Aalto University
School of Economics

Evaluating financial benefits of an identity management solution CASE Logica

Information Systems Science

Master's thesis

Eetu Heino

2011

Department of Business Technology
Aalto University
School of Economics

Aalto University
School of Economics

Evaluating financial benefits of an identity management solution – CASE Logica

Master's Thesis

Eetu Heino

Spring 2011

Faculty of Information and Service Management

Approved by the head of department of _____

___/___ 2___ and awarded the grade _____

Abstract

Research Objective and Method:

Main purpose of this study is to discover different financial benefits that identity management solution can deliver and to build a ROI model for identity management solution. The ROI model will show yearly cash flows and calculates widely used financial measures, such as NPV, IRR, ROI and payback time for Logica's identity management solution RIMA. Therefore this study adopted a constructive approach which aims to solve a relevant problem by constructing a model. First a vast literature was conducted in order to gain solid understanding on identity management solution's financial benefits. These benefits are then implemented into the ROI model and the model is tested by using fictional case company X's numbers.

Summary of the Findings

The benefits of identity management solutions were identified and a conceptual model of these benefits was constructed. The conceptual model identified that identity management solution can deliver intangible benefits that are revenue increasing and tangible benefits that are cost reducing. On the base of the conceptual model the ROI model for measuring and illustrating identity management solutions financial benefits was constructed. The ROI model identifies following areas that deliver savings: provisioning, self-service, SSO, compliance, IT-security, licenses and improved efficiency. The ROI model was tested in order to prove that it delivers desired outputs according to the assumptions and input parameters.

Keywords:

Return on investment, ROI, identity management, identity and access management, information security, IAM, IdM,

Table of Contents

Table of Figures

1 Introduction

1.1 Background

In today's business environment employees need to access various applications and services in order to do their job. However, it can be very challenging to provide employees with correct accounts and accesses in timely manner. Furthermore, managing multiple identities, accounts and credentials can be very burdensome and time consuming task for employees and for the companies as well. In addition, ever increasing competition and legislation requirements force companies to re-evaluate their information security standards.

Companies are implementing identity management solutions which automate and streamline companies' identity management through employees' whole life cycle. According to IBM (2007, 5) "Identity management is the process of managing information used to identify users, control user access, determine user privileges and delegate administrative authorities". Earlier identity management solutions were clumsy, expensive and implementation projects could take years. However, identity management solutions have evolved to be more agile and are nowadays offered as a standardized service which shortens implementation time from years to weeks or months. Furthermore, identity management solutions are now available also for smaller companies thanks to relatively small initial investment and Software as a Service (SaaS) model. SaaS allows companies to use software over the internet without installing it on their own machines and therefore it is a flexible and cost efficient choice.

Cost savings are one of the drivers behind IT system implementations but also legislation requirements are bringing identity management solutions into the frontline of companies' IT investments. According to Computerworld (2006) compliance and legislation requirements are justifying identity management projects which may not otherwise be economically feasible. Therefore cost savings and legislation pressure combined with information security issues make identity management very current topic. Furthermore, according to Cser & Penn (2008) "The identity management — or identity and access management (IAM) — market will grow from nearly $2.6 billion in 2006 to more than $12.3 billion in 2014 (including revenues from both products and implementation services)."

The field of identity management is relatively young and it is evolving all the time and there are only few academic studies from the business point of view. Most of the articles and publications concentrate on the technical side of identity management or authentication models but not on the identity management as a whole. However, large identity management solutions vendors, such as Oracle and IBM have published non-academic white papers and redbooks which describe business side as well the technical side of identity management. Furthermore, economical feasibility of identity management solutions is not widely discussed in academic studies and there are not well crafted financial calculation tools for identity management solutions. Large vendors of identity management solutions have their own tools but they are not usually publicly available.

This study explores benefits of identity management system from the financial point of view and therefore the purpose of this thesis is to develop a return on investment (ROI) model for identity management solutions. This model is done for Logica which is a business and technology service company, employing 39,000 people across 36 countries. Logica offers service called RIMA (Rapid Identity Management Assembly) which is identity management as a service. Nowadays companies are requiring more proof of their IT-investments' economical feasibility and the ROI model will answer to this requirement. The ROI model will present financial benefits of identity management solution in an easily understandable form. This model is not limited only to calculate ROI performance measure but also other financial measures, such as Net Present Value (NPV), Internal Rate of Return (IRR) and payback period. These financial measures will be discussed more deeply in subchapter 4.3. Furthermore, ROI model shows cash flows from different years and calculations will be visible for the customer so customer can better evaluate the results of the ROI model.

1.2 Research Problem

In this Chapter I will present my research problem and main research question. The main goal of my thesis is to construct a ROI model and provide answer to the following research question:

How to measure and illustrate identity management solution's financial benefits?

Managers require IT investment to show positive Net Present Value (NPV) and clear results instead of being only obligatory "black-box" applications. Times are over when IT department could invest large amount of money into IT-systems without proving their financial benefits for the company. However, it can be challenging to measure cost savings or revenues which identity management solution generates. These possible sources of revenues and cost savings will be closely examined in the following chapters and the ROI model will be constructed. The constructed ROI model can then used in selling situations to illustrate different cost saving possibilities related to identity management solutions.

Purpose of the ROI model to be constructed is not only to produce one financial measure, such as ROI, but rather act as a guide line for the user in identity management investment. The ROI model will illustrate the most important tangible benefits that identity management solution can deliver and calculate yearly savings. In addition, the ROI model will calculate widely used financial measures, such as NPV, IRR, ROI and payback time and support different calculations with illustrative graphs.

Identity management solution will generate also a large amount of intangible benefits that cannot be easily converted into dollars or Euros. I also explore these intangible benefits in the following chapters and take them into account when constructing a conceptual model in Chapter 3. However, these intangible benefits will be excluded from the ROI model because they cannot be converted into monetary measurements in a feasible manner.

The ROI model can be used for illustrating financial benefits in an easily interpreted form for the customer. Therefore this study has a pragmatic orientation and the model constructed is specially designed to support Logica's identity management service. However, because all the identity management solutions deliver similar benefits, the constructed ROI model can be at least partly utilized for evaluating also other identity management solutions.

1.3 Limitations and Scope of Research

The research concentrates on the tangible financial benefits of identity management solutions and will not dive deep into intangible benefits that identity management solutions can deliver.

However, these intangible benefits will be notified and discussed but the main emphasis is on more easily measurable tangible benefits.

The research will explore identity management system's benefits on a general level but the ROI model will be especially designed to support Logica's RIMA solution. However, as mentioned before benefits of RIMA and other identity management solutions are very similar and it is possible that the ROI model developed can be used as a guide line also for assessing other vendors' products financial benefits. Furthermore, goal of the ROI model is to be an easily usable guide for estimating financial benefits of identity management solutions. Therefore, it will not take every possible variable into account, but rather tries to identify the most important sources of cost savings. This will give a better overall picture about the benefits and logic behind the ROI model and it is easier for the customer to use.

As every model, also the ROI model introduced in this thesis is very dependent on the values that the customer provides and thus it is crucial that the input data is as accurate as possible. However, formulas will be clearly stated, so the customer can easily see how the inputs are utilized. Furthermore, assumptions made in formulas or in calculation logic are based on literature review and experienced identity management consultants' advice.

The constructed ROI model will be tested by using fictional case company X's parameters in order to see that the ROI model is able to deliver desired outputs. When testing the ROI model, emphasis will be in functionality testing and not in accuracy testing. In other words, I will be testing that the constructed ROI model is able to deliver desired outputs, such as financial measures, graphs and cash flows. Therefore, testing is not trying to measure accuracy or validity of the ROI model's outputs. Testing the validity of the ROI model's results cannot be done because of the limited time scope of the Master's thesis.

1.4 Research Method and Structure

As mentioned before, the objective of this study is to produce a financial measurement model for evaluating identity management solution's financial impacts. Therefore I will be utilizing constructive research method. According to Kasanen, Lukka & Siitonen (1993) constructive

approach can be used for problem solving by constructing models or procedures. Furthermore, Kasanen et al. (1993) list six stages that constructive approach consists of:

1. Find a practically relevant problem which also has research potential.
2. Obtain a general and comprehensive understanding of the topic.
3. Innovate, i.e., construct a solution idea.
4. Demonstrate that the solution works.
5. Show the theoretical connections and the research contribution of the solution concept.
6. Examine the scope of applicability of the solution.

As stated this thesis will follow the constructive approach and is organized to six Chapters. First, introductory Chapter 1 shortly described importance of the identity management solutions, purpose of this study and established a practically relevant problem. In Chapter 2 a vast literature review is conducted in order to gain a general understanding of the identity management and all the issues related to it. The literature review is written in a form which will keep the financial perspective present through different subchapters. After establishing solid understanding about tangible and intangible benefits of identity management solution, I will construct a conceptual model in Chapter 3. This conceptual model will be an upper level description of the identity management solution's financial impacts. Furthermore, the constructed conceptual model will be used in Chapter 4 when creating the ROI model that measures and illustrates financial impacts of an identity management solution to a company's performance. In Chapter 5 the ROI model will be tested in the context of fictional case company X and all the results will be analyzed. Finally in Chapter 6 the ROI model will be discussed and further research suggestions will be presented.

2 Literature Review

In order to fully understand functionality, benefits and challenges of identity management solution, wide literature review is conducted. First, I will go shortly through functionalities of the identity management system. Second, I will present key drivers and benefits behind identity management solution implementation. Third, I will take a look into challenges related to identity management systems and their implementation. Fourth, I will present identity management from information security perspective which includes access management, passwords and password policies. Finally, I will introduce concept of Single Sign-On (SSO) and self-service interface which are solutions that closely link into identity management.

2.1 Identity's Lifecycle Management

Purpose of this subchapter is to give a comprehensive picture about identity management lifecycle which includes all the identity related procedures which take place during employee's career in a company. Benantar (2006) defines identity as follows: "An identity in computing reflects real-life entities in that its level of granularity can be coarse (such as representing an organization; a group of people) or can represent a specific individual or a particular computing device". Furthermore, identity presenting specific individual has to be uniquely linked to the individual by a unique attribute. This kind of unique attribute can be, for example, employee number. Identity management is all about managing employee's identity through its whole life cycle. Life cycle begins when a new employee enters to the company and ends when the employee leaves the company. In this subchapter I will give a short overview to the operations related to identity's life cycle management.

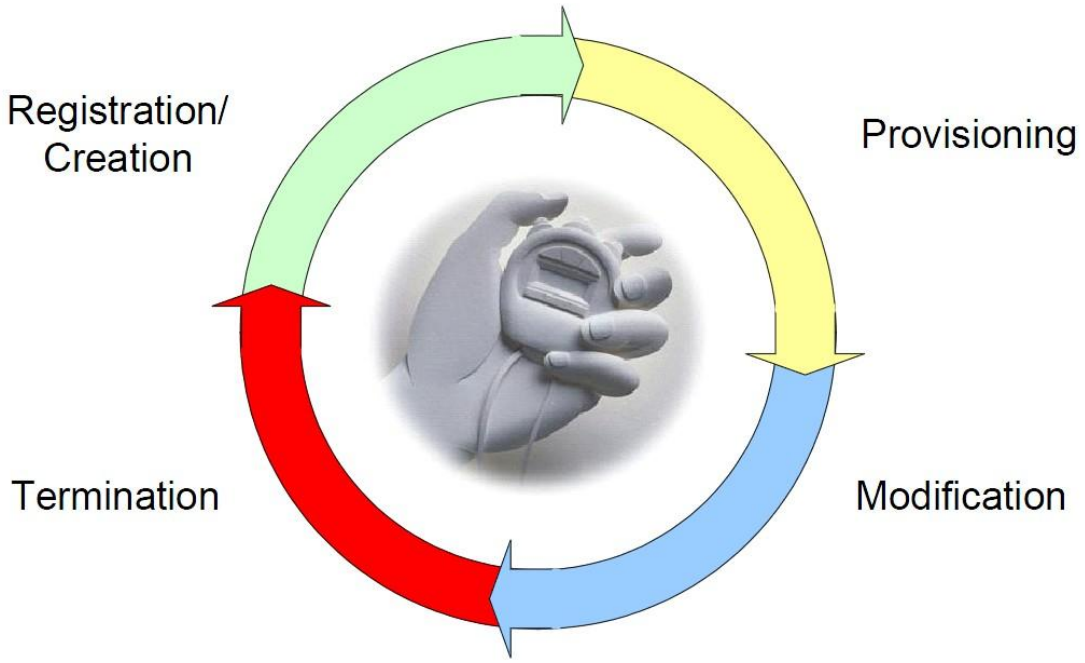


Figure 1: Life cycle management overview (Buecker, Filip, Palacios & Parker, 2009)

Figure 1 illustrates the main procedures that employee's identity will go through during his/her career in a certain company. Basically registration and creation means creating user's identity into HR-system and identity management system. Provisioning, on the other hand, means that accounts are created automatically after they have been approved. Modification can be granting additional accesses or revoking existing ones. Finally, identity's lifecycle ends in termination where all the accesses are revoked, accounts suspended and finally deleted. Termination usually takes place when an employee leaves a company. All of these operations will be discussed separately in the sections 2.1.1- 2.1.4. In addition to operations presented in Figure 1, identity lifecycle needs to be managed and this can be done through recertification and lifecycle rules. Recertification and life cycle rules are handled in the section 2.1.5.

2.1.1 Registration and Provisioning

Registration and provisioning will take place when a new employee enters to a company and he/she needs user IDs and passwords for accessing different systems. Furthermore, a new

employee needs also physical resources, such as mobile phone and laptop. Identity management system can use provisioning to create the required accounts automatically for the new employee. However, if automatic creation of certain accounts is not possible identity management solution can collect required approvals and inform administrator to add accounts manually. Workflow, on the other hand, is an automated process for doing manual processes, such as requesting approvals or sending email automatically and it will be discussed more deeply in subsection 4.2.2.2. Accounts provisioned or created by using workflow can give access to different applications or services but are not limited to them. Mobile phone, for example, can be considered as an account attached to employees user ID. Moreover, when every physical asset is an account under employee's identity, it is easier to manage these assets and collect correct assets from the employee when he/se leaves the company.

Identity management can create all the accounts under one identity and therefore one credentials grant access to needed systems but all the account creation processes cannot be automated. Peterson, Smedegaard, Heninger & Romney (2008) argue that different systems may have different policies for user ids and passwords but identity management system helps to combine all the different systems under one username and password. They also point out that because of technical limitations all the account creation cannot be automatic and some of the work has to be done manually. Therefore, workflows mentioned in the previous paragraph can be used to ease manual work as much as possible. To conclude, automated account provisioning, using workflows and combining different user accounts under one identity are benefits that identity management solution can deliver and they can also be source of huge monetary savings for the company.

2.1.2 Modification

Employees change their roles in the organization time to time and modification is used to change their accounts to correspond the current need. An employee may get promoted or assigned into a special role; these actions will probably require changes in access permissions. Permissions may be added, deleted or they may remain the same, based on the present need of an employee.

In addition to changing access rights for the employee, also employee's personal information may change and it needs to be updated into the managed systems, such as phonebook or Active Directory (AD). According to Peterson et al. (2008) hardest part of managing multiple identities is to deliver and implement change requests to all the applications and services under person's identity. Main advantage of identity systems is that change request needs to be done only once in identity management system and all the managed systems will be updated either automatically or manually. Another important point that Peterson et al. (2008) mention is that change request may be based on transferring an employee from external worker to an internal employee. They explain that identity management system will streamline this transfer process because only little modification to employee's parameters is needed. In other words, almost all of the employee's personal information will usually remain the same and only business related attributes, such as title and organization needs to be changed.

2.1.3 Suspend and Restore

Suspending and restoring accounts are related to disabling employee's certain account, at least for temporarily, and restoring this account back to employee's use. Suspend operation can target to the whole employee or only to certain account of an employee. When an employee is suspended all his/her accounts are suspended as well and this way also access rights are disabled. If only, for example, sales account is suspended, employee may lose only access to certain sales software. Suspending an employee can take place, for example, when an employee is leaving the company. Usually all the accounts are suspended before they are terminated permanently.

