (Nunes Leal Franqueira et al., 2010).
- **Global Resource Manager (GRM):** In the GRM community, all global resource managers make sure there is enough capacity for all projects and no resources are idle.
- **Identity / Account:** When someone is added in PDS/PIM, it is an identity. When the identity is activated in EMI, it becomes an account that one can use on the Philips network/applications.
- **Identity and Access Management (IAM):** IAM systems deal with the authentication and authorization of individuals in one or multiple systems.
- **Line Manager / Team lead:** Philips employee who manages the resource. This can be a different person per platform/location (US, NL, IN). The difference is that line managers are managers for Philips employees and team leads manages partner resources. In some systems (PDS/PIM) this is called line manager while a team lead is meant in practice. This is because PDS and PIM are used within Philips globally (team lead are only used at IT delivery).
- **Offshore development centre (ODC):** ODC's are secure buildings in India where resources are working on AMS projects (Wipro and Cognizant).
- **Partner / Vendor:** In the scope of this research, partners (also called vendors) are Wipro, Cognizant, Ciber and Capgemini.
- **Partner resource:** An employee of a partner who does work for Philips.
- **People Data Store (PDS):** PDS is currently the leading system for identities. It is also the link between HR systems and IT systems.
- **Peoplefinder:** System where Philips employees can look up their college's and see their place in the Philips hierarchy.
- **Philips Identity Manager (PIM):** PIM centralizes the administration of all user identities, login accounts and passwords.

- **RFI:** Request for Information.
- **Service-Level Agreement (SLA):** A SLA is part of a contract in which a service is defined. The SLA is often referred to as the maximum delivery time to complete the service.
- **Service Manager 7 (SM7):** The Service Manager (version 7) which is used within Philips. In this service manager all kinds of services can be requested based on a ticket system. SM7 consists of two parts, the analyst portal and the One IT help desk.
- **SM7 – Analyst portal:** The analyst portal consists of assignments groups and change management groups. The assignment groups are for support, they can be used to report incidents or request a service. The change management groups are divided in three categories: Request, Approve and Execute a change per domain. Philips regulations do not let someone be assigned to all these groups at the same time for a project (this leads to conflicts with output based partners who sometimes want all these roles assigned to one resource).
- **SM7 – One IT help desk:** The One IT help desk consists of several services like support for Philips laptops and software, but resources can also unlock SAP access here (when it was disabled after 90 days of inactivity). There are key user groups for each service, so only if someone is assigned to a group for the service, he can use it. It is also possible to be assigned to request a service on behalf of someone else (like team leads can request SAP access for partner resources).
- **Single point of contact (SPOC):** Each partner has one SPOC person.
- **Tech Lead:** Philips employee who is part of a project team. He has in depth knowledge of IT applications and platforms and the translation of high level solutions into detailed technical design. He also keeps tracks of development in IT solutions and is the counterpart of the Architects.
- **Third party gateway (TPG):** TPG is the firewall between partners (Third parties) and the Philips network.
- **Virtual Desktop Infrastructure (VDI):** VDI is a service that hosts users' desktop environment on a remote server. In this desktop environment, virtualized applications can be used by the resources.

Table of contents

List of figures

List of tables

1. Introduction

1.1. Organisation

Philips focuses on improving people's live through timely innovations with a brand promise of "sense and simplicity". With a portfolio consisting of three divisions (Healthcare, Lighting and Consumer Lifestyle), Philips has approximately 118.000 employees with sales and services in more than 100 countries worldwide making €24.8 billion sales in 2012 (Philips, 2013).

This research will focus on the IT delivery department of Philips that delivers IT infrastructure and applications to the three divisions. This was formerly fully done in-house but over the last few years, Philips focused more on its core business so maintaining and developing of IT applications is outsourced to partners. The outsourced work is mainly done by four partners of Philips: Wipro, Cognizant, Capgemini and Ciber.

Philips recently changed from just in time-hired to also output based working with these IT partners. This means that the partner does not get paid for every hour they work on something anymore, but they get one fixed price based on the result. Master Service Agreements with these Output based partners are made in which all conditions and key performance indicators are standardized. So when the partners start on a new project, they do not have to check payment conditions for example, the only thing that matters are the required capabilities (Zijlstra, 2013). As a consequence, partner resources need to be onboarded quickly for every project (and also change- and offboarded). Philips has a Service-Level Agreement (SLA) of ten days to get someone fully onboarded, but in practice this SLA is not always met. Why this process often is delayed, is unknown to Philips.

In this research, I defined onboarding as the process of providing a new employee or a partner resource with all the required access rights and facilities to do a required job. Changeboarding is the process of changing someone's required access rights and/or facilities and offboarding is the process of removing someone's access rights and retrieving the facilities. The partners need to make sure that their workers have had the right training to work with the business applications and know all the used terminology.

1.2. Problem description

[CONFIDENTIAL]

1.2.1. Problem perspective

[CONFIDENTIAL]

1.2.2. External insiders

Nunes Leal Franqueira et al. (2010) identified the partner resources that have access to systems as External Insiders. They define them as "individuals that are not trusted and have (some) authorized access over the organisation's assets". They state that external insiders arise when organisations are cooperating with third parties. This cooperation will only be initiated if there is a certain level of trust between these organisations, however this does not mean that there is trust between the organisation and the individuals who do the actual work. Since it is mostly not possible to do risk assessment on an individual basis, standard access policies are agreed upon in contracts between these organisations. The contracts however are typically abstract and do not contain the level of detail required to grand access to external insiders. A problem with identity management with these external insiders is that it is sometimes impossible to uniquely identify individuals (Nunes Leal Franqueira et al., 2010).

1.2.3. Goal and scope

The goal of this research is *to develop an approach to improve the boarding process of external insiders in a specific context*. The context will be defined with variables that have impact on the boarding process. To validate the approach, it will be applied to the Philips case. The improvements should help organisations saving time with boarding while being compliant to their business partners to support an agile way of working.

For the Philips case, the scope will be limited to the four output based partners at IT delivery for application development and maintenance. Excluded in this case will be the boarding process of Philips own employees since Philips uses a different HR process for them. Also the implementation of the improvements are out of scope for this research.

1.3. Research approach

Hevner et al. (2004) created a framework for understanding, executing, and evaluating Information Systems (IS) design research by combining behavioural-science and design-science paradigms, as shown in figure 1.1. The framework describes all the factors that will influence this research. From the Knowledge Base, I will use various theories and methodologies from literature. The Environment represents Philips and its partners. All the information gathered from both sides will lead to the design of the approach to improve the boarding process (which is the Artifact).

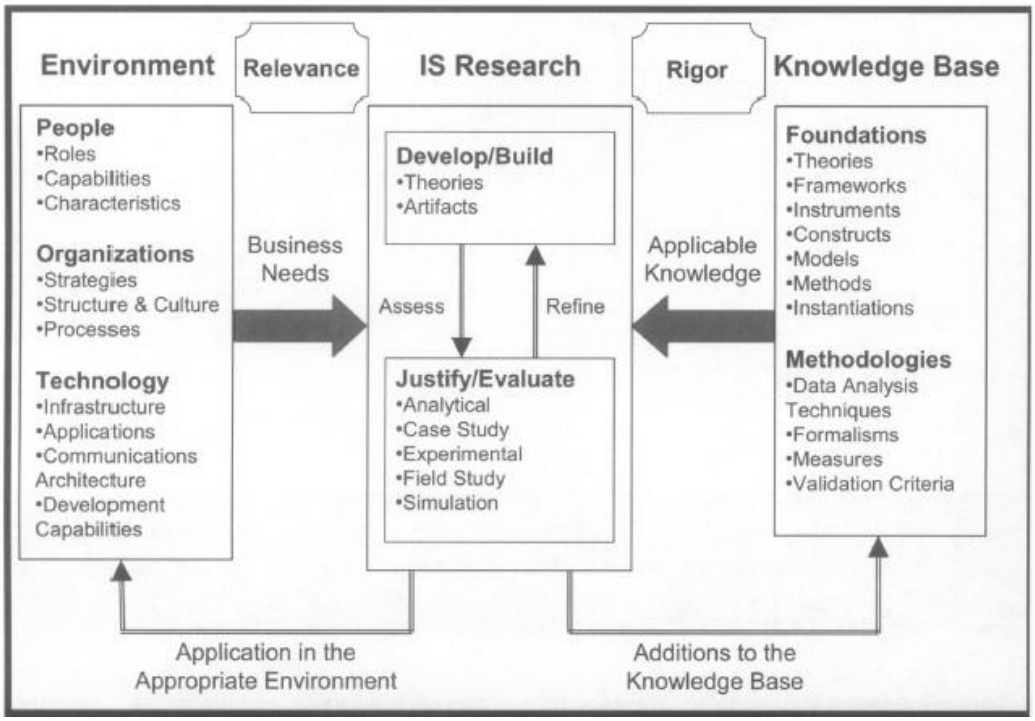


Figure 1.1: Framework for IS research (Hevner et al., 2004)

As described above, the goal of this research is to develop an approach to improve boarding process of external insiders in a specific context. Therefore, I will first discuss what the guidelines are on how to design such an artifact. Walls et al. (1992) made a foundation for this with their Information system design theory (ISDT). Gregor and Jones (2007) extended the work of Walls et al. by identifying the structural components of a design theory. Appendix A: Gregor and Jones (2007) eight components of a

design theory lists the identified eight components of design theories. I will use these components to structure the design process of this research in table 1.1.

Component	In this research
Purpose and scope	The goal of this research is to develop an approach to improve the boarding process of external insiders in a specific context. The context will be defined with variables that have impact onboarding situations.
Constructs	Onboarding, Identity and access management, Flowchart models, External insiders, Process design.
Principles of form and function	An approach will be given to help large organisations with boarding of external insiders.
Artifact mutability	The approach will need to take the situation and requirements of each individual organisation in mind when being applied.
Testable propositions	The approach will help organisations speed up their onboarding process.
Justificatory knowledge	The approach will be designed with identity and access management literature as well as existing identity and access management systems from different vendors. Also the experience from the Philips case is used to develop the approach.
Principles of implementation	The approach can be applied to large organisations that recently started outsourcing IT or still struggle with the onboarding process of external insiders.
Expository instantiation	The Philips case will be used to validate the approach.