Restoring accounts or an employee, opposed to suspending, is enabling disabled accounts or making a suspended employee active again. An employee may need to be suspended for a certain time period because of maternity leave, lay off or other business or personal reason. When the employee returns to work, his/her accounts can be easily restored and she/he will have the same accounts and accesses as she/he did before leaving the company. Therefore, restoring procedure can save a lot valuable working time for the employee because employee can avoid fuss related for applying different accounts and accesses. Furthermore, employees' time savings can be interpreted as monetary savings for the company.

2.1.4 Termination

Termination occurs when the employee leaves the company and all the accounts and accesses under the employee's identity should be removed. Furthermore, the employee's identity should also be removed. Removing all the accounts and accesses is very crucial from the information security point of view but also from the compliance point of view. If accounts are not deleted in a timely manner, they may be used for retrieving valuable information or performing illicit acts against the company. Furthermore, these "extra" accounts will prevent company to follow compliance regulations. Legislation requirements will be discussed more in section 2.2.2. In addition to information security threats, unused accounts can cost money for the company in a form of licenses. Therefore it is very essential to delete all the unneeded accounts.

Peterson et al. (2008) list four types of common exceptions or deficiencies during user account review:

- Generic account
    - Account that is shared and have no precise accountability.
- Outdated account
    - Account with permissions that are no more appropriate based on employee's current needs or role.
- Stale account
    - Account that has not been used for a very long time.
- Orphaned account
    - Account that remain in the system although the user has been deleted.

All the mentioned account types above may impose risk of decreased performance for the company in a form of costs, weakened information security and failing to follow compliance requirements. However, recertification and lifecycle rules can help administrators to find

these types of accounts listed above. These recertification and lifecycle rules will be discussed in the next section.

2.1.5 Recertification and Lifecycle Rules

The main objective of recertification and life cycle rules is to keep the managed identities updated with correct access permissions and delete unneeded permissions. Removing access permissions usually realizes by deleting or suspending a certain account. Recertification and life cycle rules utilize operations presented in earlier sections to manage employee's accounts and identity.

Recertification is a process for obtaining information about who has access to what. Furthermore, recertification is used to ensure that the employees have a valid need for their accounts and access rights. When the recertification process is performed, it can send to an employee a message asking whether the certain accounts are needed. The Employee needs to reply to this message during a certain period of time in order to maintain his/her accounts. (Buecker et al. 2009) Recertification frequency can be adjusted to correspond with company's information security policy or recertification can be processed on the demand. Recertification is an effective audit tool that can save a lot manual work that would be otherwise needed. This decreased amount of manual work can be interpreted to a financial saving when constructing the ROI model.

According to Buecker et al. (2009) life cycle rules define life cycle operations which will take place as a result of a predefined event. Predefined event might be, for example, certain date or password expiring. These operations can be, for example, sending mail to an employee or modifying employee's accounts. Buecker et al. (2009) state that life cycle rules are especially efficient in automating often occurring administrative tasks. These life cycle rules can do automatically routine administrative processes and administrators can concentrate on more important IT issues. Buecker et al. (2009) list few examples of life cycle rules which will make their potential more clearer:

- Password policy compliance checking

- Notifying users to change passwords before they expire
- When a contract expires, identifying all accounts belonging to a business partner or contractor's employee and revoking their access rights

As we can see, life cycle rules can automate many operations that would otherwise have to be done manually. For example, suspending all the user accounts when a contract expires is a great advantage for the company from information security point view as well from the business efficiency point of view. However, usually only a portion of all accounts can be automatically suspended because implementing fully synchronization through all the systems can be very expensive and hard. However, as mentioned before identity management system can send an email to an administrator and notify which accounts needs to be manually suspended and when.

Subchapter 2.1 took a deeper look into different functionality inside the identity management solution especially related to identity's life cycle management. Different identity life cycle operations start from creating a person, provisioning accounts, modifying these accounts and finally terminating all the accounts and removing the person from the identity management system. Lifecycle rules and recertification, on the other hand, are tools that can be used for identifying who has access to what and ensuring that employees have only the accounts that they need for doing their job.

2.2 Key Drivers and Benefits behind Identity Management Implementation

In this subchapter I will concentrate on the key drivers behind identity management solution and the benefits that a well implemented identity management solution can deliver for the companies. All the key drivers are not only benefits and also, for example, legislation requirements can be a reason for implementing an identity management solution. Figure 2 below well illustrates all the drivers behind identity management solution: cost reduction, business performance, operational efficiency, regulatory compliance and risk reduction.

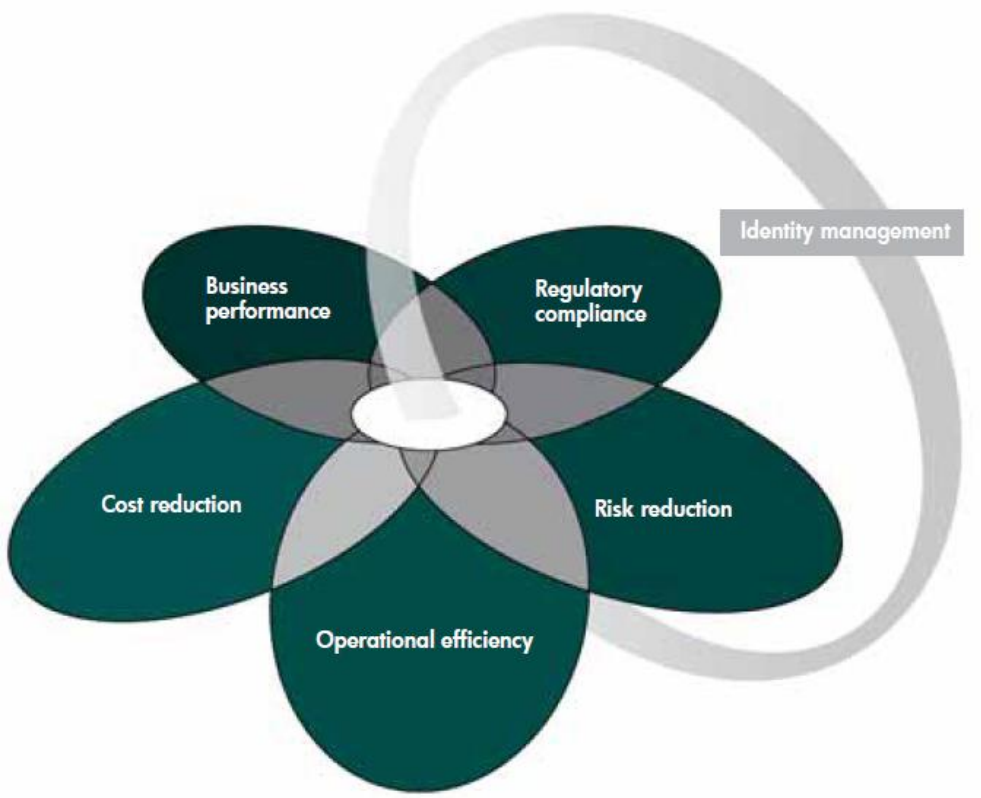


Figure 2: Business drivers behind identity management (HP, 2004)

This paragraph will shortly present the drivers shown in the Figure 2. Cost savings are only one of the factors pushing companies to implement an identity management system. Cost savings consist mainly from working time saved, improved information security and decreased load for service desk. Furthermore, identity management system can increase company's operational efficiency and business performance. This is achieved by eliminating employees' unproductive time and by enabling the company to react faster to changes in its business environment. However, more and more companies are forced to implement an identity management system because of legislation requirements. Legislation can require companies to keep a close track on who can access and on what data. Furthermore, information security risks can be greatly reduced when an identity management solution is in place. These drivers mentioned will be discussed in more detail in the following three sections 2.2.1-2.2.3.

2.2.1 Cost savings, Operational Efficiency and Business Performance

According to Kho (2009) cost savings and efficiency are usually oldest drivers when companies are considering new IT systems. Operational efficiency will be increased when the employees do not have to manage several user IDs and passwords. According to IBM (2007, 3) "A significant percentage of calls to IT help desk are typically related to password and access issues". Therefore implementing identity management's user self-service tool for password reset will take a huge workload away from the service desk. Self-service tool allows employees to reset their password or change personal information without contacting to the service desk. This way a company can gain cost savings and service desk can concentrate on more critical issues instead of routine tasks. Also Computerworld (2006) notes that when a case company (15000 user accounts) rolled out a password self service application help desk calls dropped from more than 6,683 to 534 per year. This drop in service desk load is very radical and indicates that password reset self-service may deliver very considerable savings. However, service desk load could have been most likely decreased also by educating employees in password management.

When an employee has many passwords and user IDs he/she will be probably using very simple passwords or write them down. Habit to use weak passwords and writing them down will decrease company's information security significantly. These kinds of actions might be consequences of password fatigue which many user experience because they have to remember several different credentials. Also Jøsang, Zomai & Suriadi (2007) identify identity and password fatigue for the users who has to access many different services with different credentials. They also point out that users will routinely forget passwords which will increase workload for the service desk and prevent working because the needed resources are not accessible. Furthermore, password fatigue is a problem which decreases employee's capability to properly control and protect their digital identities. Passwords and password policies are discussed more deeply in section 2.4.1.

According to a 2004 Gartner report estimated cost for resolving a password problem by calling to a service desk is between $10 and $31 dollars (Kho, 2009). Even if the cost is

"only" $10 dollars per call it will cumulate great savings when multiplied by thousands of incidents. Furthermore, an employee is probably able to solve the password problem faster with password self-service compared to the time it takes to find the service desk number, call to the service desk, wait for someone to answer and wait for the password to be changed. By using self-service to reset a password, the employee saves working time and money for the company. I will return to the ROI of identity management in Chapter 3 where the conceptual model for identity management is constructed. Also self-service interface and its advantages will be discussed more intensely in section 2.5.2.

Benantar (2006, 69) argues that "Automation of account provisioning on the managed services and systems is an important element of reducing cost in enterprisewide identity management. " Basically automatic provisioning means that certain widely used accounts, such as email and windows accounts, can be automatically created when a new employee enters into a company. Provisioning reduces significantly manual work needed and assures that a new employee will have required accesses at the very first working day. Furthermore, automated provisioning can increase company's business performance by enabling company to react more quickly to changes in its business environment. According to HP (2004) it is critical to ensure that employees are provisioned with correct access rights in real time and this way company can concentrate on more important business issues. Provisioning and provisioning policies were discussed more deeply in section 2.1.1.

This section introduced how identity management solution can save costs, improve operational efficiency and enhance business performance. Business drivers presented in this section are relatively easily transformable into monetary values and will be used when constructing the conceptual model in Chapter 3 and the ROI model in Chapter 4.

2.2.2 Legislation and Regulatory Compliance

In addition to improvement in financial performance and better IT security, identity management solution implementations are heavily driven by legislation and regulatory compliance. One of the key drivers behind identity management, at least in the U.S, has been

Sarbanes-Oxley act (Sarbox or SOX). According to Sarbanes-Oxley Act of 2002 (2002) purpose of Sarbox is "To protect investors by improving the accuracy and reliability of corporate disclosures made pursuant to the securities laws, and for other purposes".

"SOX applies to all public companies in the U.S. and international companies that have registered equity or debt securities with the Securities and Exchange Commission and the accounting firms that provide auditing services to them" ("Sarbanes-Oxley," n.d.). This means that Sarbox is affecting on many US based companies and also some international companies and is therefore creating a need for the identity management systems. On the other hand, companies that are not affected by SOX do not have an urgent need for identity management solution from the legislative point of view.

Sarbox has been published in a year 2002 but still many more recent articles express the need for identity management solutions to show compliance. According to Computerworld (2006) it is very hard or even impossible for companies to produce compliance reports which are required by the Health Insurance Portability and Accountability Act (HIPAA) or Sarbox. Kho (2009) agrees that HIPAA and SOX regulations are placing pressure on enterprises. Furthermore, Kho (2009) notes that companies probably have to be even more transparent in the future. This assumption about companies' transparency creates increasing need for the identity management solutions.

Sarbox sets certain requirements for the companies but does not explicitly explain how these requirements should be fulfilled. According to Sarbanes-Oxley Act of 2002 (2002) section 404 (a) requires companies' annual report:

> (1) state the responsibility of management for establishing and maintaining an **adequate internal control** structure and procedures for financial reporting; and
>
> (2) contain an assessment, as of the end of the most recent fiscal year of the issuer, of the effectiveness of the internal control structure and procedures of the issuer for financial reporting.

However, Sarbox does not explicitly define what these "adequate internal controls" mean, or what systems should be used in order to achieve adequate internal controls (Sun Microsystems, 2004).

This paragraph will provide a list created by Sun Microsystems which provides insight to issues that a company needs to consider if it wants to be Sarbox compliant. However, this list only presents Sun Microsystems opinion and is not the only way to deal with Sarbox but can be seen as a good guideline. Sun Microsystems (2004, 4) list the requirements that companies need to fulfill in order to be Sarbox compliant:

- Access rights in distributed and networked environments should be effectively controlled and managed.
- Companies should be able to remove terminated employees' or contractors' access to applications and systems immediately.
- Companies should be able to confirm that only authorized users have access to sensitive information and systems.
- Control over access to multiuser information systems should be put in place — including the elimination of multiple user IDs and accounts for individual persons.
- The allocation of passwords should be managed, and password security policies must be enforced.
- Appropriate measures must be taken to prevent unauthorized access to computer system resources and the information held in application systems.
- Periodic assessments and audits of access rights and privileges must be performed.

List above seems to be a catalog of identity management system features and that is why it is important to note that Sun is a big identity management solution vendor. Furthermore, because Sarbox does not define precisely what companies need to do in order to be compliant, of course identity manager vendor lists all the identity management system's features that might be related to showing compliance. However, companies have been struggling in order to be Sarbox compliant and identity management solutions are offering sufficient methods for showing compliance.

This section took a short overview into legislation requirements, especially Sarbox, which will motivate companies to invest in identity management solutions. Legislation issues discussed in this section relied heavily on references and citation because legislation is not in

the core of this research. However, this section was important in order to better understand legislative drivers behind the identity management solutions.

2.2.3 Information Security

Identity management solutions can increase company's information security in many ways. Control over employee's accounts and access rights can be increased and security policies can be efficiently implemented through work flows. Furthermore, information security policies can be centrally managed and implementation is immediate. The biggest threat for the companies is not necessarily attacks and hacking attempts coming outside the company but rather attacks and hacking attempts coming from inside the company. According to Gartner 70 percent of attacks on IT systems come from insiders (Viega & Messier 2004). This illustrates well why it is vital to have internal security policies updated in real time. Furthermore, all the unnecessary accounts existing in the information systems expose company to information security risks. Recertification process and lifecycle rules described in section 2.1.5 helps in removing these unnecessary accounts from the system.

Information security return can be hard to measure and it is many times measured by assessing possible risk. Identity management solution can help companies to minimize information security risk with reasonable cost. Information security issues will be discussed in more detail in subchapter 2.4 IT Security.

2.3 Challenges Related to Identity Management Solutions

Identity management systems offer solution to many problems but there are also many challenges in implementing an identity management solution. Purpose of this subchapter is to explain possible challenges and pitfalls that companies may confront when dealing with identity management implementation. First, I will explain challenges related to defining business processes and roles, which can be the biggest challenge. Second, I will describe technical challenges related to lack of unique identifiers and incorrect data in old information

systems. Third, I will concentrate on possible information security concerns that may relate to implementing an identity management solution. Finally, I will explain shortly other possible challenges related to identity management solution implementation.

2.3.1 Defining Business Processes

Business processes need to be clearly defined before implementing an identity management solution. If the company's business processes do not support efficiently business needs, identity management solution cannot help the company. When a company automates rubbish it gets automated rubbish and that is not probably the wanted situation. According to Jaferian et al. (2009) it is a classic situation in the companies that they buy a tool and think it will solve all the problems. Furthermore, company's own processes, access administration and identity lifecycle should be carefully mapped out before going down to technical side of identity management solution (Jaferian et al. 2009). After company has have mapped out its business processes, identity management can support and automate these processes in order to increase company's overall performance.

The most cumbersome business process to define is the roles and accesses related to them. Usually identity management systems support Role Based Access Control which means that employees can be provisioned with accounts according to their organizational role in the company. RBAC will be explained in more detail in subsection 2.4.2.1. Many identity management solutions rely on role based access control and therefore roles should be carefully defined.