Table 1.1: Components of Gregor and Jones applied to this research

1.3.1. Research methodology

Figure 1.2 represents the structure of this research. The theoretical framework consist of literature research of context variables (the variables that can complicate the boarding process), ways to use identity and access management, identity and access management components and identity and access management barriers for implementation. This theoretical framework will be used to develop the approach to improve the boarding process. To validate the approach, it will be applied to the Philips case.

To apply the approach at Philips, information is acquired by internal analysis at Philips and analysis at Philips IT partners. This information is used to identify all bottlenecks and issues in the boarding process of Philips. For these issues, a high level solution will be designed which will result in recommendations for Philips. While applying the approach to the Philips case, the approach will iteratively be modified and improved, based on the experience of the Philips case.

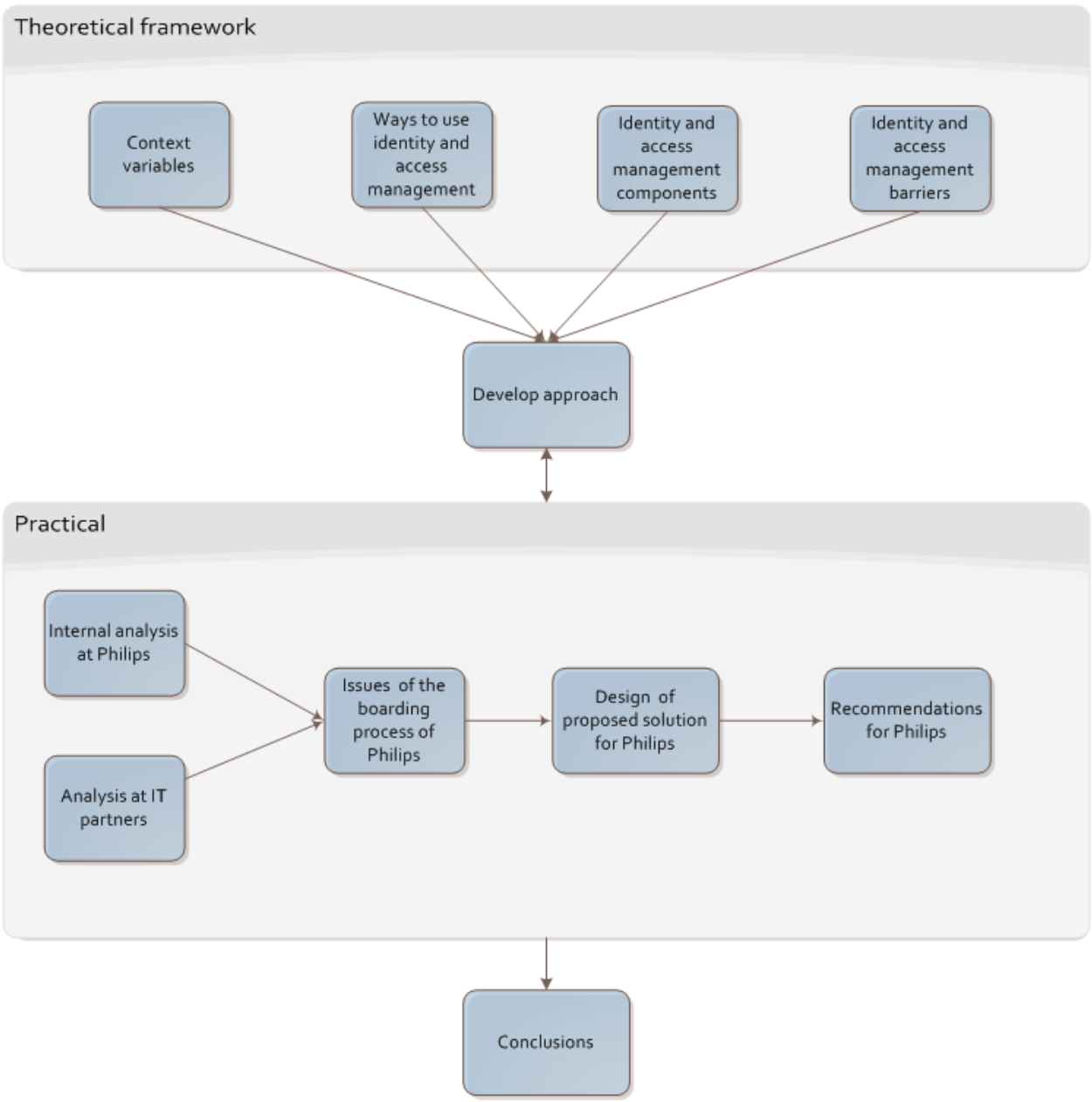


Figure 1.2: Research structure

To work towards the goal of developing an approach to improve the boarding process, the following research question is defined: ***How can organisations improve the boarding process of external insiders?*** To answer this question, the first step is to find out which factors complicate the boarding process to define a context. These factors will be used with identity and access management literature as well as existing identity and management systems information to find out what the important identity and access management components are. This will continue with what the barriers are for the implementation of identity and access management. This theoretical framework will lead to the development of the approach of improving the boarding process of external insiders. The approach will be applied to the Philips case to validate it. Table 1.2 summarizes the research questions that are derived from this research, including a methodology to answer the questions. The research is divided

into two parts: (1) the theoretical framework in which the approach is developed by doing design research and (2) the practical part in which the approach is applied to the Philips case.

Part	Research question	Methodology
	How can organisations improve the boarding process of external insiders?	Develop an approach to improve the boarding process.
1.	1. Which context variables can complicate the boarding process?	Identify factors which complicate boarding with literature research and case based validation at Philips.
	2. What are the different ways of using identity and access management?	Discuss identity and access management models with literature research.
	3. What are the important identity and access management components?	Identify identity and access management components with vendor research and literature research.
	4. What are the barriers to implement identity and access management systems?	Discuss identity and access management implementation model(s) from literature and case based validation at Philips.
2.	5. How can the Philips boarding process be improved?	Apply the approach to the Philips case. Examining Philips documentation, interviews and meetings.

Table 1.2: Research questions and methodology

The interviews and meetings conducted at Philips are with persons who have the following roles: Team leads, Global Resource Managers, partner Single Point of Contacts (SPOCs), partner workers, IT support office, Security and Authorization (S&A) secretary, Security and Authorization experts and PIM experts, Service Manager 7 experts and identity managers. Sometimes there were contradictions in the stories which needed a follow up conversation, but in most cases it turned out that someone was talking about a difference in scope. For example the difference between output based partners and time and material contracting.

1.3.2. Systematical literature research

The literature research was done systematically following the five-stage grounded-theory method from Wolfswinkel, Furtmueller and Wilderom (2011). Their method consists of the iterative stages define, search, select, analyse and present. The first stage is 'define' in which the criteria for inclusions and/or exclusion are set, the fields of research are identified, the appropriate sources are determined and specific search terms are defined. In the 'search' stage the actual search is done through the identified sources. The next stage is 'select' which is about filtering doubles and papers which do not match the criteria. This is done by reading the titles, abstracts or more of the text. Also forward and backward citations are checked in this stage. In the 'analyse' stage the papers are read and relevant parts are highlighted. The last stage 'present' is used to structure the data in a logical way categorized by subjects. All these stages are executed in an iterative way, so after the first time analysing, new keywords came to mind for which the method was used again from stage one. The method was finished when no new papers showed up with the search.

For this research I started to find papers about third party onboarding and inter-organisational access management. This did not give any useful results. So I had to change my focus to identity and access management without the inter-organisational aspect. I used Scopus, Web of Science and Google (Scholar) as search engines and I focussed my queries on the research fields of Computer science, Business process Management, Outsourcing and IT Security. Criteria of exclusion were top management onboarding and Human resources. Also outdated papers about identity and access management were excluded. In the end, this resulted in around 200 (white)papers that were selected of which by far the most were about identity and access management.

1.4. Conclusion

This chapter gave an introduction to the Philips case describing how the boarding problems came about. It explained the problem perspective of why it is hard for organisations to structure the boarding process. The main research question is defined as: *How can organisations improve the boarding process of external insiders?* The chapter continued with describing the research method that will be followed to develop an approach to improve the boarding process of external insiders.

2. Theoretical framework

This chapter describes the literature research that was conducted as mentioned in the research approach. The research starts with explaining what the factors are which can complicate the boarding processes. The chapter continues with describing identity and access management, the ways it can be used and the important components. After that, barriers for the implementation of identity and access management will be identified. This chapter will end by concluding how the boarding process of external insiders can be improved by introducing an approach with a series of steps.

2.1. Factors complicating boarding

This research starts by explaining why it is hard for organisations to shape the boarding process of external insiders. Several factors which can complicate boarding will be discussed. First the factors will be discussed which are related to the size and age of an organisation. The second part of this section discusses the factors which are related to the type of sourcing. These complicating factors will create a specific context of an organisation. These context variables will be used in the approach to analyse why boarding is complicated in the organisation on which the approach is being applied.

2.1.1. Size

Various researches were conducted on the relation of the size of organisations and factors like innovation, R&D expenditures, market power, implementation and use of IT and enterprise resource planning. Some researchers use the number of employees as a definition of size while others use the revenues. In this research, a large organisation is defined as an organisation with over 10,000 employees. Boarding is more complicated in large organisations as more people tend to be involved in the process. For example, in a small organisation of ten employees where one person is in charge for onboarding a new employee, he will arrange everything for the new employee and give him access to the IT systems. The one person knows everything and is always the direct contact for questions. This is different in large organisations with over 10,000 employees where several people all do a small part in the onboarding process (Mabert, Soni and Venkataramanam, 2003).

Also the applications and systems of an organisation have an influence on boarding. Old applications might be harder to connect to an identity and access management system because they use old technologies which are incompatible with modern identity and access management software or it might not even be possible to link them at all. The number of applications is also a factor which can complicate boarding. Within the onboarding process, employees will need to get access to the applications they need for their job. So organisations need to have processes in place to request, approve, and change access rights for these applications. Thus, the more applications an organisation has, the more complicated the boarding process will be (Mabert, Soni and Venkataramanam, 2003). This might become even more difficult when there is a wide variety of applications within the organisation which all use a different way of linking to the identity and access management system to exchange authentication and authorization data.

Not only the size and applications of the organisation influences the complexity of boarding, but also the number of organisations it has partnerships with. Other organisations can have different systems, habits and ways of working, so the organisation might need to modify their boarding process for each individual partner in order to work together. Also, an organisation can have different levels of trust or privacy regulations with their partners, some might be allowed full access to the intranet while others need to be as limited as possible (Sabherwal, 1999).

2.1.2. Types of sourcing

There are four types of sourcing arrangements based on the country and company (Moe, Mite and Hanssen, 2012):

- Onshore insourcing: Sourcing is done in the same country at the same company;
- Offshore insourcing: Sourcing is done in a different country at the same company;
- Onshore outsourcing: Sourcing is done in the same country at a different company;
- Offshore outsourcing: Sourcing is done in a different country at a different company.

In contrast to insourcing, outsourcing requires an organisation to make several arrangements with the other organisations and it deals with trust and privacy issues. Within IT outsourcing, there are various ways of cooperating. For example, an organisation can outsource certain information system functions, an application building project or hire a partner resource to do a specific job or take place in a team. Kishore et al. (2003) categorized outsourcing based on how extensive the partnership goes, as shown in table 2.1. Both Reliance and Alliance have a high extent of substitution of the service providers while Support and Alignment have a low extent of substitution of the service providers. The other dimension Kishore et al. used is the strategic impact. This means the way the partnership influences the competitive positioning and the long-term strategy of the organisation. Reliance and Support have a low impact and Alliance and Alignment have a high impact.

Reliance • Extent of substitution: high • Strategic impact: low • Cost reduction is generally the major motivation for outsourcing. • Contract periods are usually longer term.	**Alliance** • Extent of substitution: high • Strategic impact: high • Most comprehensive type of outsourcing. • This relationship involves management of a strategic partnership with the service provider.
Support • Extent of substitution: low • Strategic impact: low • Typically traditional IS services such as payroll processing. • Insourcing is usually the primary governance mode for the firms in this cell. • Outsourcing is only used on a selective basis to support information services of a firm. • This relationship imposes the lowest switching and set-up costs.	**Alignment** • Extent of substitution: low • Strategic impact: high • Generally consulting type high-impact IS services like implementation of ERP systems. • Mostly project-based IS services, such as those required for new application systems development or implementation of package solutions. • Gaining access to world-class technical expertise is generally a major motivation for outsourcing.

Table 2.1: Characteristics of outsourcing categories (Kishore et al., 2003)

The difference of outsourcing types for onboarding is if the third party worker needs access to the systems and applications of the company or sometimes even assets from the company. So the depth of outsourcing also can have influence. For example if maintenance of certain applications is outsourced, a partner only will need access to the same application each time. However, if a whole project is outsourced, the partner will need more access rights. Also the contracting can be different, for example if a partner is paid for every hour someone works or based on the performance/output. With

performance (or output) based contracting, organisations do not always know who exactly does the work, so this complicates things when access rights are required for example.

When comparing onshore and offshore sourcing, offshore will complicate boarding more because of the time and culture differences. Also when a line manager is working in the same office, working the same hours and speaking the same native language as the resource, they can communicate easier than if they would work on the other side of the world.

2.1.4. Conclusion

Table 2.2 summarizes all the context variables which were identified after conducting the literature research and by examining the Philips case. The factors which can make boarding complicated are large organisations which outsource time-hired and output based to many offshore partners where there is low trust between the organisations, a high extent of substitution and a high impact on competitive positioning and long-term strategy.

Context variable	Simple for boarding	Complicated for boarding
Size	Small organisations	Large organisations
Type sourcing	Insourcing	Outsourcing
Location	On-shore	Offshore
Trust	High trust between organisations	Low trust between organisations
Number of partners	Few partners	Many partners
Type of contracting	Only Time hired	Both Time Hired and Performance (Output) based
Access required	Access required for same applications	Access required for various applications
Type of applications	Homogeneous applications which use open standards for exchanging authentication and authorization data	Heterogeneous (old) applications which use different ways for exchanging authentication and authorization data or are not able to exchange it at all
Extent of substitution of service providers	Low extent of substitution	High extent of substitution
Strategic impact	Low strategic impact	High strategic impact

Table 2.2: Context variables summarized

2.2. Ways of using Identity and access management

As was stated in the introduction, onboarding is defined as the process of providing a new employee or a partner resource with all the required access rights and facilities to do a desired job. This means that an account needs to be created and maintained (identity), including access rights. This is done with identity and access management (IAM) which consists of two interrelated parts: identity management and access control. Identity management includes the whole identity life cycle such as creating, modifying and deleting user accounts. Access control includes authentication and authorization services, management of access control policies, enterprise-wide access management and a single sign-on (SSO) system (Luostarinen, Naumenko, and Pulkkinen, 2006). Figure 2.1 shows a high level Identity and Access management model made by Bradfort et al. (2014). The model shows the different types of users, the main functions of IAM (Identification, Authentication and Authorization) and examples of ERP systems. The model also shows the relationship with IT Governance. The IAM components will be discussed into more detail in the next sections.

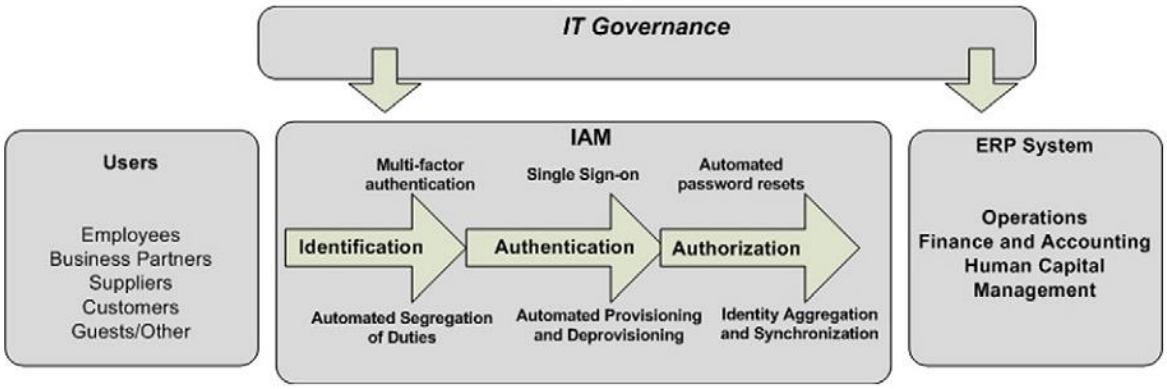


Figure 2.1: IAM High level model (Bradford et al., 2014)

Each application can have its own identity and access management module with its own user database and its own process to create, manage and delete those accounts. For large organisations with hundreds of applications, this situation would be a nightmare to maintain. It makes it more easy to have one centralized IAM system that is connected to all applications with one user database (identities), where users only need to authenticate once (single sign-on) to access all application and where there is a clear process of changing authorization. In this research, IAM will always be seen as a centralized enterprise-wide system.

For organisations there are several reasons to pay attention to identity and access management. First of all, it is a way to ensure security of applications and data. Secondly, it can reduce costs. For example, when people need to call the IT helpdesk to reset passwords while it can easily be an automated process the user can do himself. Another factor is that many enterprises, depending on their industry, need to be compliant to certain regulations such as HIPAA, SOX or the FDA. They put pressure on enterprises to have verifiable audit trails for information and physical access (Davis Kho, 2009). Identity and access management can also help with application integration (Witty, Allan, Enck and Wagner, 2003).

2.2.1. Identity Models

Jøsang et al. (2005) identified four types of identity management models which will be discussed in this section. The organisation that hires the service provider to do the outsourced work is called the client in these models. The models are made from the point of view of the worker of the service provider (who does that outsourced work).

Isolated identity management model

With isolated identity management (figure 2.2), both organisations use their own identity system. The worker will have a different identity and credentials for both organisations. Both organisation manage their own identities separately, so when a worker is onboarded to the client organisation, the client organisation will create a new identity on their own system. If the worker does outsourced work for several companies, he will have many credentials which he needs to remember. Another disadvantage is that the client organisation does not know the worker, for example if another name is given at onboarding, the real person might stay hidden which can cause problems for an audit for example. An advantage is that there does not need to be any trust between the organisations (Jøsang et al. 2005) (Jøsang and Pope, 2005).

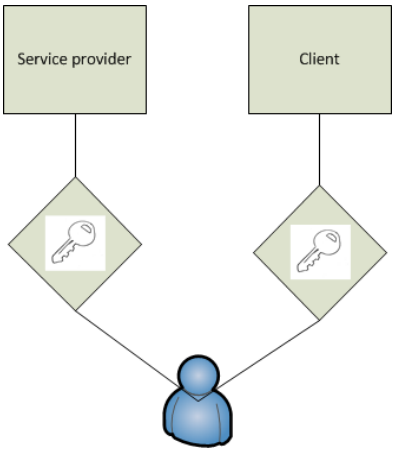


Figure 2.2: Isolated model

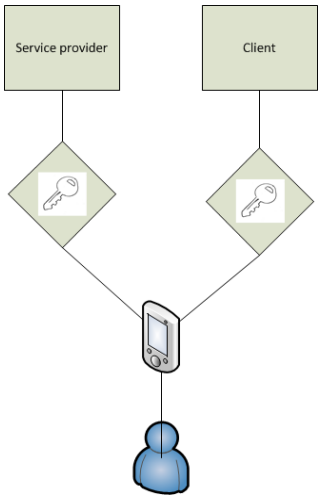


Figure 2.3: Personal model

Personal identity management model

Jøsang and Pope (2005) developed a personal (user centric) identity management model (figure 2.3) which is related to the isolated identity model because the identity management systems of the service providers are also isolated from each other. The difference however is that the user uses a Personal Authentication Device (PAD) on which the different credentials are encrypted and stored. This PAD can be a mobile phone or a laptop for example and it also needs its own password, but it brings its own risks like when a user loses the PAD (Jøsang et al. 2005) (Jøsang and Pope, 2005). The PAD can remember the different credentials, so there is an advantage compared to the isolated model in terms of usability since the worker does not have to do it.