According to Buecker, Karl & Perttilä (2008) implementing a basic user role with, for example, network and e-mail account can stimulate the RBAC design process. Therefore, implementing even only a basic user role can save a lot of money and time for the company. Furthermore, it is not obligatory to implement all the roles in the company at once but one role at a time during a longer time period. Basically every automated role will make company's business processes more efficient. According to Molloy, Chen, Li, Wang, Li, Bertino, Calo & Lobo (2008) there are role mining tools that can help role defining process but usually problem with these tools is that they do not always identify semantic meanings

behind the roles. In other words, these role mining tools cannot identify true business roles behind different sets of access rights analyzed from the access controlling systems.

2.3.2 Lack of Unique Identifier and Incorrect Data

Companies may have many data repositories containing employee information but they might be lacking mapping and standardization between these repositories. It is hard to implement an identity management system if there is no standardization on how the identities are stored in the data repositories (Jaferian et al., 2009). Usually it is problem if the data repositories do not have a unique identifier for each employee that links identities from different repositories to the same employee. This kind of unique identifier is typically employee number which is unique for each employee in each data repository.

According to Computerworld (2006) data cleaning and mapping is a challenge and needs to be done before data can be brought together into a common identity repository. Data cleaning can mean, for example, setting information in different repositories into a common format. Data mapping, on the other hand, can mean creating a link between different data models in different repositories. Therefore, data cleaning and mapping can be costly which needs to be taken into consideration when planning an identity management system implementation. Furthermore, data might also be incorrect in some repositories and needs therefore to be cleaned. The Identity Project (2007) argues that inaccurate data can be due to a manual work included when data is typed into the system. Implementing identity management system can decrease manual work needed and ensure that in the future data will be more accurate.

2.3.3 Information Security Concerns

Companies want to keep their information security controls inside the company's firewalls and it can be challenging for them to buy identity management as a service. Every company takes their information security issues seriously and understand how devastating it can be if possible information security threats, such as data leakage or data theft realize. According to

Kho (2009) companies are nervous about how their employee data, contractor data and even customer data is handled outside of their own system. Furthermore, to convince companies about Software as a Service (SaaS) concept vendors need to provide customer companies access and visibility, so that identity management system is not only a "black-box" application (Kho, 2009). However, emerging trend in identity management is to offer identity management as a service. SaaS is more flexible for the customer and also cheaper because the customer does not need to keep a vast pool of technical people and hardware in place. All the resources saved will improve company's financial performance.

According to The Identity Project (2007) heterogeneous IT infrastructure and disparate systems may pose a big challenge for identity management implementation. Furthermore, Jaferian et al. (2009, 53) argue that "deploying the loosely integrated components of the IdM system was a challenge". In addition, it is expensive and requires a lot of effort to configure and link different systems together. However, The Identity Project (2007) points out that sometimes it is wise from information security point of view to keep sensible data away from the centralized identity management. This approach is quite questionable because inside the identity management system can be done measures to ensure that only authorized people has access to the data. The identity project (2007) argues that finance department could be one of the critical systems that could be kept outside of the central IDM administration in certain situations.

2.3.4 Other Challenges

In addition to challenges mentioned earlier, The Identity Project (2007) lists following ones:

- Limited Consensus on Defining "Identity Management"
  - Different decision makers understand concept of identity management differently thus it can lead to misunderstandings in identity management related projects.
- Limited De-provisioning
  - De-provisioning problems arise when users are granted extra access rights that are

not normally granted to users belonging to the similar role. Therefore when the extra access rights are not needed anymore, de-provisioning of them is easily forgotten.

- Lack of Formal Procedures
  - Many institutions have formal policies regarding ICT management. However, it is common that these policies do not cover all the identity management related areas or policies are not enforced through whole organization.

- Lack of Common Standards and Central IDM Administration
  - Different departments and groups may have different policies and standards in use. Furthermore, these departments may have dedicated administrators and this leads to a decentralized IDM administration.

- Lack of Policy of Reuse of identifiers
  - When an individual leaves the organization his/her credentials is retained for certain period of time. However, when he/she rejoins organization, there is a danger that he/her is provisioned with brand new credentials. Furthermore, his/her old credentials may be provisioned accidentally to some other individual.

- Lack of Adherence to the Code of Practice for Information Security Management
  International codes of practices are over run by the organization's internally developed policies and practices. This can lead to lack of confidence in the IdM data records integrity and inadequate IdM related risk assessment procedures or audits.

Defining business processes and roles remain probably the biggest challenge when considering identity management system implementation. It should be remembered that company can reap significant benefits from the identity management solution without implementing fully automated RBAC. Furthermore, technical challenges may arise from heterogeneous IT architecture, poor data quality and lack of unique identifier for individual employee. All the challenges can be overcome but there should always be careful cost/benefit evaluation conducted before advancing with identity management implementation.

2.4 IT Security

In this subchapter I will take a closer look into two information security issues that I find very important from the identity management point of view: Passwords and access management. First I will discuss about passwords and password policy. Multiple passwords has been causing headache for the employees and they tend to write them down which is a significant information security risk. Identity management provides solution to this problem but also importance of well planned password policy needs to be emphasized. It is very critical that an employee has a strong password if all systems can be accessed with single credentials. After password policy section, access management will be discussed. Access management can be seen as one of key concepts related to identity management and needs to be defined and discussed. Furthermore, deeper look into role based access control (RBAC) model will be taken.

2.4.1 Password Policy

Employees use passwords everyday in their jobs and at home when logging into websites, emails, computers and other services. However, many employees are probably using too weak passwords, do not change their passwords often enough or use same password to all services. Employees' weak password policies create a new information security challenge for the companies. Companies can educate and create efficient password policies in order to improve their information security. Identity management solution can decrease amount of passwords to one. In this way employees are most likely more willing to create a strong password because they only need to remember one password.

Password policy plays a critical role in identity management system from information security point of view. Single Sign-On (SSO) and one credentials for every application can deliver huge advantages in many ways. Basically SSO enables user to log on all the needed applications and services by typing his/her credentials only once. SSO will be discusses more deeply in section 2.5.1. However, in wrong hands these "all access" user ID and password

may have disastrous consequences. Therefore, use of only one credentials to all the systems can be seen as a double-edged sword.

According to Summers & Bosworth (2004) passwords are often the first and only line of defence. Summers &Bosworth (2004) also note that typically many users choose trivial or the default passwords and passwords are not frequently changed. It is an evident security risk if employees are using default passwords or easily guessable ones. Companies can prevent use of trivial passwords by forcing employees to use numbers, capital letters and special characters in their passwords. This can be easily implemented with identity management solution's centralised password policy management feature. Summers & Bosworth (2004) argue that another solution to overcome employees that select easily guessed passwords is to assign passwords randomly. However, randomly assigned passwords are hard to remember and many employees will write them down.

Florêncio & Herley (2007) argue that users choose passwords with an average bit strength 40.54 bits and majority of users uses only lower case letters in their password. The more bits there are in the password the harder it is to crack. In other words, using numbers, small letters, capital letters and special characters in the password increases password's strengths significantly. Florêncio & Herley (2007) define that less than 30 bits passwords are weak and over 60 bits passwords are strong. However, study did not take into consideration account passwords of strength less than 20 bits. It is worrying that users are conducting passwords which only consist of lower case letters because using also, for example, capital letters would increase their passwords security tremendously. However, as mentioned before identity management solution's central password policy management can ensure that employee's passwords are strong enough.

A good password policy is essential for company's information security and in this paragraph is presented characteristics of a good password policy. Password policy's main objective is to ensure that all employees have secure passwords all the time. Summers & Bosworth (2004) list some of the features of strong passwords and password policies:

- Alpha, number and special characters must be mixed up.
- Do not use "dictionary" words.

- Minimum length of six-ten characters.
- Maximum password age of 45-60 days.
- Do not write any password down.
- Do not share your password.
- Publish and EDUCATE the users of the password policy.

Company has to observe that do the employees follow password policies and that they are aware of them. In addition to forcing password policies centrally, companies can educate employees to create hard guessed passwords which are easy to remember. Summers & Bosworth (2004) offer following example "May the force be with you" becomes Mt4%wU where the F in force becomes 4 and the b in be becomes %." This kind of password is easy to remember from the famous film quote but still it is classified as a strong password. Creating a more complex password than wife's or children's names is obligatory. It is very important to explain employees why certain password policies are in use because this way they can really understand the benefit of the password policy

Passwords can be seen as the basic defence line of the company and companies should have password policies to ensure that employees' passwords are strong enough. This is extremely important when a company is using an identity management solution and each employee has only one user ID and one password. Enforcing well planned password policies through all the company's systems combined with education will help employees to improve whole company's information security.

2.4.2 Access Management

In this section I will explain basics of access management and its connection to identity management. Identity management and access management are very closely connected together and their combination is referred with term IAM. Controlling access is one of the key elements in a company's information security

Paavilainen (1998) suggests that access control should be based on authorization, authentication and access control. These methods ensure that only authorized employees have access to the certain resources. Authorization is used to define who has the right to use certain system or premises. In authentication, on the other hand, employee's identity is verified and lastly in access control is checked that only authorized employees can access to the certain resource. Implementing this kind of access control to all systems and premises is basis for information security. Identity management systems follow these three access control principles. Employees are authenticated before they are authorized with accesses. Usually line manager conducts authentication and authorizes access by requesting access for his/her subordinates. Furthermore, when employees try to access certain resource access is controlled and only authorized employees will be granted with access.

In addition to physical access control it is even more important to control employee's rights to access company's databases. According to Cronkhite & McCullough (2001) employees represent the greatest threat of wrongful use or even theft of data. Cronkhite & McCullough (2001) also point out that most instances of computer crime are inside jobs. Data loss, theft and misuse are serious threats for information security and companies should take action to prevent these unwanted events. Sometimes employees may share sensitive information accidentally and purposelessly to those who should not have access to this information. To prevent these kinds of information security risks companies should limit access to databases which contain sensitive information and also educate employees about use of sensitive information. Identity management solution can be used to ensure that employees do not have any excess accesses but only the ones they need for doing their job. However, if information security breaches occur, identity management system can tell who had access to a certain system and who had approved this access for the employee.

Segregation of duties is an identity management solution's feature that can improve company's information security and access control efficiency. Segregation of duties is about ensuring that single employee will not have combination of accesses that is not feasible from information security or business point of view. Main purpose for segregation of duties is to prevent fraud or errors (Buecker et al. 2009). Employee, for example, cannot be assigned to roles that allow him/her to request himself more access rights and also approve them.

Therefore roles allowing requesting accesses and roles allowing approving the same request needs to be separated so that same individual cannot be assigned to both roles simultaneously.

Well implemented Role Based Access Control (RBAC) is the most efficient access control model from the business point of view. However, other access control schemes include, for example, mandatory access control (MAC), discretionary access control (DAC), user-based permission systems and access-control lists (Windley, 2005). In the next section I will finally concentrate on roles and RBAC which are key concepts in identity management.

2.4.2.1 Role Based Access Control (RBAC)

In this Chapter I will describe in more detail Role Based Access Management (RBAC) which is one the key features in identity management solutions. Business processes define certain roles for employees and accesses that employees need for performing their role efficiently. In identity management system these roles include certain access rights to certain applications and resources. Employees are either assigned to zero, one or many roles which all grant different sets of access rights for the employee. In addition to RBAC, this subsection also explores features of request based provisioning and hybrid approach.

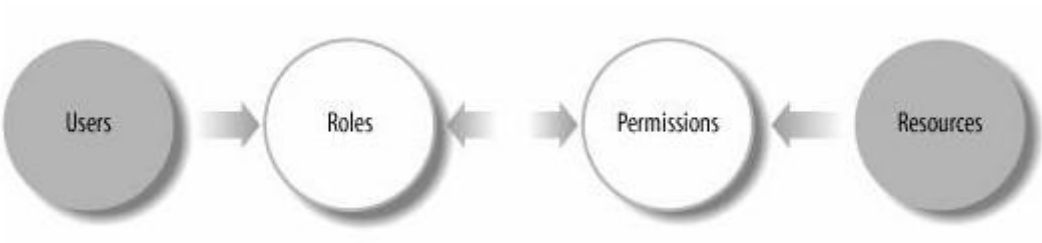


Figure 3: Permission hierarchy for role-based access control (Windley, 2005)

Figure 3 illustrates permission hierarchy in RBAC model. Employees are assigned to certain roles according to their position in organization. Usually this role is based on information in HR-system. Furthermore, resource owner can grant permissions for certain accounts that are attached to certain roles. In other words, roles include certain accounts that grant access to

certain resources. Therefore employee belonging to a role will have access to a certain resource with certain permissions.

When business processes and roles are well defined from the business point of view, technical implementation of these roles into identity management system is a relatively easy task. However, as discussed in section 2.3.1 defining business processes and roles can be very hard and cumbersome task which might be even a barrier for implementing RBAC. According to Computerworld (2006) defining business processes may take many times longer than the technical configuration itself. However, there are role mining tools which can help the process of defining roles.

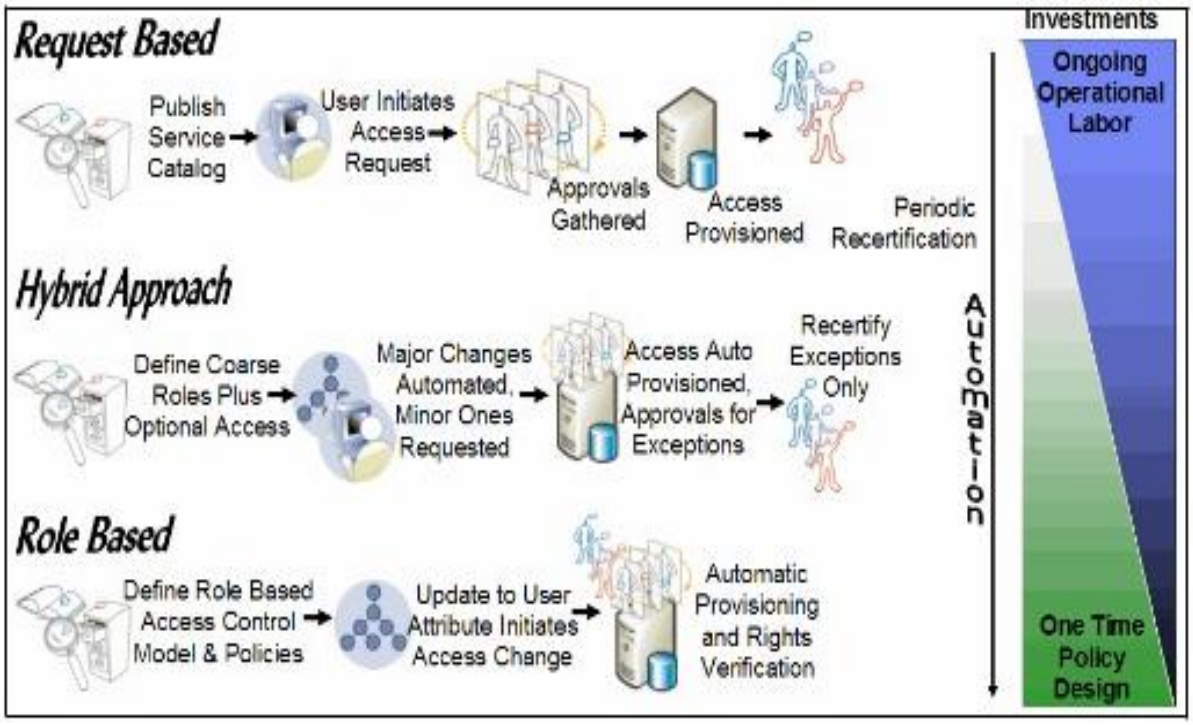


Figure 4: Identity management provisioning models (Buecker et al. 2009)

Figure 4 illustrates well differences between request based, hybrid approach and role based account provisioning models and also the automation related to these processes. All of these approaches are enabled by the identity management solution and the most appropriate model should be selected according to the business needs.

According to Buecker et al. (2009) request based access provisioning requires that the user requests certain access which is validated by approvals and also audited by recertification.

Different aspects of recertification were discussed in more detail in section 2.1.5. In the request based access model each access is requested individually and no roles are involved in the process. In the request based provisioning automation is low and need for operational labor is very high.

Buecker et al. (2009, 44) argue "Using role-based provisioning, business can automate and accelerate the process of granting access to resources and lower the risk of individuals gaining more system access than required by their job or other relationship to a company". Role based provisioning would be ideal for any company because of its ability to take a full advantage of automation. However, usually defining roles may be a tough obstacle and also critical amount of accounts to a certain system is needed in order to justify costs of implementing automation. Therefore companies can implement hybrid approach which combines request based provisioning with role based provisioning.