Centralized identity management model

With centralized identity management (figure 2.4) there is one central identity management system used both by the service provider and the client. The user has only one credential for the centralized system to gain access. Who manages this identity management system needs to be agreed on by the service provider and the client. High trust is needed between the organisations since they both will use the same identity management system, for example as part of an alliance. (Jøsang et al. 2005) (Jøsang and Pope, 2005).

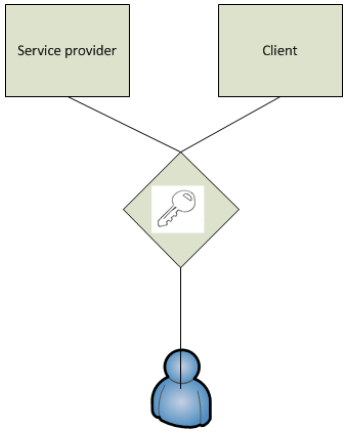


Figure 2.5: Centralized model

Federated identity management model

With federated identity management (figure 2.5), the identity management systems of the service provider and client can communicate with each other. The worker will only need one credential and can use it to access both the domain of the service provider and the client. It is used to allow cooperation on identity processes, policies and technologies across company borders. It facilitates secure resource sharing among collaborating partners in heterogeneous IT environments (Jensen 2012). Organisations will need to use a common data schema for the identity information which is exchanged. Standards and protocols need to be aligned, which becomes hard when multiple organisations are involved (Hommel et al., 2005). Sharing personal information is also a great concern for managing privacy, protecting data and complying with regulations (Maler and Reed, 2008). Trust is needed between the organisations, since their systems will be connected to each other (Jøsang et al. 2005) (Jøsang and Pope, 2005). Federated identity management can also be used within one organisation when there are different systems with its own identity and access management module to extend the user of single sign-on and reduce administrating tasks.

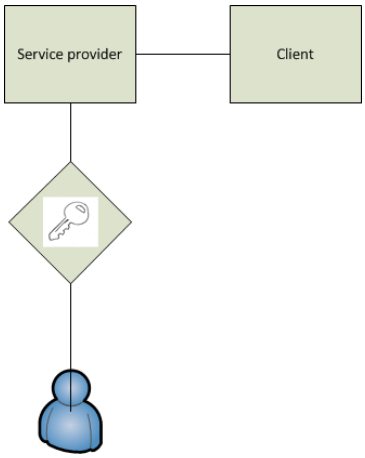


Figure 2.4: Federated model

Which model is best for an organisation is dependent of the situation they are in and what kind of architecture they have. When the client and service provider have long-term contracts on a big scale, federated identity management might be the best option. When there is only a small partnership as a one-time thing, isolated identity management will be the best fit. When the worker has many clients

with one-time contracts personal identity management will be the best option. Centralized identity management is might be the best fit when there is an alliance created between the two organisations as a joint venture.

2.2.2. Conclusion

In this chapter, I explained what identity and access management is. The isolated, personal, centralized and federated identity model were described, each showing a different way of using identity and access management with a partner. When applying the approach of improving the boarding process, these models can give insights if IAM was used in a proper way or if it is better to change it, depending of the organisation situation, its architecture and the relationship with its partner.

2.3. Identity and access management components

The important features of identity management for large enterprises will be determined by reviewing 14 identity management system vendors and combining them with the results of a report made by SURF. This is not meant to give an ultimate comparison between the vendors, but it will give a view of what vendors are capable of with the current technologies. The vendors are selected by searching the first four pages of google.com for "identity manager" in January of 2014. The vendors include big and small companies as well as open source and proprietary software. To make sure all the important players are involved, all missing leaders are added from the Gartner Magic Quadrant for user administration and provisioning 2012 and the Gartner Magic Quadrant for Identity and Access Governance 2012 plus the Gartner Magic Quadrant for Identity Governance and Administration 2013. Note that in 2013, Gartner consolidated the two magic quadrants from 2012. (Perkins, 2012a, Perkins, 2012b, Perkins et al., 2013). These Gartner quadrants and the results of this IAM vendor research are listed in Appendix B: Gartner quadrants & IAM vendor research.

SURF, a collaborative organisation for Dutch education institutes and research institutes which aims at breakthrough innovations in ICT, made a report comparing several IAM vendors. In their report they made a decomposition of the IAM functions and services (SURF, 2014).

Figure 2.6: Components of IAM (SURF, 2014)

As shown in figure 2.6, SURF distinguished functions that have a ten year or more history as Classical IAM and functions that are from the last few years as Modern IAM. I will not go into detail of Social logon because as SURF notes themselves, trust and security are not at a high level with social logon. It should only be used for (semi-) public information like with marketing purposes but not for IAM within an organisation (SURF, 2014). In this section, I will discuss these components by combining the SURF report and my own vendor research from Appendix B: Gartner quadrants & IAM vendor research.

2.3.1. Classical IAM components

Identity vault / life cycle management

The identity vault is a central repository where necessary information for account and role provisioning is stored and maintained. From here, the basic access rights are assigned in different systems. The life cycle management can be implemented on top of the identity vault. This defines the existence and state of a user account (SURF, 2014). In Figure 2.7 an example identity life cycle if shown.

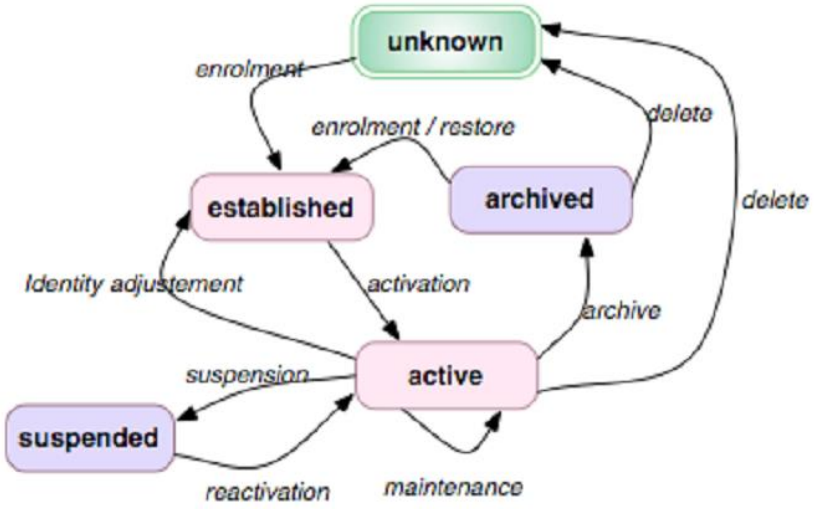


Figure 2.7: The identity lifecycle (ISO/IEC, 2011)

User provisioning

With user provisioning all applications and authentication databases are provisioned with account information in order to provide access to a user (SURF, 2014). User provisioning encompasses user account management; create, modify and delete user accounts and privileges. Ideally, user provisioning is done from a single point of administration (Witty et al., 2003).

Access control (Role and group assignment and Access request management)

Which systems are appropriate for a user and which access rights a user can get in a system is defined by the roles a person has or a group to which a user belongs. Assignment to a role or group is mostly done through an access request workflow. Line managers and application owners will have to approve requests by employees. Employees can also be automatically assigned to a group or role based on their job function or department (SURF, 2014).

Delegated administrator

A delegated administrator is used for user account management outside of the normal workflows. For example, administrators can create or delete user accounts and they can change the state of the account or perform self-service tasks on behalf of the user. Often these delegated administrators are part of the IT helpdesk (SURF, 2014).

Single Sign-On (SSO)

Single Sign-On is mainly a technical implementation that allows the user to log in only once to have access to all systems and applications without having to log in again. The biggest challenge is to integrate SSO over different platforms or organisations, for example desktop applications and cloud-based applications (SURF, 2014).

Strong Authentication
Secure authentication should be done in a secure way using 2-factor authentication or otherwise stronger authentication methods than just a username and passwords (SURF, 2014). 2-factor authentication means that the user needs to authenticate himself two times in preferably different ways. There are three categories of how the user's identity can be verified:

- Secrets, which is something the user knows. For example a password or security question. Using one security question is not very secure since many answers could easily be guessed (favourite colour), are known to other people (pet names), change after the user provides the answer (favourite movie) or are available in public records or social media (birthdays). This will become more secure when the user needs to answer at least three of secret questions and the company is more selective in which secret questions are allowed. Another way is to use a secret password, but when this password will not be used very often it might be forgotten (Hitachi ID, 2014).

- Tokens, which is something the user has. For example a smartcard, usb-token or a code is sent via e-mail or SMS to a mobile phone (Hitachi ID, 2014).

- Biometrics, which is something the user is. For example a fingerprint scanner on a laptop or facial recognition with a webcam (Hitachi ID, 2014).

To make a selection of what to implement, each organisation should make its own consideration of costs, security and ease of use.

User Self-service
To avoid unnecessary administrating or helpdesk costs and decrease service time, the user should be able to reset his own password and change basic profile information. A portal for self service could support this. Which way to implement the password resetting is dependent on the security requirements of the company. A security measure that could be taken for example is that a warning is send to all devices (SMS/e-mail etc.) when the password has been reset. So in case of an unidentified password reset, the user is alerted and can notify the system administrators to take the necessary actions (Hitachi ID, 2014).

Another use for self-service is that a user could be able to place his own access requests for applications. Although this could be limited for some secure applications where the manager needs to do this or where external users are prohibited. After submitting a request for access, the authorized approver will need to review the request and grand access (or deny access) (Hitachi ID, 2014).

Reporting and auditing
Reporting and auditing is useful to obtain insights in access rights, delegated administrator activity, self-service activity, provisioning and intrusion detection. Also when wrong data is entered in a system or there is a malicious attempt, it can always be traced back which user account was used (SURF, 2014).

2.3.2. Modern IAM components

Federation
As explained earlier at the Federated identity management model, federation is when two identity domains are connected to each other, for example to extend the use of single Sign-on. These domains can be within one company, for example two separate divisions, or they can be separate companies. When it are separate companies, they will need a high level of trust and it will only be feasible if they

work together extensively for a long time. For example when company A does a lot of outsource work for company B, both companies could connect their identity systems to each other so that the employee who does the outsourced work only has one account to login at both companies. In this example, company A is the identity provider which could work as follows (depending on the implementation): When an employee is doing work for company B, company A marks this in their identity system so it becomes synchronized to the identity system of company B. Company B can now set access rights to the account of the employee.