Hybrid approach is a combination of request based provisioning and role based provisioning. According to (Buecker et al. 2009) this kind of approach may be useful when a company wants for a subset of employees automated role based provisioning and others to use request based provisioning. Buecker et al. (2009) continue that hybrid approach may be ideal goal for some companies when others see it as a step towards full role based provisioning. As always, it is based on company's current and future needs which approach will be implemented. Furthermore, it is important to evaluate each approach also with financial measures before deciding which of the presented approaches to implement.

2.5 Services Related to Identity Management Solution

Identity management solutions are usually modular and they can be easily expanded with related services. Usually it is easy to integrate other software to work with identity management solution, at least if the software is from the same vendor. This additional software can deliver several advantages for the company in terms of features and functionality. Following two subchapters will present Single Sign-On (SSO) and identity management self-service features which can be easily implemented with identity management solution.

2.5.1 Single Sign-On

In this section an overview of Single Sign-On functionality, benefits and infrastructure will be given. First, I will give short introduction why companies want to implement SSO. Second, I concentrate on defining more deeply basic concepts behind the SSO. This section will not cover different technologies and types of SSO, but concentrates on defining SSO on more pragmatic level. Single Sign-On is one of the key features that can be implemented simultaneously with identity management system. SSO will deliver great deal of value for the company without huge effort and budget.

Pohlman defines Single Sign-On as follows: "Single Sign-On (SSO) framework is a mechanism that allows several different applications common to an enterprise to share a user authentication service. SSO … provides a secure way for users to be authenticated just once while enabling enterprisewide access to the data." (Pohlman, 2008, 85). From this definition can be seen that the main idea of SSO is to centralize authentication in order to provide access for the employees. Furthermore, according to Lakner, Bobak, Cifka, Greene, Lachman, Taylor & Wayman (2004) in typical environment employees will have many user names and passwords for different systems. This problem can be solved by implementing SSO solution for the company.

Nowadays employees in many companies need to log-in several different services during a workday in order to get their job done efficiently. Especially in knowledge heavy fields of business employees may need numerous different applications for doing their routine duties. Furthermore, companies are trying in every possible way to improve their employees' productivity. The more productive employees are the more company is able to make profit. Every time user signs in for a service or application it takes time that could be used for working. However, Single Sign-on (SSO) is a solution which makes applications, resources and services more easily reachable for the employee. When SSO is in place, employee needs to type his/her username and password only once, instead of typing his/her credentials separately for each service, in order to get access for all the applications and services he/she needs. In other words, employee is authenticated only once and after that all the needed resources are available for him/her. In addition, SSO will reduce administrative costs and

improve company's overall information security. This is due to decreased password reset requests and usage of stronger single password. Password and password policies are discussed in more detail in section 2.4.1.

This paragraph will shortly describe problems, from the user point of view, that are drivers behind implementing SSO solution. Different systems and services usually have different ID and password policies, which will force user to use different kinds of user ID and passwords for each service or system. These policies may, for example, define length or minimum number of special characters for the user id/password. Furthermore, services usually require users to change their passwords frequently which will lead into a situation where the user needs to keep track of several passwords and user IDs. Situation is well illustrated in Figure 5 where John Smith needs to remember vast amount of credentials in order to do his job. This can be time consuming and at the same time will reduce productivity of an employee (Lakner et al, 2004). To conclude, SSO can streamline password management for the users by allowing them to use only one user ID and password instead of dozens. This can save working time and ease users' password management stress. However, also identity management solution enables employee to have only one credentials but he/she needs to type them separately for each application/service needed. SSO decreases daily logins needed noticeably by requiring employees only to type once their credential in order to get full access to all of the needed applications.

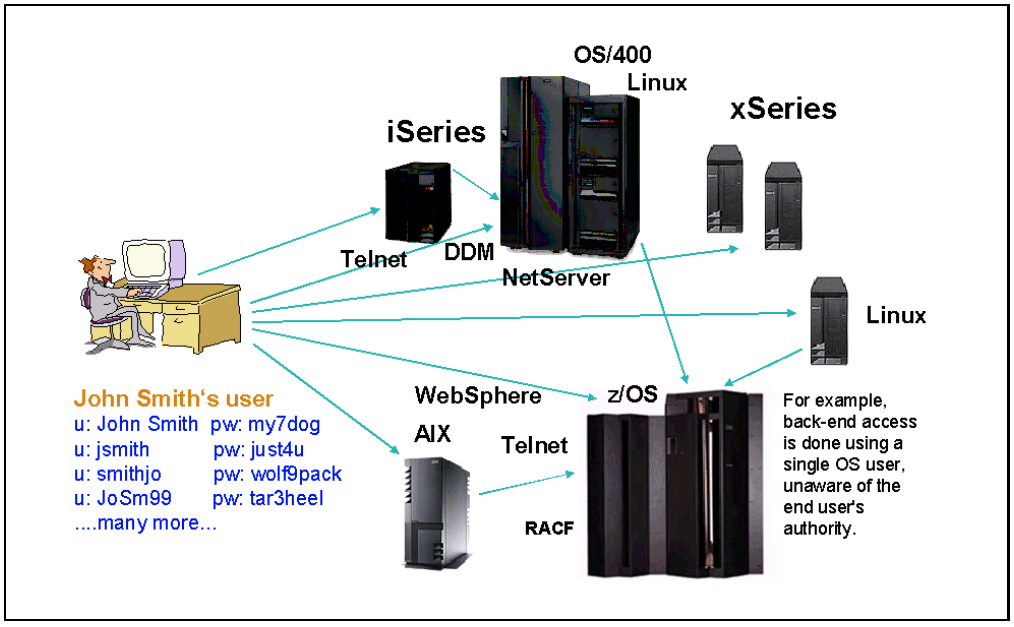


Figure 5: Employee's credential jungle (Lakner et al, 2004)

SSO will streamline user authentication and ease password fatigue by unifying user's usernames and passwords under one credentials. In addition, SSO allows user to access all needed resources with only one authentication instead of logging in all the different resources separately. Furthermore, these SSO's advantages can be a source of monetary savings for the company and can be used when constructing the ROI model in subchapter 4.4.

2.5.2 Identity Management Self-service

Identity management self-service interface usually enables employees to reset their password, request new roles or accesses and change their personal information. Identity management self-service is another feature, like SSO, that can be easily implemented with the identity management solution. Implementing self-service can bring notable savings for the company and increase the company's performance. Figure 6 illustrates different identity management self-services types and their features. There is different self-service interface for employees and line managers. These different interfaces and their features will be explained in the following paragraphs.

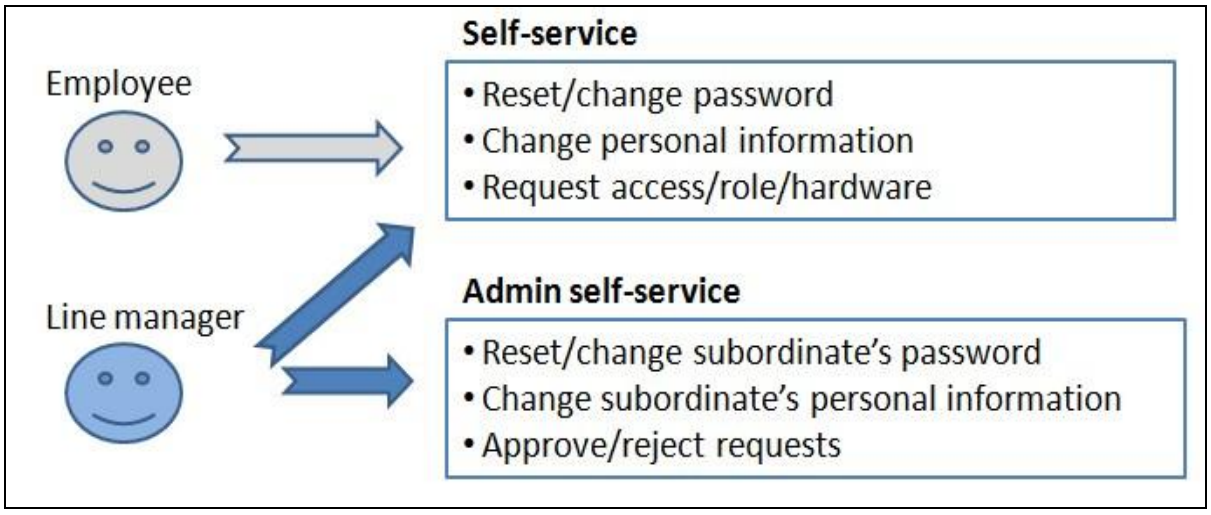


Figure 6: Identity management self-service features

Probably the greatest advantage of self-service is the feature which enables employees to reset their forgotten password without contacting the help desk. Savings cumulate from saved time for employees and the fact that help desk is not needed for the password reset. In addition to

resetting the password, it can also be changed through self-service interface. Furthermore, I believe that self-service interface is also more convenient and hassle free way for employees to handle routine password problems, such as password reset or change.

Self-service is used for enabling employee's to do routine tasks instead of requesting these tasks to be fulfilled by the service desk. Self-service interface allows employees to change predefined personal data such as their phone number or home address. More importantly self-service interface enables employees also to request new accounts or hardware, such as new laptop that they need for their work. Usually request goes to employee's line manager or other designated person who can approve or reject the request. These requests can be approved in admin self-service interface that will be discussed in the next paragraph.

Admin self-service, on the other hand, is mainly designed for line managers or owners of a certain resource and it allows them to approve role/access requests from their subordinates. Furthermore, in admin self-service interface line managers can request accesses for their subordinates or change subordinates' personal information. Through admin self-service line managers can ensure that their subordinates have all the required accounts for performing their work.

It is important to remember that employees in the companies have very different computer skills and some employees may need a lot of guidance for using self-service interface. Peterson et al. (2008) note that when implementing self-service, company should consider how tech savvy their employees are. Peterson et al. (2008) suggest that it might not be recommended to implement self-service if employees are not computer savvy. They continue that, on the other hand, if employees are proficient computer users, company may be ready to accept self-service. I agree that it is important to take into account employees' computer skills but not implementing self-service because of employees' weak computer skills is in my opinion an error. Therefore better solution would be to educate and train employees instead of dropping whole self-service out. Training of employees can be costly but it will pay back by decreasing load in help desk and by increasing employees' productivity. Self-service can bring great savings with little effort and should be implemented if there are not well justified reasons against the implementation. Peterson et al. (2008) also note that properly preparing and training business units will help company to maximize IAM solution's intended value.

Identity management's self-service feature can bring many advantages for the company and it is easy to implement with identity management solution. Self-service interfaces allow users to conduct routine tasks, such as password resets by themselves without contacting the service desk. However, companies should educate employees to use self-service efficiently in order to reap most of it. This is even more important if the employees are not computer savvy.

3 Developing a Conceptual Model for Identity Management Solution's Financial Benefits

Purpose of this Chapter is to create a conceptual model for identity management solution's financial performance which integrates earlier discussed issues with financial performance. In the previous chapters basic understanding of identity management solution principles was established and its importance for the companies illustrated. Furthermore, benefits, business drivers and challenges were discussed and they create a base for this Chapter. However, in this Chapter I will first shortly introduce earlier researches on ROI model for identity management solutions. Thereafter I will construct my own conceptual model by combining results of the earlier research and concepts introduced in the literature review. The constructed conceptual model will be utilized when developing a ROI model in Chapter 4.

3.1 Previous Research on Identity Management's Financial Performance

Identity management is a relatively young field of business and there is not much previous research on identity management's financial performance. Furthermore, purely academic sources cannot be found and therefore I will have to rely heavily on information that is published by major identity management solution vendors. However, I do not see this as a problem because I am using these publications as a guide line on the way creating my own conceptual framework which will link identity management and financial performance. Next I will be presenting three studies which concentrate on identity management solution's financial return.

A10 (2006) notes that benefits of identity management can be achieved without implementing full suite Identity and Access Management solution, but by choosing the most appropriate identity management solution components. A10 identifies following benefits that will deliver identity management solution ROI:

- Improved Efficiency and Minimized Management Overhead

- Increased Security, in depth Visibility and Compliance
- Reduced Complexity and Lower Cost

A10 (2006, 5) identifies that "the actual cost and return-on-investment for and IAM project will depend on two main factors - the IAM features deployed and the salary and operational expenses for the company." Cost side is quite forward, the more features company wants the more it needs to pay for them. However, it is important to notice that savings will be cumulated from the savings in salary and operational expenses.

OSM (2005), on the other hand, identifies five main problems in the companies that identity management solution can solve and thus be source of ROI:

- a massive administration workload
- a security nightmare
- poor service levels
- exposure to the skills shortage
- overload on the help desk

As can be seen, also OSM identifies mostly the same issues as A10. However, exposure to the skills shortage is interesting because it can be seen also as a cost of missed business opportunities.

Finally, I will introduce Alinean's ROI model and methodology which is the most comprehensive and proper for my purposes. Alinean's (2002) model includes three factors:

- Net tangible benefits
- Intangible benefits
- Risk

These net tangible benefits will take into account the total cost of identity management solution implementation compared to the quantifiable financial savings and benefits of the

solution. The intangible benefits, on the other hand, include strategic element of identity management solution. Furthermore, risk in Alinean's model mean risk that may affect on projects costs or hinder achieving expected intangible or tangible benefits. Main contribution of this study for my conceptual model is identifying that identity management solution can also deliver intangible benefits.

3.2 Introducing a New Conceptual Model of Identity Management Solution's Benefits

In this subchapter I will present a new conceptual model of identity management solution's benefits and its connection to previous research. This conceptual model shown in Figure 7 is an upper level model which will be used as a guide line when drilling deeper to each component in the phase of creating the ROI model in Chapter 4. The conceptual model has been created by combining components from research introduced in this Chapter as well everything discussed in the literature review.

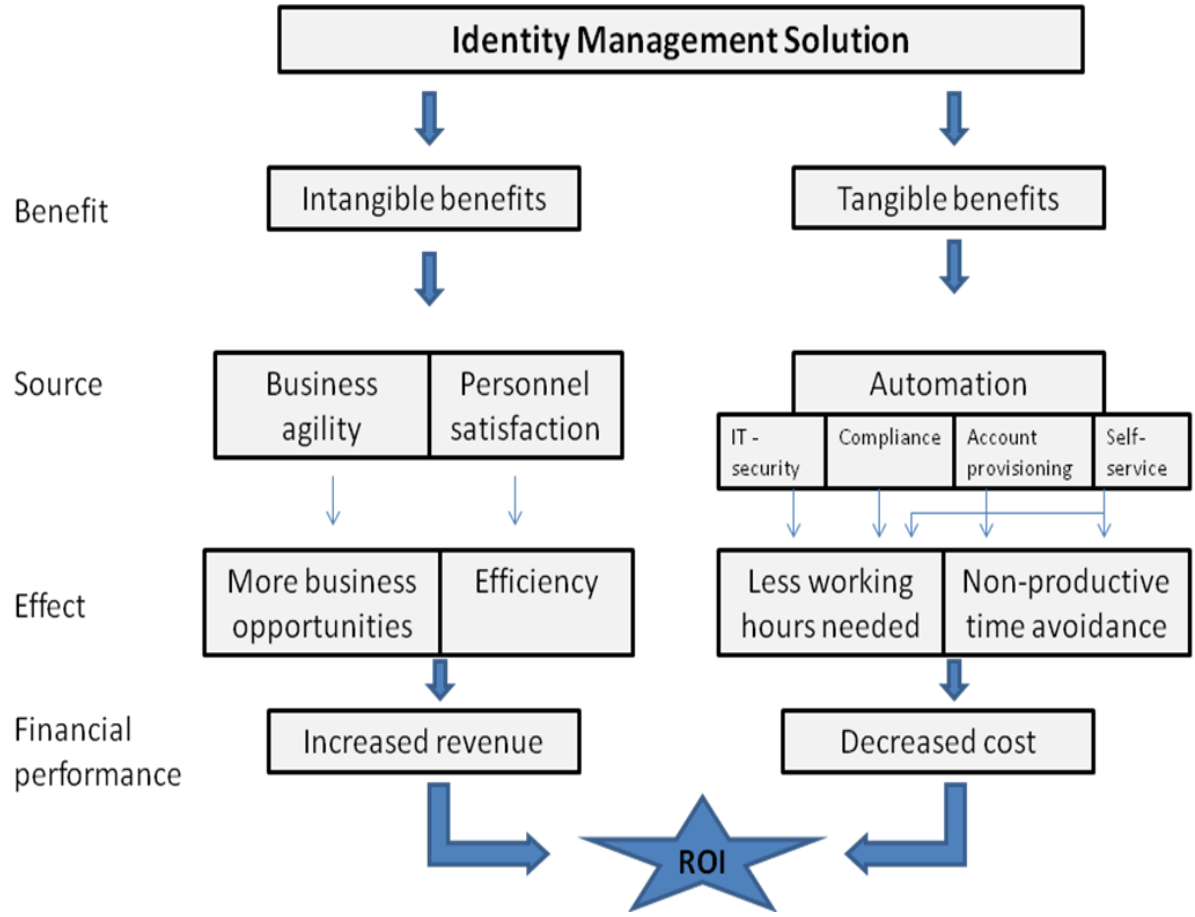


Figure 7: A model of identity management solution benefits

As can be seen in Figure 7, benefit level divides benefits into two categories: tangible and intangible. This approach was directly adopted from Alinean's model. Tangible benefits are measurable and easier to implement into the ROI model. On the other hand, intangible benefits are harder to measure in financial terms but should be considered when implementing identity management solution. These intangible benefits may have many indirect effects on company's financial performance.

Second level in Figure 7 defines source of the benefit presented in the first level. Intangible benefits are divided into two main categories: business agility and personnel satisfaction. Business agility depicts company's ability, for example, to react fast when business environment suddenly changes or company merger occurs. Business agility concept was developed from HP's (2004) claim that identity management solution can increase company's business performance. Personnel satisfaction, on the other hand, illustrates that employees are

more satisfied with their working environment when they do not need to waste time in handling several credentials and identities. This conceptual model presents only those intangible benefits that I believe are the most relevant ones. However, there are probably many other minor intangible benefits that are not presented in the conceptual model.

Source of tangible benefits is automation which is further broken down to four subcategories which are as follows: IT-security, compliance, account provisioning and self-service. It should be noted that in this model all the auditing capabilities are included in compliance category. Identity management will automate process of producing compliance reports and enforce password policies centrally. Furthermore, manual work related to creating accounts into the target systems can be automated. Lastly self-service enables users to reset their password, change personal information and request accounts without calling to the help desk. These issues were acknowledged by all the previous researches presented in the previous subchapter.

The effect level defines how the source of the benefit affects on the company's performance. Slim and light blue colored arrows show which source is driver behind which effect. First, on the tangible side in Figure 7 is presented two effects: more business opportunities and efficiency. More business opportunities are thanks to business agility that company can achieve with identity management solution. Furthermore, personnel satisfaction leads to efficiency. Employees are known to be more efficient when they are satisfied with their job. On the tangible side, all the automation benefit sources are directly affecting on working hours needed to complete tasks. Furthermore, automation of account provisioning and implementing self-service can decrease employee's non-productive time significantly. Non-productive time in this model means the time employee is unable to do his/her job because of, for example, inappropriate access rights or forgotten password.

The last level before the ROI is financial performance which depicts what financial effects these tangible and intangible benefits have on the ROI. Intangible benefits will lead into increased revenue and tangible benefits will decrease costs. However, this separation into increased revenue and decreased cost is not solid and can have exceptions. Non-productive time avoidance, for example, can be seen as a factor that increases revenue because employee has more efficient working time in use. On the other hand, non-productive time can be a cost for the company and eliminating employee's non-productive time can be seen as a decreased

cost. Furthermore, as mentioned intangible benefits are hard to measure but they may have significant indirect affect on the company's financial performance.

The constructed conceptual model gathered together the most important identity management solution's benefits that can affect on company's financial performance. Benefits for the model were combined from ones mentioned in the literature review. In addition, model was influenced by earlier identity management ROI research presented in the previous subchapter. As a result the constructed conceptual model well depicts the most important identity management solution's benefits from the financial point of view. In the next Chapter this conceptual model will be used as a basis when constructing the ROI model for an identity management solution.

4 Developing a ROI Model for RIMA

In this Chapter I will be developing a ROI model for RIMA based on knowledge established in the literature review and in constructing the conceptual model. Starting point for the ROI model will be the conceptual model developed in Chapter 3. Upper level descriptions of revenue sources presented in the conceptual model will be broken down into more accurate variables and eventually applied in the ROI model. First I will introduce RIMA solution from business point of view. Thereafter, I will show the functionality of RIMA from more technical point of view. After presenting RIMA from business and technical view, I will introduce different ways of measuring financial performance. Finally I will introduce assumptions, logic, attributes and functionality of the ROI model.

4.1 RIMA from Business View

This subchapter will present RIMA from business view and introduce its most important features. RIMA is acronym for Rapid Identity Management Assembly and as the name refers it will provide companies an identity management solution with fast implementation. RIMA is a standardized identity management solution that is delivered as a service (SaaS).

RIMA provides an extensive identity management solution for the customer and is also cost effective and easy to implement. Customer will receive a standard solution which will include wide catalog of features but can also be expanded according to the customer's preferences. Different features of the basic installation can be modified and activated according to the customer's wishes. This way the best solution for each individual customer can be achieved. Furthermore, RIMA can be implemented by using standard procedures and quickly implementation. ("RIMA," n.d)

Standard solution includes but is not limited to the following features ("RIMA," n.d):

- Servers and applications including monitoring services and licenses
- Centralized user access rights management process
- Automated access rights management
- Self-service interface for managing and requesting access rights
- Basic auditing and reporting tools
- Service help which includes advising customer when needed and solving malfunction issues
- Service extensions on demand

4.2 RIMA Architecture

In this subchapter I will introduce RIMA architecture, functionality and features from the technical point of view. First I will go through different software that is combined in order to create RIMA solution. Thereafter, I will present technical functionality and information flows inside IBM Tivoli Directory Integrator and IBM Tivoli Identity Manager 5.1 which are the main components of RIMA.

4.2.1 RIMA Components

RIMA is based on IBM Tivoli Identity Manager 5.1(ITIM) which provides all the identity management functionality. In order to use identity management system many components need to be installed. Following list summarizes key components of RIMA:

- VMware
- IBM Tivoli Identity Manager 5.1

- WebSphere Application Server
- IBM DB2 Software (database)
- IBM Directory Server (Lightweight Directory Access Protocol (LDAP))
- IBM Tivoli Directory Integrator

VMware is a virtualization solution which makes it possible to run several virtual machines on one physical machine. Virtualization enables companies to take all the advantage out of their physical machines and take step away from ideology where one physical machine runs only one software. Therefore, virtualization enables physical machine's resources to be used more efficiently. Basically this means that one physical machine can run, for example, five Windows 7 instances simultaneously instead of only one instance of Windows 7.

IBM Tivoli Identity Manager 5.1 (ITIM) is the heart of the identity management solution. Using ITIM's administration interface all the needed roles, workflows, rules and other desired attributes can be configured in order to gain benefits mentioned in the earlier chapters. Furthermore, ITIM is used for controlling accesses, managing password policies and configuration of other important identity management features.

WebSphere Application Server (WAS) is needed to run ITIM 5.1. IBM Tivoli Identity Manger is a JAVA based software which uses WebSphere Application Server provided services for writing data into database and for handling connections with other components.

IBM DB2 is a database that is used for saving all the transaction data needed in ITIM. Database can contain, for example, transaction entries of create user, modify user and delete user tasks. Furthermore, after the transaction has completed, these transaction entries become log/audit entries into the DB2.

Lightweight Directory Access Protocol (LDAP) is used for authentication of users and saving identity management data. Difference between LDAP saved data and DB2 stored data is that the LDAP stores the static user and ITIM configuration information, and DB2 stores the current and past transactions.

IBM Tivoli Directory Integrator (ITDI) is used for interpreting data mainly from the Human Resources (HR) system. Usually companies want to keep their HR system isolated from other information systems and ITDI interprets feed pushed out from HR-system. In addition, ITDI also can be used for a multitude of tasks, such as generating user ID and email address attributes for the employees.

4.2.2 RIMA's Logical Information Flow

Earlier I have explained how the identity management solution works but now I will take a deeper look into RIMA's logical information flow. I will provide explanation what occurs behind the user interface and how everything is connected together. I will go through Figure 8 and explain all the connections, components and their functionality shown in the picture. First I shortly explain HR-system and HR-feed. After that there will be designated sections for flows occurring inside IBM Tivoli Directory integrator and IBM Tivoli Identity Manager.

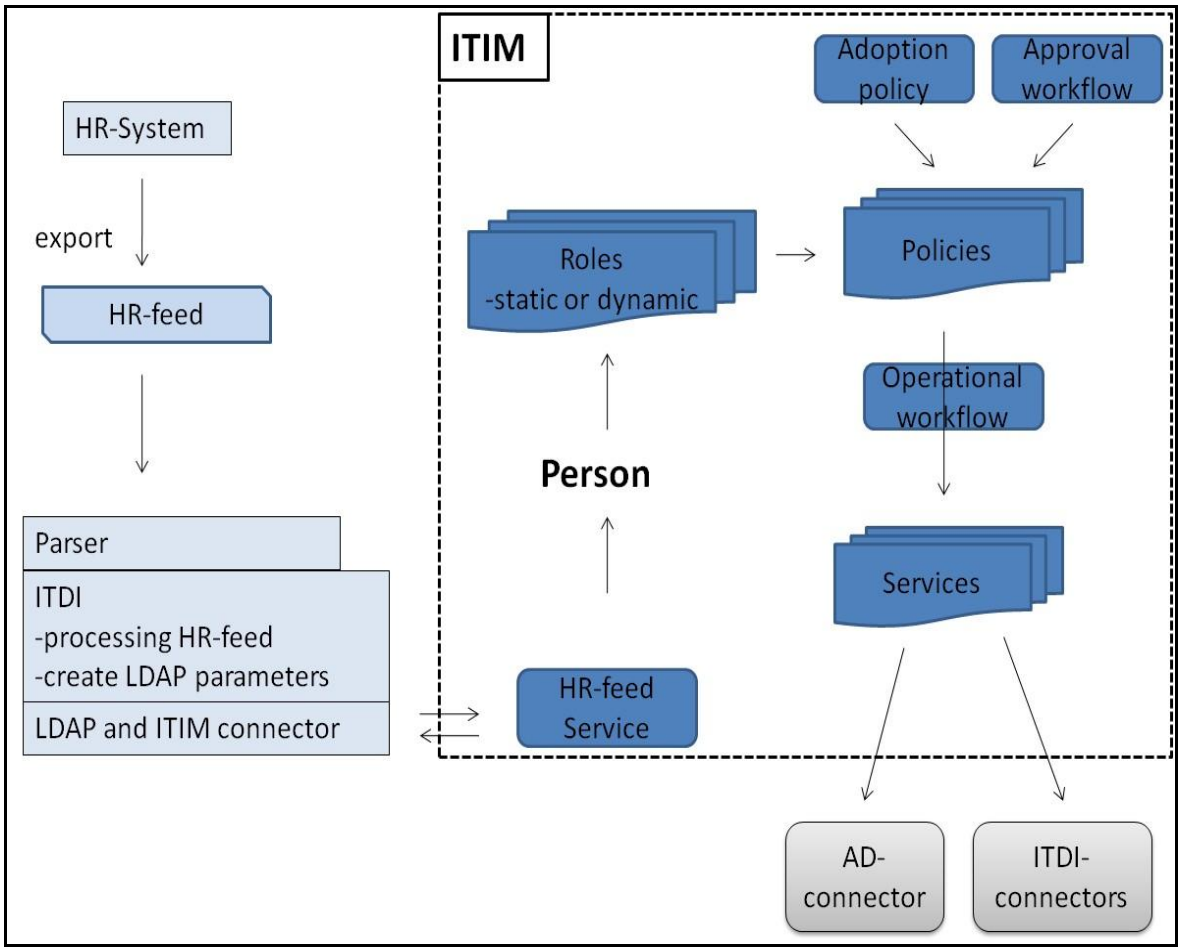


Figure 8: RIMA architecture

In the top left corner of Figure 8 is a HR-system, which is usually the core of every company's personnel management. Usually companies do not allow direct connections to their HR systems but these systems are able to export a file (HR-feed) containing all the needed employee data. Generally this file contains following information: first name, last name, employee number, role, department and other employee related information. It is very important that the HR-feed contains also a unique identifier for each employee so that identity management system can uniquely identify each employee.

4.2.2.1 IBM Tivoli Directory Integrator

IBM Tivoli Directory Integrator enables administrators to create assembly lines which will execute certain processes in a desired order. In the following paragraphs I will explain functionality of an assembly line which contains following components: parser, processing HR-feed and connectors.

Usually HR-feed is in a format that IBM Tivoli Directory Integrator cannot interpret without parsing it first. ITDI contains parser functionality which will interpret the HR-feed. HR-feed can be, for example, in CSV (Comma Separated Values) format. Furthermore, ITDI parser allows you to write your own parser and supports also many other file formats/protocols including HTTP, LDIF, XML, etc (IBM , n.d)

After the HR-feed has gone through the parser, ITDI will be able to process the data. Usually HR-feed's schema is different than the ITIM's LDAP schema. Schema defines the attributes that are available. Therefore ITDI will map the HR-feed attributes to match with the LDAP attributes. HR-feed may have attribute "fname" containing employee's first name. However, this "fname" attribute needs to be mapped to match with LDAP's schema where employee's first name is stored in the attribute called "givenname". Furthermore, in this stage of the process ITDI could also create the desired username for each user according to the customer's preferences. Username could be, for example, composed according to the following rule "Username contains three first letters of the first name and two first letters of the last name." By following this rule John Smith's username would be "johsm". Furthermore, also email addresses and other required attributes can be constructed in a similar way.

As mentioned, ITDI assembly line will also have connectors which are used for communication between different systems. ITDI assembly line uses LDAP and ITIM connectors to push and pull data from these target systems. Furthermore, ITDI uses LDAP connector to compare HR-feed data with LDAP database in order to see who does not yet exist in LDAP database. Therefore usernames and other custom attributes are created only for the employees who do not exist in LDAP. If employee exists in LDAP database, only defined attributes are updated into ITIM but no custom attributes, such as user ID or email address are created. ITDI uses connector also for pushing data to ITIM system.

This section shortly described IBM Tivoli Directory Integrators components and functionality related to identity management and ITIM. Furthermore, logical information flow through ITDI was presented. In the next subsection I will discuss logical information flow in ITIM and ITIM's components which are inside the dashed square in Figure 8.

4.2.2.2 IBM Tivoli Identity Manager

Now I will be moving from ITDI functionalities to IBM Tivoli Identity Manager itself. ITIM contains many different components, which are illustrated in Figure 8. In the following paragraphs I will explain functionality and information flows related to the following components: services, identity, roles, policies and workflows.

Services handle connections to systems outside of ITIM. Therefore these services might handle connections to systems like Active Directory (AD), ITDI and Lotus Notes. Before services are usable they need to be configured. Configuration includes naming the service, defining network connections and other service related attributes. After a service is configured to connect to the correct target system it can manage the target system through an adapter. Adapters can contain various connectors that are used for communicating with different systems. ITIM can use the service "HR-feed service" to retrieve data from ITDI. Prerequisite for this data retrieval is that a listener in ITDI is configured to listen for ITIM commands. ITIM retrieves all the needed employee information from ITDI through HR-feed service and creates for every employee a person instance in ITIM. Furthermore, every employee will be provisioned with an ITIM user account. Moreover, this ITIM account is used for accessing ITIM self-service discussed in section 2.5.2.

I already introduced roles and RBAC in subsection 2.4.2 and now I will explain how roles are configured in ITIM and how they link to services and workflows. There are two types of roles, static and dynamic ones. Employees are assigned automatically to dynamic roles if they fulfill certain attribute requirements. Therefore "Sales representative" role would be assigned, for example, every employee who belongs to the sales department. Moreover, belonging to a certain department is evaluated by the value presented, for example, in "department number" attribute. Static roles, on the other hand, are roles that employees can request manually

through self-service interface or line managers can assign their subordinates to certain static roles. After an employee is assigned to a role, either automatically or manually, the provisioning policies to which the roles are assigned to will be activated, which in turn activates provisioning workflow. These policies and workflows will be discussed in the next paragraph. However, after different workflows have been completed successfully employee will have correct accounts under his identity in ITIM. These accounts, on the other hand, grant access rights that employees need in order to carry out their job. For sales person this might mean, for example, that he/she will get an "AD" account in ITIM and through automation he/she will be also assigned to sales group in Active Directory (AD).