Federated Identity Management is also used for web and mobile applications (where the user is a consumer) or semi-public information so the user does not have to create a new account for each application but is able to login with one central account. In this case the identity provider sets up an API which software developers can let their application connect to check the credentials and retrieve information like the name of a person (SURF, 2014).

A note has to be made here that technically a federation is not a component of identity and access management, but more a way of using it. I still added it also in this component list because federated identity management has the ability to extend an identity and access management system and it can enable functions like single sign-on over multiple IAM domains.

Identity and Access Governance (IAG) (Identity and Access Intelligence)
Identity and access governance (also called identity and access intelligence) is a service that can retrieve access rights from all systems and present them for review. An example is shown in figure 2.8. This can create a comprehensive, real-time view of the multi-dimensional relationships between identities, access rights, policies, resources and activities across multitude of enterprise systems and resources. Access rights can be labelled by risk and a manager can get an overview of the access rights his employees have (risk, licence costs, etc.). Managers can also be alerted when access rights for their employees are changed. Identity and Access Intelligence can also help to detect unintentional errors and wilful fraud with access rights (violation of segregation of duty) (SURF, 2014).

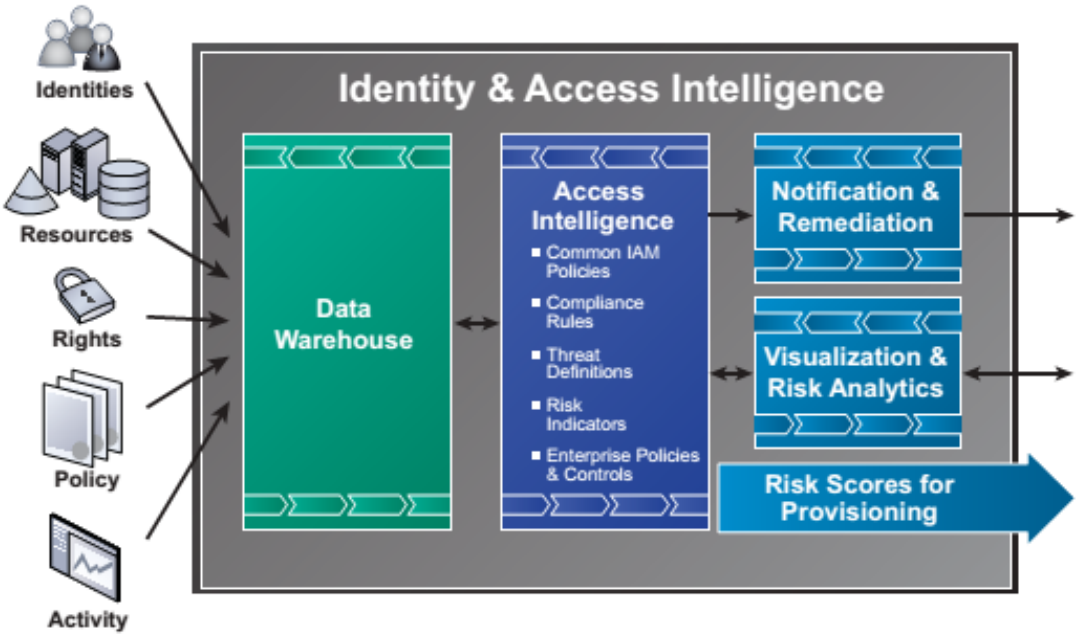


Figure 2.8: Components of an Identity & Access Intelligence system (Berents, 2013)

Risk-based access
With risk-based access, an organisation can make decisions on the behaviour of the users. For example when users try to access a system at unusual hours or from a strange location/country their access could be disabled until the user verifies it is really him to prevent hacker attacks (SURF, 2014).

Identity-based device management
Devices can also be linked to identity management systems to ensure life cycle management is effective for personal devices. This enables an organisation to define personal access rights for devices and it can also be used for risk-based access (SURF, 2014).

Cloud provisioning
When applications are running in the cloud, identity and access management and security is more complex because the IAM systems needs to communicate over the internet with these applications. Open standards like SAML should be used to provision and deprovision accounts and roles (SURF, 2014).

2.3.3. Conclusion
The important components of identity and access management that were identified by combining the vendor research and the SURF report are:

- Identity vault / life cycle management: a central repository where necessary information for account and role provisioning is stored and maintained;
- User provisioning: Creating, modify and delete user accounts;
- Access control: Delegating access rights;
- Delegated administrator: Account management outside the normal workflow;
- Single sign-on: Allows the user to login only once to access all applications;
- Strong authentication: A secure method for the user to login;
- User self-service: A portal for the user to do its own administrating tasks like resetting his password.
- Reporting and auditing: Gain insights in access rights, delegated administrator activity, self-service activity, provisioning, intrusion detection and traceability of user accounts;
- Federation: Connecting multiple IAM systems to each other;
- Identity and access governance: Use advanced statistics on access data to detect errors or fraud;
- Risk-based access: Prevent malicious attempts by disabling user accounts when accessed from unusual locations or at unusual times;
- Identity-based device management: Define personal access rights for individual devices;
- Cloud provisioning: Make use of open standards to communicate with cloud applications.

When applying the approach to improve the boarding process, these components can be used to solve issues or to add extra functionality to the IAM system. Since the technology of IAM systems develop rapidly, further research is needed to keep this list up to date.

2.4. Identity and access management barriers
Identity and access management is connected to many parts of an organisation thus it is also widely dependent of the situation and architecture of the organisation. Bradford et al. (2014) made a model for factors affecting Centralized End-To-End-Identity and Access Management, which is shown in figure 2.9. They call it ‘centralized IAM’ because they wanted to make a clear distinction with a separate IAM for every system. They call it ‘end-to-end’ because it incorporates automated tools for virtually every area of IAM such as tools that approve and provision users, assist with password resets and multi-factor

authentication, facilitate enterprise single singe on, provide for user activity compliance and monitor segregation of duties violations. Since these tools are already part of the IAM components as listed above and in section 2.2 I stated that IAM in this research is treated as Centralized IAM, this IAM and Bradford et al. Centralized End-To-End IAM is actually the same.

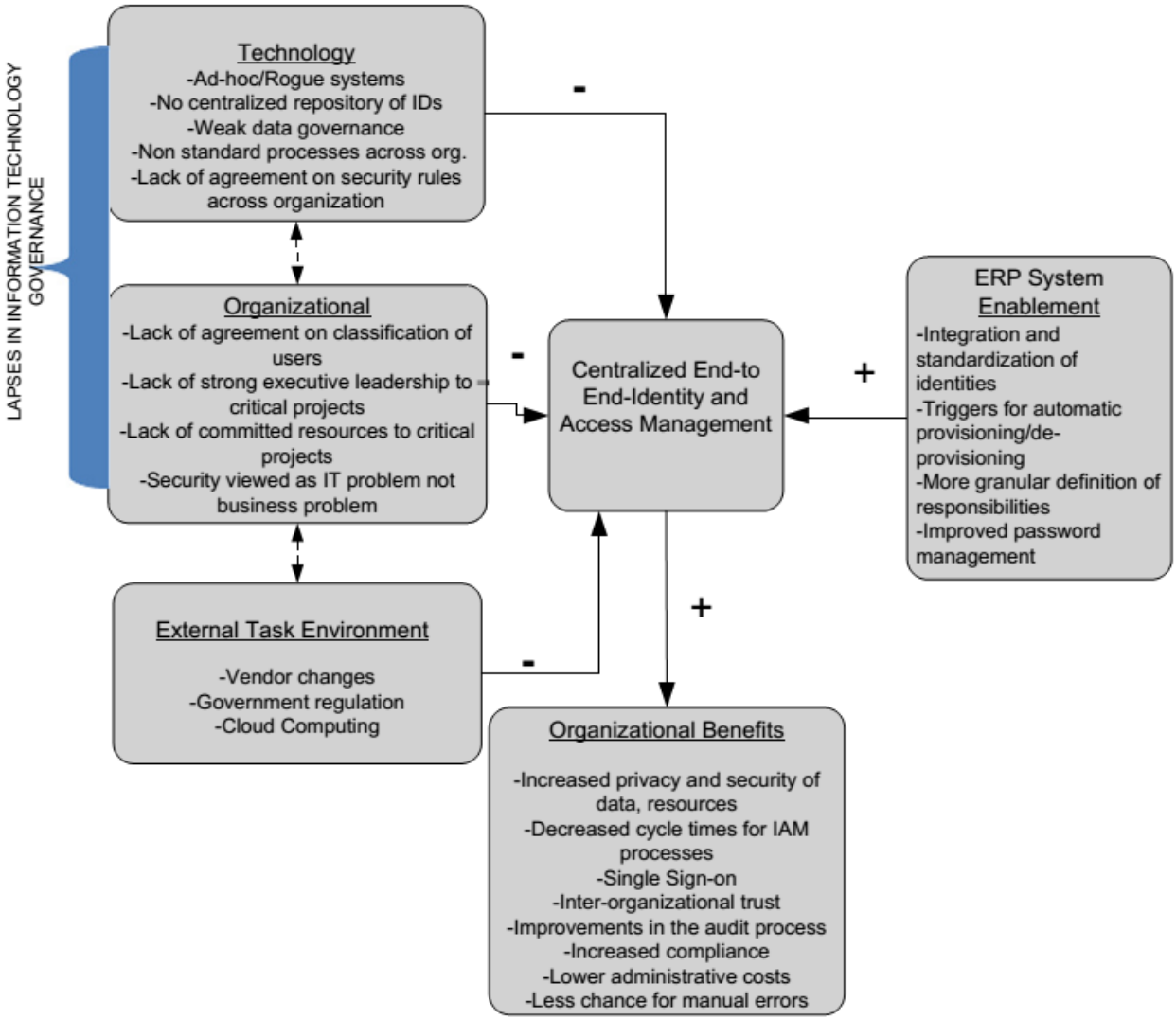


Figure 2.9: Barriers for IAM implementation (Bradford et al., 2014)

Bradford et al. (2014) used the Technology, Organisation and Environment (TOE) framework from Tornatzky and Fleischer (1990) as a base for the IAM model. The model states that both technology, organisation and external task environment factors can form a barrier to the implementation of an identity and access management system. These barriers are in accordance with the context variables which I identified in section 2.1, no contradictions were encountered.