This paragraph will define more precisely what policies and workflows are. As mentioned, roles are associated with provisioning policies which will initiate workflows. Most common policy is probably provisioning policy which provisions desired account for the user. In addition, there are also password policies, adoption policies and other minor policies. Provisioning policy will, for example, define what attributes will be written into the managed system. Managed system can be any system that is associated with the identity management solution. Furthermore, before initiating operational workflows, policy will start approval workflow if one is defined. In approval workflow, approval request is sent to the line manager or some other predefined person. Line manager can approve or reject requests through self-service interface. If the request is rejected, the requestor will be informed and all further provisioning steps will be aborted. However, if the request is approved it will initiate an operational workflow which will use services in order to push data to the managed resource. Pushing data means creating account, changing account information, deleting account or other actions performed for the desired account in the target system. Services, on the other hand, use adapters for performing these account modification requests.

Purpose of this section was to describe different processes inside the ITIM. However, to avoid too technical details, processes were only partly defined and many not even mentioned. However, I believe that this Chapter was a good introduction to processes running inside the identity management solution.

4.3 Different Ways to Measure IT Investment's Financial Performance

Measuring financial performance of an IT investment is ever increasingly important and purpose of this subchapter is to present different ways to measure IT investment's financial performance. Nowadays it is not enough to show that IT solution is functioning well, but it also needs to be feasible from the financial point of view. Therefore it is very important that vendors are able to offer concrete calculations showing financial benefits that their solution can deliver. In this subchapter I will go through shortly the most popular financial performance measures including Net Present Value (NPV), Internal Rate of Return (IRR), Return on Investment (ROI) and payback period.

Net Present Value is a very popular financial performance measure for evaluating different projects. In NPV calculation all the future cash flows, positive and negative, are discounted with return requirement. Initial investment is subtracted from the net present value of future cash flows. A positive NPV value indicates that the investment will exceed investor's required return and is a good candidate for investing. On the other hand, negative NPV indicates that the return of the project will be smaller than required return by the investor and it would not necessary be the best option for investment. Furthermore, if NPV equals to zero, investment's return will be exactly the same than the return requirement set by the investor. Benefit of using NPV is that it takes money's time value into account. Furthermore, risk can be taken into account by adjusting return requirement. However, NPV does not tell anything about ratio between initial investment and the return.

Internal Rate of Return (IRR) will state the yearly return percentage for the investor. As opposed to NPV which will provide investor a monetary value of the investment. Goal of the IRR is to find return rate that will make investment barely to break even thus give value of zero for NPV. Investor should compare his required return to IRR and accept investment if IRR is greater than required rate of return and otherwise reject the investment. Benefit of IRR is that it states return percentage and makes different projects comparable. However, problem with IRR is that it speaks only in terms on percentages and not in monetary terms as Dollars or Euros.

Return on Investment (ROI), on the other hand, can be calculated by dividing net present value of investment with investment costs. Basic idea is to measure ratio between return and invested capital. ROI will give a percentage which every invested euro will return during the certain time period. However, there are many different ways for calculating ROI and a suitable one needs to be selected according to project's preferences. Ability to modify ROI to specific need is also the downside of the ROI. Therefore it is very important to understand logic behind a specific ROI calculation.

Payback period is one of the simplest financial performance measurements and it simply states how many years it takes for the project to payback the initial investment. In other words, payback period states how many years it takes until cumulative cash flows equal zero. Payback period does not take time value of money into account and does not consider cash flows occurring after the initial investment have been covered. These features make payback period bad measurement for comparing different projects.

There are many different financial measures for evaluating IT investments but none of them alone is flawless. Every measurement have different angle to the profitability of a project and all of them bring additional value for the investor. Therefore I believe it is important to include all the mentioned financial measurements in the ROI model to be constructed.

4.4 Assumptions and Justifications Related to the ROI Model

In this subchapter I will present assumptions and justifications related to the ROI model which will be constructed by utilizing conceptual model from Chapter 3. ROI model will be heavily concentrating on tangible benefits that identity management solution can deliver and ignores intangible benefits. Intangible benefits are not included in the ROI model because they are hard to convert into monetary values. Following assumptions should be carefully read before using the ROI model so the logic behind the calculations is clear for the user:

- ROI model will calculate difference between company's current cost structure and the cost structure after implementing identity management solution. Savings that IdM solution can deliver will mainly cumulate from improved efficiency through

automation and from increase in information security. However, new costs arise from initial implementation cost and monthly fee charged by the service provider.

- ROI model will not take into account "soft dollars" which can be seen as intangible benefits in Figure 7 (Chapter 3). These intangible benefits could be measured with Key Performance Indicators (KPI). However, KPI is not in scope of this thesis and the ROI model's purpose is to reflect possible dollar savings that IdM solution can deliver.

- Identity management systems are modular and ROI model introduced in this thesis is designed to support RIMA's basic installation which includes normal IBM Tivoli Identity Manager 5.1 functionality, self-service interface and Single-Sign On.

- Information security (negative) risks and their realization probabilities are hard to convert into financial measurements. However, it is important that information security issues are included in the ROI model. This way customer can by him/herself evaluate cost and probability of different information security threats occurring.

- Cost savings mostly stem from saved working hours by the employees and the model converts these saved working hours directly into monetary savings in relation to employee's salary. It should be noted that usually employees generate more profit for the company than their wage. Furthermore, employees usually also have slack time in their work that they do not use efficiently. Therefore, converting hours saved by using employee's salary can be seen as a justified approach.

- Model assumes that RIMA will be working at it best performance. This is because it would be very hard to estimate possible miss usage of the software or unplanned down times.

ROI model calculates many different financial measures and leaves it on customer's responsibility to choose which of these measures to use in decision making. Furthermore, all the calculation formulas are checked and they generate "correct" results according to the formulas stated and assumptions made. These formulas are visible for the user and the attributes in the formulas are named in a way that customer can see semantic meaning behind each attribute. To illustrate attribute naming logic; figure representing average

number of employees hired yearly is stored in the attribute named "employees_hired_yearly". Therefore, the ROI model will yield its best estimate according to input values and formulas. When interpreting the ROI model's results, user should keep in mind all the assumptions related to the ROI model and also reliability of the input values.

4.5 The ROI Model for RIMA

In this subchapter I will explain in detail logic and the functionality of the ROI model for RIMA. First I explore logic and components of the model. Thereafter, I will more deeply explain separately each excel worksheet: Company details, RIMA cost, managed system details, information security, employee time savings, cost savings summary, cost savings yearly, cost savings cumulative and return.

4.5.1 Logic of the ROI Model

In this section I will shortly go through logic of the ROI model which is shown in Figure 9 below. However, this is only an overlook to the logic of the ROI model and the functionality of the model will be discussed more deeply in section 4.5.2.

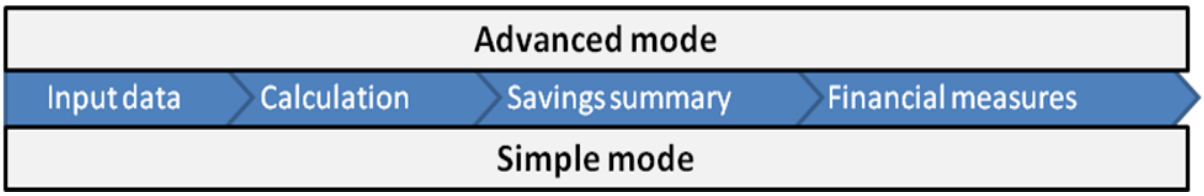


Figure 9: Structure of the ROI model

Input data contains all the basic data about the company, including number of employees, average amount of accounts per user, yearly working hours, wages of different employees and other company specific attributes. Furthermore, input data also includes probabilities and

costs of information security risks. In addition, input data will include different cost associated with identity management solution implementation and maintenance.

Calculations in the ROI model are performed based on the input data from the customer company. Formulas used for calculations will be discussed in the next section 5.4.2. Based on the input data and calculations, the ROI model will present savings summary which shows in detail monetary and percentile affect of each saving area on the total savings. Lastly, ROI model will present financial measures, such as NPV, IRR, ROI, payback period, yearly cash flows and financial graphs.

As figure 9 shows, the ROI model has two different modes: advanced mode and simple mode. Most of the attributes given by the customer are common for both simple and advanced mode calculations. Basically in advanced mode user can define in more detail different attributes. In simple mode, on the other hand, user fills in smaller amount of attributes and gives more rough estimates about different areas of savings. It is recommended to use simple mode only if customer is familiar with different costs and can give reliable estimates. However, when customer chooses to use advanced, he/she can more precisely define, for example, information security costs with additional attributes.

4.5.2 ROI Model Attributes and Functionality

This section will give an insight to the attributes used in the ROI model and their contribution to the final calculations. Figure 10 illustrates all the saving factors as well cost factors identified in the ROI model. All the factors shown in the Figure 10 have already appeared earlier in this thesis and purpose of this figure is to illustrate what factors are affecting on the end results of the ROI model.

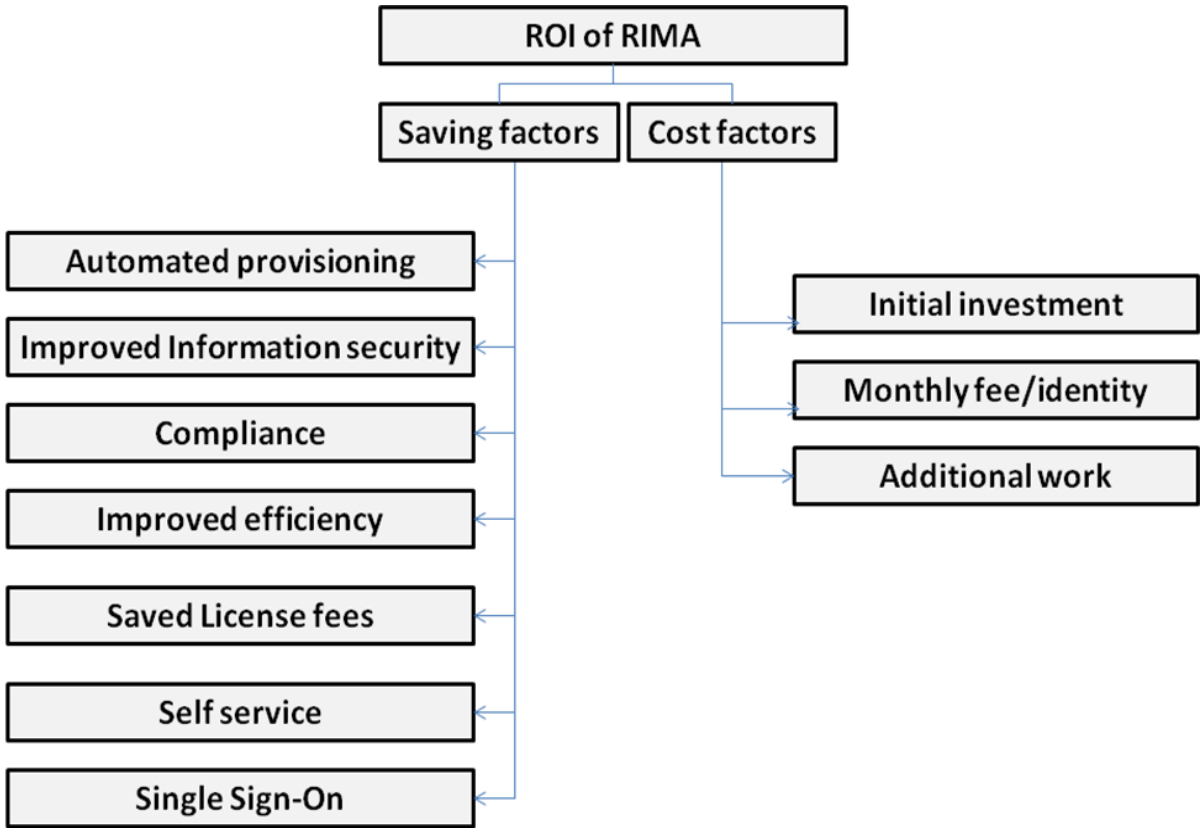


Figure 10: ROI model's benefit/cost breakdown

Figure 10 illustrates well different cost/saving areas which are the basis for the ROI model calculations. On the left side in Figure 10 is all the cost saving factors that will be positively affecting on the ROI. These cost savings stem from different benefits that can be achieved by using identity management solution. Furthermore, on the right side of the figure can be seen different cost factors that will decrease ROI. These cost factors are related to implementing, maintaining and expanding identity management solution. Savings and costs shown in Figure 10 will be discussed more deeply in the following paragraphs where different worksheets of the ROI model will be presented.

Figure 11: ROI model's most important worksheets

Figure 11 illustrates the most important worksheets used in the ROI model and all of these worksheets are common for both, advanced and simple mode. These worksheets are colored with green in order to emphasize their centrality. Company details worksheet contains

attributes that are used for the simple ROI calculation but most of these attributes are also shared with advanced calculation mode. Furthermore, RIMA cost worksheet is common for both modes and it specifies costs associated with implementing and maintaining RIMA solution. Finally cost savings summary and return worksheets will show results separately for simple and advanced mode.

Figure 12: ROI model's additional worksheets

Figure 12, on the other hand, shows worksheets that allow user to define attributes for advanced mode and to observe yearly cost savings. These worksheets do not have any special coloring because they are intended to be more optional ones than the green colored ones in Figure 11. Information security, employee time savings and managed system details are advanced mode worksheets that contain attributes that will not be needed in the simple mode calculations. However, Information security and employee time savings worksheets can be used to work out figures for simple mode calculations. In other words, user can use information security worksheet to calculate total information security cost savings and use that number in simple mode with simple copy and paste operation. This is possible because simple mode only requires one number for all the information security related cost savings.

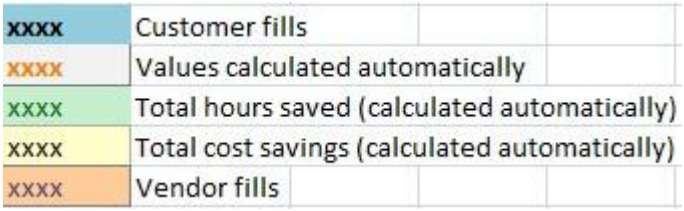


Figure 13: ROI model's cell coloring

Figure 13 illustrates meaning of different cell coloring used in the ROI model. Cells are color coded in order to guide the user to fill in correct cells and to know which cells are calculated automatically. Furthermore, cell coloring indicates are the savings in working hours or in monetary values.

In the following pages I will go through in more detail all the different worksheets shown in Figure 11 and Figure 12. All the values shown in the following figures are fictive and inserted only for illustrative purposes.

1. **Company details –worksheet**

4	**Company information**			
5	Employees with accounts	500		
6	Average amount of accounts/user	4		
7	Percentage of accounts/user (using workflow)	40 %	1,6	
8	Percentage of accounts/user (using provisioning)	60 %	2,4	
9	Average amount of users leaving company/year	30		
10	Average amount of employees hired/year	40		
11	Working days for employee in a year	230		
12	Working hours in a week (5days)	37,5		
13	Working hours in a year	1725		
14				
15				
16	**Staff expense**	Yearly wage	Hourly wage	
17	Average help desk worker	50 000,00 €	28,99 €	
18	Average administrator	70 000,00 €	40,58 €	
19	Average employee	60 000,00 €	34,78 €	
20				
21	**Account creation/deletion details**	Hour		
22	Average time needed to create an account	0,25		
23	Average time needed to delete an account	0,25		
24	Average time needed to change role or user accounts	0,25		
25				
26	**Self Service (yearly rates)**			
27	Help Desk calls associated password change/reset per user	1		
28	Average length of a call	0,2	hours	
29	Average account deletion requests/employee	1		
30	Average account change request/semployee	1		
31	Average account add requests/employee	1		
32				
36	**SSO**			
37	Average amount of logins decreased per day	2		
38	Average time spent for typing credentials/service	8	seconds	
39				
40	**Compliance**			
41	Manual reports produced/year	1		
42	Time to make one report	50	hours	
43				
44	**Information security and licenses**			
45	Estimated cost of possible Information security threats	7 000 €		
46	Estimated cost of unneeded licenses paid every year	1 020 €		
47				
49	**Employees time saved (workflow+provisioning)**			
50	Average time saved/request using provisioning	0,7	hours	
51	Average time saved/request using workflow	0,4	hours	
52	Average time saved/new employee	3	hours	

Figure 14: Company details –worksheet

Company details worksheet shown in Figure 14 include all the basic variables required for performing the ROI calculation. If customer uses simple mode of the ROI model, this is the only worksheet he/she needs to input variables. However, customer can adjust the ROI calculation specified attributes, such as investment period, rate of return and service level in the return worksheet. Company details include 28 variables

and these variables are divided under eight different categories: 1. Company information, 2. Staff expense, 3. Account creation/deletion details, 4. Self-service, 5. SSO, 6. Compliance, 7. Information security and licenses and 8. Employee's time saved. However, advanced and simple mode share attributes belonging to categories 1-6 and unneeded license cost in category 7. Furthermore, rest of the category 7 and 8 are utilized only in the simple mode. All the attributes filled into the ROI model are based on the customer company's current situation. Attributes concentrate to capture current monetary and time values related to current identity management practices.