According to Bradford et al., technology has this negative influence when there are ah-hoc/rogue systems that have their own identity systems. Also when there is no centralized repository of Ids, it becomes unclear where to store identity data and who is in control of it (weak data governance). This will lead to redundant, incorrect and incomplete data. Another problem is when there is a rapid growth of information systems resulting in non-standard processes across the organisation. Different employees

will do the same task in different way, leading to different results in data. There could also be a technological barrier when there is lack of internal agreement about basic security rules across the organisation (Bradford et al. 2014).

Also, the organisation itself can have negative influence on IAM according to Bradford et al. when there is a lack of agreement on classification of users, a lack of strong executive leadership to critical projects, a lack of committed resources to critical projects and when security is viewed as only an IT problem and not a business problem. Bradford et al. states that the lapses in IT Governance serve as a constraint for both these technology and organisation factors which have to be overcome in order to have a successful IAM.

Bradford et al. also note that the environment has influence on IAM. The IAM system needs to be flexible to cope with both changes in vendors/partners as well as changes in government regulations or auditors like data confidentiality, appropriate data access, firewall protection and more. When well implemented, IAM systems can even help with compliance towards auditors. As a last note, Bradford et al. see cloud computing as a challenge for IAM raising issues like integration and security.

When the above factors are overcome, there will be several benefits as a result according to Bradford et al. A primary benefit of IAM is increased privacy and security of data and resources and it provides a single point of support for declaring the identities of all users. Another benefit of IAM is decreased cycle times in managing the various aspects of IAM like the speed of provisioning and de-provisioning users can be greatly reduced as well as the speed of password resetting. Also, Single sign-on and other capabilities of provisioning appropriate access rights is a major benefit that also improves the user experience. The user will not be required to re-authenticate multiple times when they are doing various business tasks. Another benefit of IAM is increased compliance to IT audit processes by automating IAM controls making them insensitive for human error. IAM will also have a standard way of administering access allowing better traceability and accountability (who did what in the system using what user ID). Bradford et al. do not explicitly explain why inter-organisational trust is a benefit of IAM, but this could be derived from the reduced cycle time of inter-organisational processes and federated IAM (Bradford et al. 2014).

Bradford et al. see ERP systems as an enabler for IAM because ERP systems normally already have part of the IAM benefits in place. These benefits can include Integration and standardization of identities, triggers for automatic provisioning/de-provisioning, a more extended definition of responsibilities and improved password management (Bradford et al. 2014). A note has to be made that in large organisations not only the ERP systems but the whole architecture might enable these benefits. For example, if all applications use open standards for connecting to the identity and access management system, integration with a new IAM system will be easy. Although this could also be a barrier when the application do not use open standards and are hard to integrate with the IAM system (as was stated in section 2.1).

2.4.1. Conclusion

In this section, I continued the work of Bradford et al. by using their model in which they identified several technological, organisational and environmental factors that could form a barrier to the successful implementation of an identity and access management system. To improve identity and access management within an organisation, it needs to be checked if these barriers exist in that organisation and a solution should be found to overcome them.

2.5. Approach for improvement of the boarding process

By combining the literature research of the above sections and the experience from the Philips case, I developed an approach for improvement of the boarding process of external insiders in large organisations. This means the approach was built and improved iteratively, based on the experience of applying it at the Philips case. In this approach, the results from the literature research serve as handles to execute certain steps. The context variables (section 2.1) are used to identify the context and the ways to use IAM (section 2.2) and the IAM components (section 2.3) are used to solve issues in the design step. Also the barriers for the implementation of IAM (section 2.4) will be used in the design step.

The resulting approach has a series of steps which need to be taken as is shown at the model in figure 2.10. After the last step (evaluate), the approach can start again since it is a continues improvement cycle. As new technologies might have been developed, new issues might have arisen, goals could have changed or the organisation/environment changed, continuous improvement is required.

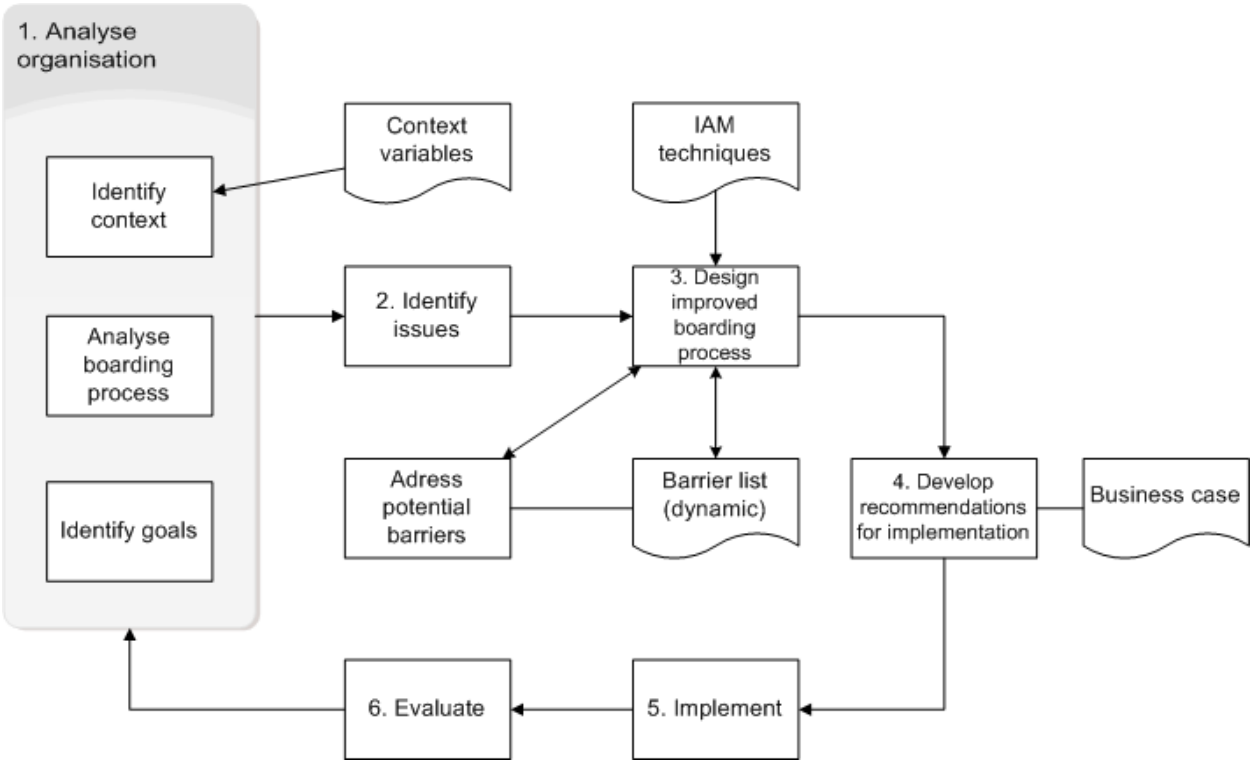


Figure 2.10: Model of the approach for improvement of the boarding process

Step 1: Analyse the organisation

The first step of the approach is the analysis of the organisation. This step is divided into three parts which can be executed simultaneously:

- Identify the context of the organisation, this is done by taking the context variables (section 2.1) and match them with the situation of the organisation;
- Analyse the current boarding process of the organisation by examining internal documents, attending meetings about this subject and interviewing employees and partners who are part of the boarding process;

- Identify the goals of the organisation that should be reached by adopting the improvements. Goals could for instance be to increase the speed of the boarding process, reduce costs, increase security or increase user satisfaction.

Step 2: Identify issues
The second step is to use the analysis from step one to identify issues regarding the boarding process. This can be issues related to the goals set by the organisation as well as issues that were identified with the boarding process analysis.

Step 3: Design an improved boarding process
The next step is to design the improved boarding process. This process is not limited to the design of one solution, but multiple scenarios could be designed that fit within the existing architecture of the organisation. The IAM techniques, which were identified in section 2.2 and 2.3, can be used to solve the issues of step two. In this step, the barriers for implementation of identity and access management (section 2.4) should also be addressed by analysing how the organisation will deal with them. Any issue in step two that can form a barrier to the implementation of identity and access management, should also be added to the barrier list (making it a dynamic list).

Step 4: Develop recommendations for implementation of the boarding process
In step four, the designs of the improved boarding process will be used to develop recommendations for the organisation to implement the boarding process by making a business case. In this business case, all different scenarios will be compared with their own costs, risks and benefits. Also a net return on investment allows the organisation to compare between different projects. Finally, the preferred solution from the business case is worked out in more detail to serve implementation.

Step 5: Implement
The next step contains the implementation of the preferred solution from the business case. All the involved employees and partners should be briefed about the new boarding process in advance. Then, an appropriate change management process should be initiated which is in line with the organisation's policy on implementing new business processes.

Step 6: Evaluate
In the final step, the new boarding process is evaluated to verify whether all goals were reached, all issues were solved and no new issues arose. This evaluation could be used as input for new improvements by applying the approach again from step one.

2.5.1. Conclusion
In this chapter, I have developed an approach to improve the boarding process of external insiders in large organisation. It consists of six steps which can be executed as a continues improvements cycle: (1) Analyse the organisation; (2) Identify issues; (3) Design an improved boarding process; (4) Develop recommendations for implementation; (5) Implement and (6) Evaluate.

The applicability of this approach is to structure the improvement process of the boarding process for large organisations. For example, an external consultant could use this approach to apply it on a client organisation. This approach is limited however to large organisations who already have a boarding process with a IAM system. For a new implementation of an IAM system, further research is needed.

3. The Philips case

[CONFIDENTIAL]

4. Conclusions

This research introduced a way to improve the boarding process of the external insiders in large organisations. Therefore, the goal of this research *to develop an approach to improve the boarding process of external insiders in a specific context* is accomplished. This approach was made by answering the research questions that were introduced in chapter one. In the first section of this chapter, the answers to these questions will be summarised. Section 4.2. discusses the validity of this research and in section 4.3 the limitations and further research are discussed.