2. RIMA cost – worksheet

7	**Initial investment**			**Yearly cost**			
8							
9	Basic deployment cost	15 000 €		Service level	Super	Good	Normal
10				Cost/user/month	6 €	5 €	4 €
11	Custom connectors			Cost/user/year	72 €	60 €	48 €
12	System one	1 000 €					
13	System two	1 000 €				Total yearly cost	
14	System three	1 000 €	Year	employees	Super	Good	Normal
15			1	500	36 000 €	30 000 €	24 000 €
16	Custom roles		2	510	36 720 €	30 600 €	24 480 €
17	Supervisor	200 €	3	520	37 440 €	31 200 €	24 960 €
18	Information analyst	200 €	4	530	38 160 €	31 800 €	25 440 €
19			5	540	38 880 €	32 400 €	25 920 €
20	Custom politics						
21	Request for special access	200 €					
22							
23							
24	Total initial investment	18600					

Figure 15: RIMA cost –worksheet

This worksheet shown in Figure 15 contains all the costs related to RIMA solution. Basic deployment cost is at minimum €15000 and it contains gathering requirements, implementation work, creating basic roles, attributes, policies and workflows and basic application connectors. Furthermore, customer pays yearly service fee which will cover all the costs required to keep RIMA solution up and running. These service costs consist of software license fees, software updates, hardware and help desk services required. There are three different service levels available which differ from each other in the means of problem solving speed and support available for the customer. Moreover, customer may purchase additional connectors or more complicated role creations as additional work. Connectors were discussed in section 4.2.2 and they are used for

communicating with additional systems. All the additional work is priced as hourly rate and there are no other associated costs. Costs shown on the left hand side in Figure 15 are total costs and not hourly rates. Costs shown in Figure 15 will be used when calculating yearly cash flows and financial measures in the return worksheet.

3. Managed system details -worksheet

6	Managed system one	Yearly requests	Average time(h)/request	Implementor's hourly wage	Cost/request	Total time (h)	Total cost
7	create account	100	0,3	30,00 €	9,00 €	30	900,00 €
8	delete account	50	0,2	30,00 €	6,00 €	10	300,00 €
9	change account	20	0,2	30,00 €	6,00 €	4	120,00 €
10	Total	170				44	1 320,00 €
11							
12	Managed system two						
13	create account	100	0,2	30,00 €	6,00 €	20	600,00 €
14	delete account	50	0,2	30,00 €	6,00 €	10	300,00 €
15	change account	20	0,2	30,00 €	6,00 €	4	120,00 €
16	Total	170				34	1 020,00 €

Figure 16: Managed system details –worksheet

Managed system details worksheet shown in Figure 16 is utilized in advanced mode and it depicts current costs of creating/deleting/changing account in the certain managed system. Customer needs to fill in yearly requests, average time used per request and request's implementor's hourly wage. Usually implementor is an administrator or a help desk person. According to these attributes the total cost of one managed system is calculated. Managed system can be, for example, Active Directory or phonebook. Cost savings cumulate directly from administrators time saved when the account creation process is automated. Therefore cost savings are simply calculated with following formulae: yearly requests*average time(h)/request*implementor's hourly wage. These cost savings will be used in the cost savings worksheet when collecting all the savings together.

I need to emphasize that also these calculations shown in Figure 16 heavily rely on the fact that the customer's input data is relevant. Managed system details worksheet allows customer to fill attributes up to five managed system. This is because RIMA is meant to be first step in the identity management solution and it creates a basis for

further implementations. Thus in basic implementation only couple of managed systems are implemented.

4. Information security –worksheet

4	Information security threats	Probability %	Cost of risk realizing		Total cost
5	Unauthorized access	1 %	100 000,00 €		1 000,00 €
6	Data theft	1 %	200 000,00 €		2 000,00 €
7	Data leakage	1 %	300 000,00 €		3 000,00 €
8	Total				6 000,00 €
9					
10					
11	Password policy changes/year	Password policy changes/year	Hours spent for policy change	cost/hour	
12	Managed system one	1	1	30,00 €	30,00 €
17	Total	5	5		150,00 €
18					
19	Time spent to find information security risks (orphan, shadow accounts etc.)				
20		Inspections/year	Hours spent/inspection	cost/hour	
21	Managed system one	2	20	30,00 €	1 200,00 €
26	total	10	100		6 000,00 €
27					
28	Total				12 150,00 €

Figure 17: Information security –worksheet

This worksheet shown in Figure 17 contains information security related costs, such as information security threats, password policy changes and cleaning unneeded user accounts. Different information security threats include: Unauthorized access, Data theft and Data leakage. Customer needs to assign certain probability and cost of risk realizing for each of information security threats. These attributes will be then converted into costs by simply multiplying probability by the cost of risk realizing. However, customer should have conducted more specified information security threat analysis in order to provide relevant numbers. If the customer has not yet conducted information security threats analysis, these attributes shown in Figure 17 can make the customer to rethink information security needs in the company.

Password policy changes and time spent for finding orphan accounts sections shown in Figure 17 allow customer to define hours and hourly wage spent for these actions. In Figure 17 only “Managed systems one” is shown but in reality worksheet contains five managed system’s that customer can input values. Therefore total numbers in the

Figure 17 have taken into account also hidden rows. These total figures will be used in cost savings worksheet when collecting all the savings together.

5. Employee time savings –worksheet

5	**Work-flow savings**	**days**	**In working hours**
6	employee getting new accounts (without workflow)	4	30
7	employee getting new accounts (with workflow)	3	22,5
8	Difference between old and new system	1	7,5
9	Work time saved factor	5 %	
10	Work time saved	0,05	0,375
11			
12	**Provisioning savings**	**days**	**working hours**
13	employee getting new accounts (without workflow)	4	30
14	employee getting new accounts (with provisioning)	2	15
15	Difference between old and new system	2	15
16	Work time saved factor	5 %	
17	Work time saved	0,1	0,75
18			
19	**Work-flow + proviosining savings (new employee)**	**days**	**In working hours**
20	employee getting new accounts (without workflow)	5	37,5
21	employee getting new accounts (with workflow+provisioning)	2	15
22	Difference between old and new system	3	22,5
23	Work time saved factor	15 %	
24	Work time saved	0,45	3,375

Figure 18: Employee time savings –worksheet

In this worksheet shown in Figure 18 customer fills in attributes that will be used for calculating employee's time saved. In other words this means avoidance of non-productive time because of locked account or inadequate access rights. Because this worksheet is not as straight forward as the ones presented before, I will go each attribute through in more detail.

Workflow time savings are achieved because employee can request account/access through self-service interface and employee's line manager can approve this request also by using self-service. After all the approvals are gathered automatically, email will go to administrator who will create access for the employee. This streamlines account requesting and approval gathering process, thus saves time.

On the other hand, provisioning time savings are achieved in the same way than in the workflow approach but administrator's work is automated and accounts are created automatically after all the needed approvals are gathered. Furthermore, there are

different parameters for the new employees and current employees because new employees are usually provisioned with the basic access rights when they enter to the company. Missing these basic access rights will lead to losing more efficient working time compared to a senior worker who probably can perform his duties quite well when missing only a certain special account. New employee parameters are meant to describe average time needed for new employee to get all the basic accesses required to perform his/her job.

Attributes:

Employee getting new accounts (without workflow):

This attribute should describe the current situation; how many days it takes from the time request is initiated to the point when employee can access to the needed resource.

Employee getting new accounts (with workflow):

This attribute is an estimate how long the same process would take when a workflow is in place and approvals are gathered automatically.

Work time saved factor:

First is calculated working days saved between the old and the new system. Work time saved factor indicates how many percentage of the time difference between the systems employee could have used more efficiently.

Work time saved:

This attribute is calculated by multiplying attribute "difference between old and new system in hours" by "work time saved factor".

Example:

Difference between the old and new account request processes is set to two (2) days. In working hours this means 2*(working hours in a day) = 2*7.5 = 15 hours if we assume 7.5 working hours/day. Work time saved factor is set to 20% and the employee would save 20%*15h = 3h working time / request.

6. Cost savings summary –worksheet

4	**Automated provisioning (simple)**		
5	Time saved	**Hours/year**	**Cost**
9	Total	117	4 747,83 €
12	**Self service (simple)**		
13	Password reset	100	2 898,55 €
16	**SSO (simple)**		
17		511,1111111	17 777,78 €
20	**Compliance (simple)**		
21	Producing reports	50	2 028,99 €
24	**Information security (simple)**		
25			7 000,00 €
28	**Licenses (simple)**		
29			1 000,00 €
30	**Increased efficiency (Employees time saved with provisioning and work-flow)**		
31			
32	**Employees' time saved**		
36	total	**410**	**14 260,87 €**
39	**Total**	1188,111111	**49 714,01 €**

Figure 19: Cost savings summary –worksheet

This work sheet shown in Figure 19 calculates and collects time savings and cost savings for the first year for each cost saving area according to the attributes customer has provided. Different cost savings areas in the ROI model are as follows: automated provisioning, self-service, SSO, compliance, information security, licenses and employee's time saved. Automated provisioning cost savings include automated creation, deletion and change requests in the managed systems. These provisioning savings are cumulated from administrators' time saved when accounts are created automatically. Self-service savings include savings that cumulate from employees' ability to reset password by themselves without calling to help desk. Savings are calculated by taking into account saved help desk worker's time because of decreased password reset calls from the employees. SSO savings, on the other hand, are cumulated from employees' time saved thanks to decreased logins needed daily. This saved time is then multiplied with the average employee salary. Compliance cost savings are calculated as follows: hours used earlier for making the compliance reports multiplied by the average administrator's hourly wage. Licenses cost savings is only an estimate provided by the customer and it does not include any additional

calculations. Calculating information security and employee's time savings were explained earlier in this section.

Furthermore, here the customer can see contribution of each cost saving area to the total cost savings. In Figure 19 under each area there are hidden cells which are visible in real calculation and would give more detailed information about each area. Furthermore, Figure 19 shows only cost savings calculated in simple mode. In the real ROI model below simple calculations there are same figures calculated with advanced mode attributes. Moreover, results presented in this worksheet will be utilized when calculating financial performance measures and yearly cash flows in the return worksheet.

7. Cost savings yearly and cost savings cumulative –worksheets

Cost savings yearly worksheet shows same information as the cost savings summary worksheet in Figure 19 but for each year separately. Yearly savings are different for each year if the amount of employees in the company is not constant. However, if every year the amount of employees stays the same, savings for each year also stays the same.

Cost savings cumulative worksheet, on the other hand, is also very similar to the cost savings summary worksheet but it will calculate cumulative savings. Basically this worksheet will calculate cumulative savings for years 1-5. This is done by summing up previous year's savings to the current year's savings.

It should be noted that in cost savings calculations only cost savings are taken into account and no identity management solution cost are included in these calculations. Identity management solution costs will be taken into account in the return worksheet in which yearly cash flows and financial measures are calculated.

8. Return –worksheet

3	**Choose service level**	**Good**			<-- choose service level		
4	**Required return**	**9,00 %**			<-- use slider to change required return		
5	**Year**	**5**			<-- choose investment period between 0 and 5		
6							
7	**Net Present Value (NPV) (simple)**		**NOTE: do not change values below!**				
8							
9	**Year**	**0**	**1**	**2**	**3**	**4**	**5**
10	**Savings**		45 627,53 €	42 429,21 €	39 447,98 €	36 669,80 €	34 081,46 €
11	**Cumulative Savings**	0,00 €	45 627,53 €	88 056,74 €	127 504,72 €	164 174,52 €	198 255,98 €
12	**Costs**	18 600,00 €	27 522,94 €	25 755,41 €	24 092,12 €	22 527,92 €	21 057,78 €
13	**Cumulative Costs**	18 600,00 €	46 122,94 €	71 878,34 €	95 970,47 €	118 498,39 €	139 556,17 €
14	**Cash Flow**	-18 600,00 €	18 104,60 €	16 673,80 €	15 355,86 €	14 141,88 €	13 023,68 €
15	**Cumulative Cash Flow**	-18 600,00 €	-495,40 €	16 178,40 €	31 534,26 €	45 676,13 €	58 699,82 €
16							
17	**Savings (not discounted)**		49 734,01 €	50 410,14 €	51 086,28 €	51 762,42 €	52 438,55 €
18	**Cost (not discounted)**	18 600,00 €	30 000,00 €	30 600,00 €	31 200,00 €	31 800,00 €	32 400,00 €
19	**Cash flow (not discounted)**	-18 600,00 €	19 734,01 €	19 810,14 €	19 886,28 €	19 962,42 €	20 038,55 €
20							
21	**NPV**	58 699,82 €	**Invest**				
22	**ROI**	42,06 %					
23	**IRR**	103,373 %					
24	**Pay back period (years)**	0,942535264					

Figure 20: Return –worksheet

Figure 20 shows return worksheet which is the final view in the ROI model. In the top left corner we can see service level, required return and year parameters which are used for manipulating the ROI calculation and testing different scenarios. RIMA is offered with three different service levels and their yearly rates are different. Furthermore, required return can be adjusted to correspond with customer's preferences. In addition, greater required return can be used to reflect with the risk related to the project or uncertainty of the attributes given. Lastly there is year attribute that defines for how many years financial measures and cash flows are calculated. The ROI model supports measures to be calculated up to five years period. Customer can choose value for the service level and year attributes from the drop down menus. To change required return customer can use a slider. These drop down menus and slider make it easy for the customer to change desired attributes and to see their affect on cash flows and financial measures instantly.

All the figures shown in Figure 20 will change dynamically when the customer changes attributes in the earlier worksheets or attributes in the top left corner of

Figure 20. Return worksheet will show savings, costs and cash flows for each year.

Furthermore, in the return worksheet customer can see following financial metrics: NPV, ROI, IRR and payback period. Furthermore, graphs will be created to illustrate cash flows through different years.

Formulas used for calculating financial measures:

NPV = discounted savings – discounted costs – initial investment
ROI = NPV / cumulative costs
IRR = Microsost Excel IRR() function.
Payback period = Initial investment / (yearly cost savings – yearly service fee)

This chapter described in detail different functionalities and worksheets of the ROI model. Also different saving areas and logic behind the ROI model was introduced. In the next chapter I will be testing that the ROI model is able to deliver functionalities mentioned in this chapter mentioned.

5 Testing the Constructed ROI Model

Purpose of this Chapter is to show that the constructed ROI model is able to calculate and illustrate different financial benefits of an identity management solution. Testing will be done by creating a case Company X which has very typical identity management problems and it wants to rationalize its identity management. First, I will explain and justify my testing method and use of fictional case company X. Second, I will introduce company X and explain their challenges related to identity management. Third, I will input case company X figures into the ROI model. Fourth, I will evaluate the results of the ROI model and make suggestions.

Fictional case company X is used because testing the ROI model's ability to produce financial measures, illustrative graphs and cash flow figures is not dependent on the values used for the calculations. Purpose of the ROI model is to be a guideline and tool for identifying different saving areas for the customer companies. Furthermore, purpose is not to test ROI model's estimates accuracy or validity but rather model's functionality. When testing the ROI model with help of company X's values, only simple mode of the ROI model will be used in order to keep testing more easily understandable and to avoid too much repetition of the previous chapter. Moreover, functionalities of the ROI model were tested in the phase of constructing the model and therefore this chapter acts more as a use case example.