4.1. Answers to the research questions

The first research question is *Which context variables can complicate the boarding process?* By analysing literature the following context variables were identified which can complicate the boarding process: Large organisations who outsource time-hired and output based to many offshore partners where there is low trust between the organisations, a high extent of substitution and a high impact on competitive positioning and long-term strategy.

The second question *What are the different ways of using identity and access management?* was answered by identifying four identity and access management models in literature: isolated, personal, centralized and federated identity model. Which model to use depends on the situation, architecture and partners of the organisation.

The next research question is *What are the important identity and access management components?* This question was answered by doing a vendor research online combined with a report from the SURF organisation. The important components include: identity vault/life cycle management, user provisioning, access control, delegated administrator, single sign-on, strong authentication, user self-service, reporting and auditing, federation, identity and access governance, risk-based access, identity-based device management and cloud provisioning.

The fourth research question continued on identity and access management stating *What are the barriers to implement identity and access management systems?* This question was answered by building on the research of Bradford et al. (2014). They identified a series of factors that have a negative influence on the implementation of identity and access management and a series of benefits that could be achieved by a successful implementation. In the Philips case, I identified two more barriers that were added to the list: Lack of documentation and Lack of control mechanisms.

The fifth research question stated *How can the Philips boarding process be improved?* This question was answered by applying the approach that was developed in this research. The final step in this case was describing a high level solution for Philips to improve its boarding process by creating a boarding service. Recommendations were provided with features for the boarding service which should be solve most of the issues that were identified.

The main research question of this research is ***How can organisations improve the boarding process of external insiders?*** By answering the previous questions, I was able to develop an approach to improve the boarding process of external insiders. This approach consists of six steps: (1) Analyse the organisation, (2) identify issues, (3) design an improved boarding process, (4) develop recommendations for implementation of the boarding process, (5) implement and (6) evaluate. To validate the approach, it is applied at the Philips case. The approach was modified and improved iteratively based on the experiences of applying it at the Philips case.

4.2. Validity

For the internal validity of this research, it is crucial that the design science research is done properly and completely. Gregor and Hevner (2013) made a design science research publication schema which describes all the parts that should be included in design research according to them. This publication schema is shown in Appendix G: Gregor and Hevner (2013) publication schema for a design science research study. Table 4.1 shows the sections of the design research publication schema and how each section is discussed in this research.

Section	This research
Introduction	Chapter one describes a clear problem definition and the goal and scope of this research.
Literature review	Chapter two discusses literature related to this research. However, only a limited amount of literature was found about inter-organisational onboarding.
Method	The research methodology is described in section 1.3.
Artifact description	The artifact of this research is the approach to improve the boarding process of external insiders which is explained in section 2.5.
Evaluation	In chapter three, the artifact (approach) was applied on the Philips case to show that the artifact is useful. However, not all steps of the approach were applied due to the limitations of the scope of this research. A note has to be made here that this case based validation might be biased because I applied the approach myself.
Discussion	In section 3.7, the conclusions of the applying the approach on the Philips case are discussed. Section 4.3 also discusses the limitations of this research.
Conclusions	Chapter four summarizes all conclusions of this research.

Table 4.1: Design research publication schema in this research

To prove the external validity of this research, the approach should be able to be applied on other cases and by different people. Different people could be external consultants for example. Due to the limitations of this master thesis, I was only able to apply the approach myself and on one case. Thus, it is uncertain if the approach can be applied on other organisations without modification and it is uncertain if external consultants are able to use this approach without special training. Further research is required to increase the external validity. Another way to increase the validity of this research could be having an expert panel discuss the approach and the findings of this research.

4.3. Limitations and further research

As stated before, due to the limited scope of this master thesis, not all steps of the approach were applied at the Philips case. In further research, the next steps of the approach could be continued as is explained in section 3.6. Only after implementing and evaluating the improved process, it can be determined whether the goals that were set by Philips were actually reached and all issues were solved.

This case was also limited to just four of the Philips IT partners, while Philips has over a hundred IT partners and even more non-IT partners. Further research could expand the Philips case by including more partners. This will probably make the case more complicated but it might introduce different barriers to overcome.

Because the approach was not completely applied at the Philips case, the validity of this research is also limited. In case Philips does not want to continue with this project, other ways to make the approach more reliable in further research would be to add an expert panel to validate the approach or to apply the approach to more organisations.

In the literature research, there was limited literature found about inter-organisational onboarding. Therefore, this research mainly focussed on identity and access management literature. In further research, more aspects of inter-organisational onboarding could be investigated. The results of this research might help with solving issues related to inter-organisational aspects in the 'design improved boarding process' step of the approach and it might identify different barriers for the implementation of IAM.

This approach focussed on the improvement of the boarding process of large organisations. It would also be interesting to apply the approach on small or medium sized organisations that are implementing their first IAM system. Some modifications to the approach will be necessary for this in further research. For example, the analysis phase of the current boarding process could be skipped and the organisation goals need to be more worked out in detail with clear requirements.

References

Berents, N. (2013) Identity and Access Intelligence: How big data and risk analytics will revolutionize IAM. Courion whitepaper.

Bradford, M., Earp, J.B. and Grabski, S. (2014) Centralized end-to-end identity and access management and ERP systems: A multi-case analysis using the Technology Organization Environment framework. *International Journal of Accounting Information Systems*, Volume 15, Issue 2, June 2014, pp. 149-165, ISSN 1467-0895, http://dx.doi.org/10.1016/j.accinf.2014.01.003.

Danti, A. (2014) Padlock and keyhole in a printed circuit. Digital illustration. http://www.shutterstock.com/gallery-54269p1.html Imagenumber 85035682 Accessed on August 2014. Used as front cover picture.

Davis Kho, N. (2009) The Changing Face of Identity Management. *EContent* 32.3 (2009): pp. 20-25.

Gregor, S. and Hevner, A.R. (2013) Positioning and Presenting Design Science Research for Maximum Impact. *MIS Quarterly*,Vol. 37: 2, pp. 337-355.

Gregor, S. and Jones, D. (2007) The Anatomy of a Design Theory. *Journal of the Association for Information Systems*: Vol. 8: 5 (2), pp. 312-335.

Hevner, A. R., March, S.T., Park, J. and Ram, S. (2004) Design Science in Information Systems Research. *MIS Quarterly* 28 (1).

Hitachi ID Systems Inc. (2014) Password Management Best Practices. http://hitachi-id.com/password-manager/docs/password-management-best-practices.html Accessed on January 2014.

Hommel, W., Center, L. S. and Reiser, H. (2005) Federated identity management in business-to-business outsourcing. *Proceedings of the 12th annual workshop of HP OpenView University Association (HPOVUA 2005), Porto, Portugal*, 2005, pp. 81–93.

ISO/IEC (2011) 24760-1:2011(E) Information technology — Security techniques — A framework for identity management — Part 1: Terminology and concepts. First edition December 2011.

Jensen, J. (2012) Federated Identity Management Challenges. *Seventh International Conference on Availability, Reliability and Security 2012*, pp. 230–235.

Jøsang, A., Fabre, J., Hay, B., Dalziel, J. and Pope, S. (2005) Trust requirements in identity management. *Proceedings of the 2005 Australasian workshop on Grid computing and e-research-Volume 44*, 2005, pp. 99–108.

Jøsang, A. and Pope, S. (2005) User centric identity management. *AusCERT Asia Pacific Information Technology Security Conference*, 2005, p. 77.

Luostarinen, K., Naumenko, A. and Pulkkinen, M. (2006) Identity and Access Management for Remote Maintenance Services in Business Networks. *Project E-Society: Building Bricks, Springer*, 2006, pp. 1–12.

Mabert, V. A., Soni, A. and Venkataramanan, M. A. (2003) The impact of organization size on enterprise resource planning (ERP) implementations in the US manufacturing sector. *Omega*, vol. 31, no. 3, pp. 235–246, Jun. 2003.

Maler, E. and Reed, D. (2008) The venn of identity: Options and issues in federated identity management. *Security & Privacy, IEEE*, vol. 6, no. 2, pp. 16–23, 2008.

Moe, N. B., mite, D. and Hanssen, G. K. (2012) From Offshore Outsourcing to Offshore Insourcing: Three Stories. pp. 1–10.

Nunes Leal Franqueira, V., van Cleeff, A., van Eck, P.A.T. and Wieringa, R.J. (2010) External Insider Threat: a Real Security Challenge in Enterprise Value Webs. *Proceedings of the Fifth International Conference on Availability, Reliability and Security (ARES'2010)*, 15-18 February 2010, Krakow, Poland. Pp. 446-453.

Perkins, E. (2012a) Magic Quadrant for user administration and provisioning. *Gartner research* http://imagesrv.gartner.com/media-products/pdf/quest/Quest_246546.pdf Accessed on January 2014.

Perkins, E. (2012b) Magic Quadrant for Identity and Access Governance. *Gartner research* http://www.gartner.com/technology/reprints.do?id=1-1DLZWHJ&ct=130115&st=sg Accessed on January 2014.

Perkins, E. Gaehtgens, F. and Iverson, B. (2013) Magic Quadrant for Identity Governance and Administration. *Gartner research* http://www.gartner.com/technology/reprints.do?id=1-1OR54B1&ct=131231&st=sg Accessed on January 2014.

Philips (2013). Philips Fourth Quarter and Annual Results 2012. http://www.newscenter.philips.com/main/corpcomms/news/press/2013/20130129_q4.wpd#.UR5AeKW4WIs Accessed on February 2013.

Rajiv Kishore, H. R. Rao, K. Nam, S. Rajagopalan, and A. Chaudhury. 2003. A relationship perspective on IT outsourcing. *Commun. ACM* 46, 12 (December 2003), pp. 86-92. DOI=10.1145/953460.953464.

Sabherwal, R. (1999) The role of trust in outsourced IS development projects. *Commun. ACM* 42, 2 (February 1999), pp. 80-86. DOI=10.1145/293411.293485.

SURF (2014) Connecting IdM services to SURFconext. http://www.surf.nl/binaries/content/assets/surf/en/knowledgebase/2014/report-idmaas-jan2014-def.pdf Accessed on June 2014.

Tornatzky L.G., Fleischer M. (1990) The processes of technological innovation. Lexington (MA): Lexington Books.

Walls, J.G., Widmeyer, G.R. and Sawy, O.E. (1992) Building an Information System Design Theory for Vigilant EIS. *Information Systems Research* pp. 36-59.

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

Wolfswinkel, J. F., Furtmueller, E. and Wilderom, C. P. M. (2011) Using grounded theory as a method for rigorously reviewing literature. *European Journal of Information Systems*, vol. 22, no. 1, pp. 45–55, Nov. 2011.

Zijlstra, H., (2013). Interview with Charel van Hoof, CIO Philips IT Delivery. *CIO magazine*, 9(1), pp. 121-124.

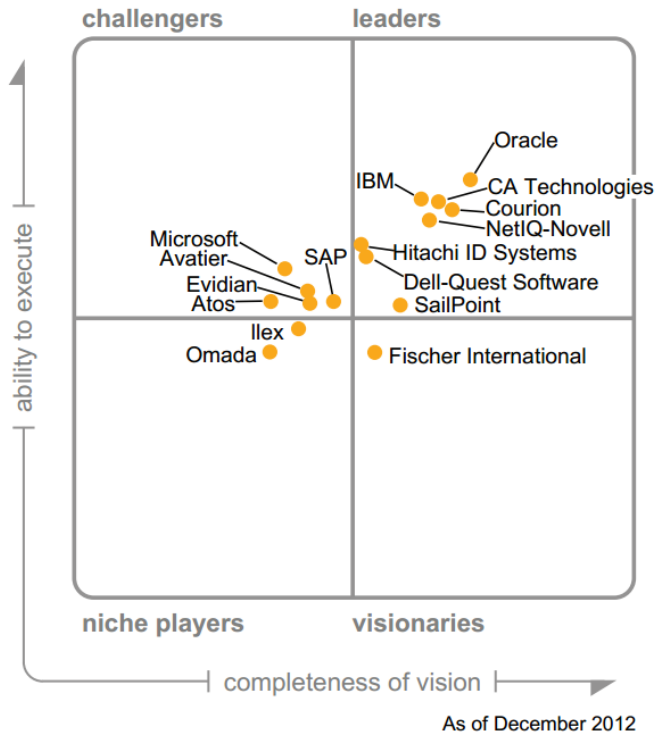
Appendices

Appendix A: Gregor and Jones (2007) eight components of a design theory
Appendix B: Gartner quadrants & IAM vendor research
Appendix C: Assignment form – output based
Appendix D: ONE IT Access request form
Appendix E: Offboarding checklist (PIC Bangalore example)
Appendix F: Changeboarding scenarios
Appendix G: Gregor and Hevner (2013) publication schema for a design science research study

Appendix A: Gregor and Jones (2007) eight components of a design theory

Component	Description
Core components	
1) Purpose and scope (the causa finalis)	"What the system is for," the set of meta-requirements or goals that specifies the type of artifact to which the theory applies and in conjunction also defines the scope, or boundaries, of the theory.
2) Constructs (the causa materialis)	Representations of the entities of interest in the theory.
3) Principle of form and function (the causa formalis)	The abstract "blueprint" or architecture that describes an IS artifact, either product or method/intervention.
4) Artifact mutability	The changes in state of the artifact anticipated in the theory, that is, what degree of artifact change is encompassed by the theory.
5) Testable propositions	Truth statements about the design theory.
6) Justificatory knowledge	The underlying knowledge or theory from the natural or social or design sciences that gives a basis and explanation for the design (kernel theories).
Additional components	
7) Principles of implementation (the causa efficiens)	A description of processes for implementing the theory (either product or method) in specific contexts.
8) Expository instantiation	A physical implementation of the artifact that can assist in representing the theory both as an expository device and for purposes of testing.

Appendix B: Gartner quadrants & IAM vendor research



Quadrant for user administration and provisioning (Perkins, 2012a)

Quadrant for Identity and Access Governance (Perkins, 2012b)

Quadrant for Identity Governance and Administration (Perkins et al., 2013)

Since all identity managers have the same goal (to manage identities), there will be quite some overlap of basic functionality which will be extracted first. After that, all extra functionality vendors use to distinguish themselves will be listed. All the vendor websites were accessed in January of 2014.

Basic functionality

- Identity vault: A central directory which stores all identities;
- User provisioning: The process of creating identities, editing them and deleting/disabling them;
- Monitoring and reporting: A dashboard to view statistics and being able to trace back users access;
- Single Sign-on: Enabling the user to only login once to access all application without having to login again;
- Access governance: Granting users access to applications, mostly used with roles (RBAC);
- User self-service: a self-service portal where users can login to do several administrating tasks like editing their profile or resetting their password.

CA: http://www.ca.com/us/identity-management.aspx

- Automate account provisioning and removal;
- Ensuring people only have access that is appropriate in their job function;
- Governance (roles, audit reports and dashboards);
- Patented analytics for new roles.

Courion: https://www.courion.com/

- Identity and Access Intelligence (IAI): how to see and make sense of the complex relationships between users' identities, their access rights, their access activity, the resources they access and the policies governing that access;
- Maintain compliance;
- Reduce Risk.

EmpowerID: http://www.identitymanagement.com/

- Multi-Tenant Extranet Directory (Managing External Identities);
- Governance, Risk & Compliance (GRC);
- Group Management and Role-Based User Provisioning;
- Mobile identity management.

Hitachi: http://hitachi-id.com/identity-manager/

- Automated User Provisioning and Deactivation;
- Delegated Security Administration;
- Report on Users and Entitlements;
- Automated Connectors and Human Implementers.

IBM:
https://www.ibm.com/developerworks/community/wikis/home?lang=en#!/wiki/Tivoli%20Identity%20Manager http://www-03.ibm.com/software/products/en/subcategory/SWI20

- new security perimeter with controls to manage, enforce, and monitor user entitlements and access activities;
- Safeguard mobile, cloud and social interactions;
- Prevention of insider threat and identity fraud;
- Simplify identity silos and cloud integrations (Directory services);
- Deliver intelligent identity and access assurance (real-time user activity monitoring and anomaly detection).

Microsoft Forefront: http://www.microsoft.com/en-us/server-cloud/products/forefront-identity-manager/default.aspx#fbid=vZMSy3aO7OS

- Integrated provisioning of identities, credentials, and resources;
- Automated, codeless user provisioning and de-provisioning;
- Automated approval workflows;
- Rule-based analytics of access;
- In-depth reporting and auditing.

NetIQ (old Novell): https://www.netiq.com/products/identity-manager/advanced/

- Comprehensive support for security and compliance;
- Automated provisioning for easier administration;
- REST API support for seamless integration with user-friendly interfaces;
- Cloud-ready identity management service;
- Comprehensive activity reporting for SaaS applications.

OpenIAM: http://www.openiam.com/

- Professional Open Source;
- Audit and Compliance;
- Low integration effort;
- Compliance with industry standards;

Oracle: http://www.oracle.com/us/products/middleware/identity-management/overview/index.html

- Comprehensive Web Access Management, Web Single Sign-On, Identity Propagation, and Federation;
- Mobile and Social Sign-On;
- Real-time External Authorization;
- Adaptive Access and Fraud Detection;
- Context aware computing– automatically collect, propagate, and leverage identity and device context for personalization and authorization across web, web services, and application tiers;
- Identity Governance.

Quest (Dell): http://www.quest.com/identity-manager/ http://software.dell.com/products/identity-manager/

- Automated Provisioning;
- Self-Service Lifecycle Identity Management;
- Business Process Management;
- Compliance-ready IAM Stance;
- Auditor reporting.

RSA Aveksa (EMC): http://www.aveksa.com/

- Mobile;
- Cloud.

Sailpoint: http://www.sailpoint.com/

- Identity Governance (compliance controls and audit reporting);
- Provisioning with self-service;
- Access Management to mobile devices;
- Identity Intelligence;
- IAM for cloud environment (IAM-as-a-service (IDaaS)).

Tools4Ever: http://www.tools4ever.nl/

- Cloud Identity and Access Management;
- Audit & Compliance;
- Real Use Dashboard (monitoring);
- Active Directory Tools.

Appendix C: Assignment form – output based

[CONFIDENTIAL]

Appendix D: ONE IT Access request form

[CONFIDENTIAL]

Appendix E: Offboarding checklist (PIC Bangalore example)

[CONFIDENTIAL]

Appendix F: Changeboarding scenarios

[CONFIDENTIAL]

Appendix G: Gregor and Hevner (2013) publication schema for a design science research study

Section	Contents
1. Introduction	*Problem definition, problem significance/motivation, introduction to key concepts, research questions/objectives, scope of study, overview of methods and findings, theoretical and practical significance, structure of remainder of paper.* For DSR, the contents are similar, but the problem definition and research objectives should specify the ***goals*** that are required of the artifact to be developed.
2. Literature Review	*Prior work that is relevant to the study, including theories, empirical research studies and findings/reports from practice.* For DSR work, the prior literature surveyed should include any prior design theory/knowledge relating to the class of problems to be addressed, including artifacts that have already been developed to solve similar problems.
3. Method	*The research approach that was employed.* For DSR work, the specific DSR approach adopted should be explained with reference to existing authorities.
4. Artifact Description	A concise description of the artifact at the appropriate level of abstraction to make a new contribution to the knowledge base. This section (or sections) should occupy the major part of the paper. The format is likely to be variable but should include at least the description of the designed artifact and, perhaps, the design search process.
5. Evaluation	Evidence that the artifact is useful. The artifact is evaluated to demonstrate its worth with evidence addressing criteria such as validity, utility, quality, and efficacy.
6. Discussion	*Interpretation of the results: what the results mean and how they relate back to the objectives stated in the Introduction section. Can include: summary of what was learned, comparison with prior work, limitations, theoretical significance, practical significance,* and *areas requiring further work.* Research contributions are highlighted and the broad implications of the paper's results to research and practice are discussed.
7. Conclusions	*Concluding paragraphs that restate the important findings of the work.* Restates the main ideas in the contribution and why they are important.