Investigating ROI model's estimates accuracy would be good topic for further research. In this paragraph I describe how ROI model's accuracy could be tested in a real life case company. In an ideal testing situation the case company would have accurate data on its identity management costs before implementing RIMA solution. This identity management cost data could be then processed in the ROI model in order to create an estimate of possible cost savings that RIMA could deliver. After deployment of RIMA solution the case company would check its current identity management costs. Difference between old and current identity management's costs should then be compared with the estimates which the ROI model originally produced in order to see accuracy and validity of the ROI model's estimate. However, this kind of process is very complex and time consuming and therefore out of Master's thesis scope.

5.1 Case Company X Presentation and Their Motivation to Implement RIMA

Company X is a middle sized company which is now confronting identity management problems in its IT environment. Company X operates in telecommunication business and it employs 1000 person. Company X's employees need to use computer and various applications every day. However, company X's IT infrastructure is fragmented and they do not have clear picture what kind of access rights each employee have. Because company X operates in telecommunication business it is vital to know that employees have only required access rights. According to CIO there are probably many outdated accounts in Active Directory. In addition, CIO notes that they have estimated that they are paying 10 000€ for unneeded licenses because of active accounts who has no legitimate owner. Furthermore, company X's help desk is overwhelmed with users' password reset requests.

Case company's CIO tells that they have tens of applications which all are managed manually. According to CIO managing accounts manually is very time consuming and accounts are not always up to date. These outdated accounts are seen as a very serious information security threat. CIO elaborates that all the employees have basics accounts whose automatic creation and updating would ease administrators' job significantly. These accounts include AD account, email-account and phonebook account. Furthermore, CIO believes it is possible to automate also creation of other accounts if RIMA delivers wanted advantages.

Many different applications with different password policies cause problems to company X's employees in a form of forgotten passwords and locked accounts. CIO tells that company X's would like to have a tool that would allow employees to reset their forgotten passwords for the basic accounts. At the moment over half of Administrator's daily hours is spent in password related issues.

Case company X wants to see all the financial benefits that identity management solution can deliver but the main emphasis is in the following three areas:

- Decrease password reset calls to help desk
- Increase information security

- Automate reporting activities

5.2 Company X's Input Values for the ROI Model

In this subchapter I will present company X's input figures for the ROI model. Some of the figures will be discussed in more detail in order to grasp ideas behind them. However, most of the numbers are very basic attributes, such as employees with accounts or working hours which will not need any further explaining.

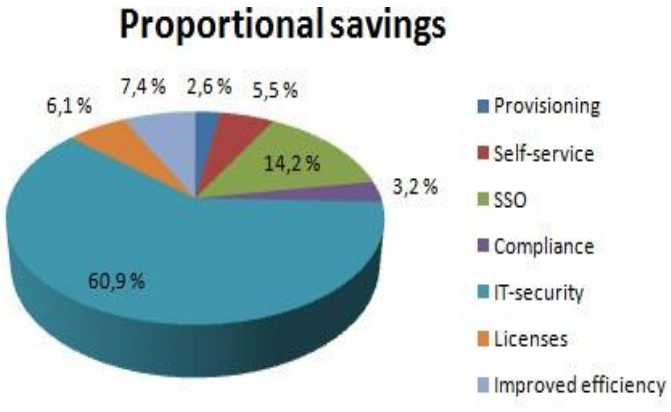
4	**Company information**		
5	Employees with accounts	1000	
6	Average amount of accounts/user	3	
7	Percentage of accounts/user (using workflow)	0 %	0
8	Percentage of accounts/user (using provisioning)	100 %	3
9	Average amount of users leaving company/year	80	
10	Average amount of employees hired/year	100	
11	Working days for employee in a year	230	
12	Working hours in a week (5days)	37,5	
13	Working hours in a year	1725	
14			
15	**Staff expense**	Yearly wage	Hourly wage
16	Average help desk worker	49 000,00 €	28,41 €
17	Average administrator	60 000,00 €	34,78 €
18	Average employee	70 000,00 €	40,58 €
19			
20	**Account creation/deletion details**	Hour	
21	Average time needed to create an account	0,25	
22	Average time needed to delete an account	0,2	
23	Average time needed to change role or user accounts	0,25	
24			
25	**Self Service (yearly rates)**		
26	Help Desk calls associated password change/reset per user	2	
27	Average length of a call	0,16	hours
28	Average account deletion requests/employee	0	
29	Average account change request/semployee	0	
30	Average account add requests/employee	0	
31	**SSO**		
32	Average amount of logins decreased per day	1	
33	Average time spent for typing credentials/service	9	seconds
34			
35	**Compliance**		
36	Manual reports produced/year	1	
37	Time to make one report	150	hours
38			
39	**Information security and licenses**		
40	Estimated cost of possible Information security threats	100 000 €	
41	Estimated cost of unneeded licenses paid every year	10 000 €	
42			
43	**Employees time saved (workflow+provisioning)**		
46	Average time saved/new employee	3	hours

Figure 21: Company X's input values

Figure 21 shows all the basic information about company X which is needed for performing ROI model calculations. Company X wanted to calculate advantages of RIMA's basic installation which includes three managed systems whose accounts are managed automatically. This is done by setting attribute "Average amount of accounts/user" to 3 and "percentage of accounts/user (using provisioning)" to 100%. This 100% means that all the user account are managed automatically. In Self service section only "Help Desk calls..." and "Average length of a call" attributes are filled in because company X did not want users to manage their accounts through self-service interface. Company X's administrators do once a year a report which purpose is to detect all the "extra" accounts in AD and this report is filled under Compliance section in the ROI model. Producing this kind of report manually is very time consuming and report's accuracy can be affected by the fact that the report is done manually. Company X has produced a information security threats analysis which reveals that cost of information security threats that identity management solution could prevent is 100 000€. Furthermore, company X estimates that by suspending and disabling AD accounts in timely manner could save them 10 000€ in license costs. Company X also estimates that their new employees will save on average 3 hours/new employee efficient working hours because accounts are automatically provisioned and they are usable at the very first working day.

5.3 Analyzing ROI Model's outputs for Company X

In this subchapter I will be analyzing results of the ROI model for company X and make conclusions. First, I will explore what the saving areas are for company X and their magnitude. After that I will move on to analyze financial measures and cash flows for company X.



Provisioning	2,6 %	4 278,26 €
Self-service	5,5 %	9 089,86 €
SSO	14,2 %	23 333,33 €
Compliance	3,2 %	5 217,39 €
IT-security	60,9 %	100 000,00 €
Licenses	6,1 %	10 000,00 €
Improved efficiency	7,4 %	12 173,91 €
total	**100 %**	**164 092,75 €**

Figure 22: Proportional savings for company X

Figure 22 illustrates different saving areas which company X can achieve by implementing RIMA solution. As Figure 22 shows, over 60% and 100 000€ of the savings cumulate from improved information security. This is directly based on company X's information security threats evaluation. Figure 22 also states that implementing SSO solution can bring considerable savings for company X. Also because new employees are able to get their accounts fast, company X could gain 7.4% of the savings in form of improved efficiency. Provisioning, on the other hand, does not seem to be very big factor in savings but it should be remembered that company X did not want its employees to manage their own accounts through self-service interface. Therefore provisioning savings include only new employees account creation costs and deletion costs when an employee leaves company X. Self-service saving area includes only savings cumulated from decreased password reset calls to help desk.

10	Year	0	1	2	3
11	Savings		155 538,16 €	148 012,14 €	140 848,11 €
12	Cumulative Savings	0,00 €	155 538,16 €	303 550,30 €	444 398,41 €
13	Costs	15 000,00 €	56 872,04 €	54 985,29 €	53 140,69 €
14	Cumulative Costs	15 000,00 €	71 872,04 €	126 857,33 €	179 998,02 €
15	Cash Flow	-15 000,00 €	98 666,12 €	93 026,86 €	87 707,42 €
16	Cumulative Cash Flow	-15 000,00 €	83 666,12 €	176 692,97 €	264 400,39 €
17					
18	Savings (not discounted)		164 092,75 €	164 741,22 €	165 389,68 €
19	Cost (not discounted)	15 000,00 €	60 000,00 €	61 200,00 €	62 400,00 €
20	Cash flow (not discounted)	-15 000,00 €	104 092,75 €	103 541,22 €	102 989,68 €
21					
22	NPV	264 400,39 €	Invest		
23	ROI	146,89 %			
24	IRR	692,047 %			
25	Pay back period (years)	0,14410225			

Figure 23: Company X's cash flows and financial measures

Figure 23 illustrates company X's cash flows and financial measures when investment period is set to three years, required return is 5,5 per cent and service level is good. At good service level company X's costs are 6€/identity/month. Figure 23 illustrates that company X's investment in RIMA would pay itself back very quickly already in first year. Also all the financial measures are in favor to invest in RIMA and NPV for three year investment period is over 264 000€. However, it should be remembered that many of these savings are not directly realizing for the company X. Improved information security, for example, does not increase direct cash flows but will prevent very costly information security threats from occuring.

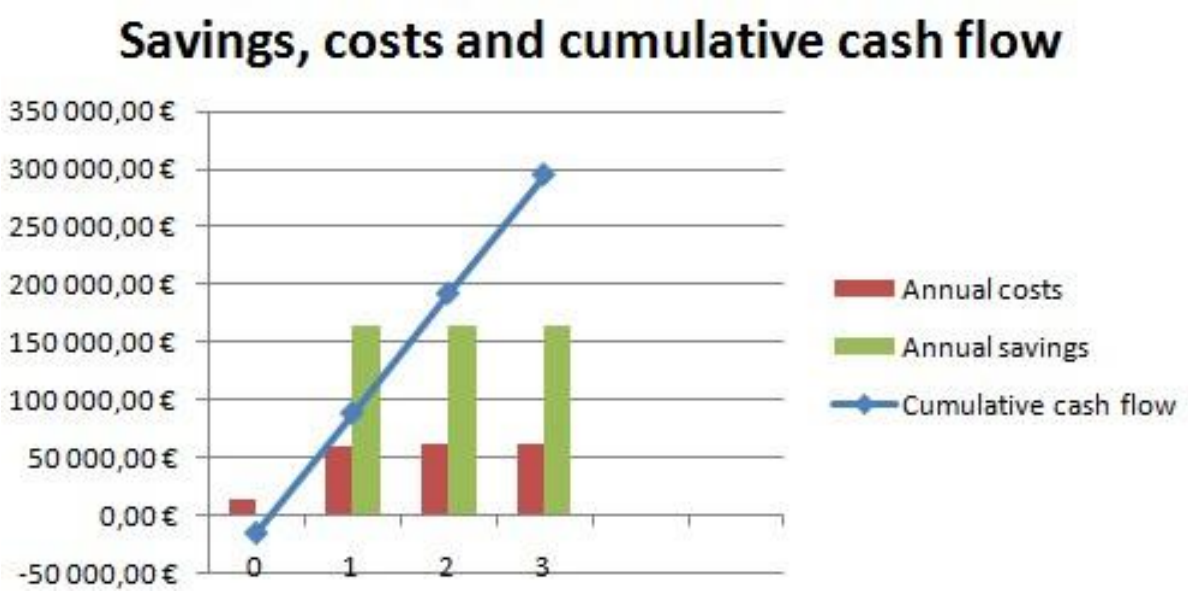


Figure 24: Savings, costs and cumulative cash flow for company X

Figure 24 illustrates well all the most important cash flows in the same picture for company X. It is clear from Figure 24 that annual savings for company X are much greater than the annual costs. In the left down corner of Figure 24 can be seen that break even for RIMA project is achieved in the very beginning of the first year.

Results from the ROI model indicate that implementing RIMA would be a good choice for company X. By implementing RIMA, company X could achieve necessary information security improvements, reporting capabilities and self-service tool for password resetting which were their greatest concerns. Furthermore, the ROI model illustrated to company X that they can also achieve savings from other saving areas with identity management solution.

Basis of this chapter I conclude that the ROI model is able to deliver desired outputs according to customer's input values and the assumptions related to the ROI model. The ROI model is able to illustrate different savings areas related to identity management, calculate financial measures and show yearly cash flows. These ROI model's outputs will help customer to better understand different financial affects of an identity management solution and help in decision making.

6 Discussion and Conclusions

The purpose of this study was to identify financial benefits that identity management solution can deliver for the companies and to construct a ROI model based on these benefits. There were only few academic researches on financial benefits of the identity management solution's implementation. Furthermore, there were no well crafted ROI models for identity management solutions publicly available. Therefore, in this study I identified key drivers and benefits behind the identity management solution implementation and constructed the ROI model based on these benefits.

6.1 Research Summary and Main Findings

This study utilized constructive approach which aims to solve a relevant problem by constructing a model. The ROI model was constructed in order to illustrate financial benefits of identity management solution and to justify investment in identity management. The ROI model was constructed especially to measure Logica's RIMA solution's financial benefits for the customer company but the model can be also used for analyzing other identity management solutions.

A vast literature review was conducted in Chapter 2 in order to gain better understanding of identity management and to identify key drivers and benefits behind identity management solution implementation. Identified drivers behind identity management solution implementation were improved efficiency, cost savings, information security, legislation and business performance. These identified drivers were utilized when constructing a conceptual model in Chapter 3. Furthermore, in Chapter 2 also the most common challenges related to identity management solutions were identified.

After acknowledging all the different characteristics of identity management solution in Chapter 2, I constructed a conceptual model of identity management solution's financial benefits in Chapter 3. Earlier identity management ROI models were inspected in Chapter 3 and a conceptual model was constructed based on the findings in these researches and benefits discussed in Chapter 2. In addition to tangible benefits, the conceptual model also recognizes

intangible benefits related to identity management solution. The constructed conceptual model was used also as a starting point for the ROI model that was constructed in Chapter 4.

In addition of constructing the ROI model, Chapter 4 also presents RIMA solution's architecture and different financial measures used in the ROI Model. Before the ROI model was constructed, RIMA solution was introduced from business and also from more technical point of view. Furthermore, different financial measures, such as NPV, IRR, ROI and payback period needed to be introduced and defined before constructing the ROI model. Chapter 4 presented different attributes and worksheets used in the ROI model. Furthermore, assumptions related to the ROI model were presented.

Finally, in Chapter 5 ROI model was tested by using fictional case company X's parameters and identity management related problems. Main purpose of Chapter 5 was to test that the ROI model is able to deliver desired outputs, such as financial measures and cash flows in a correct way. As a result of testing could be concluded that the ROI model is able to deliver desired outputs according to the assumptions and input values.

6.2 Discussion and Implications

The constructed ROI model is similar to models that were presented by earlier studies on identity management solution's financial benefits. However, implementing two different modes into same model was different from earlier approaches. Simple mode enables customer to get results faster and advanced mode can be used for defining different attributes more carefully in order to get more precise results. In selling situation it is important that the vendor is able to provide preliminary cost saving estimates quickly.

The ROI model is meant to be used in a selling situation in order to demonstrate possible cost savings that identity management solution can deliver for the customer. As mentioned before, the ROI model should be used only as a guide line to determine possible savings from identity management solution. At its best the ROI model will only give an estimate that is based on values that the customer provides. However, if all the provided numbers reflect the real

situation and all the assumptions presented are understood, the ROI model can give quite reasonable estimates.

One of the benefits of the model is easily modifiable attributes on the return worksheet which enables user easily to try out different scenarios. User can use slider and drop down menus in order to change service level, interest rate or time frame and see instantly how the changes affect on financial measures and cash flows of identity management project. Furthermore, informative and dynamically changing graphs make the ROI model more easily understandable for the customer. Therefore I believe that the ROI model can be used in a selling situation to demonstrate financial benefits of an identity management solution.

6.3 Limitations of the Study and Suggestion for Further Research

The conceptual model constructed in Chapter 3 has some limitations considering about its scope and relative strengths between different benefits and effects. First, the conceptual model does not take all the possible benefits related to identity management system into account. It would be merely impossible to identify and include all the possible benefits into a single model. Therefore only those benefits that I found to be the most relevant ones are included in the conceptual model. Second, the conceptual model does not consider relative strength between the benefits or their effects. Furthermore, causality of different effects has not been studied thoroughly. The conceptual model only depicts the most relevant effects of the benefits. Third, separation to revenue increasing and cost saving effects is not solid. Some of the effects may have both, cost saving and revenue increasing, abilities depending on the point of view.

The ROI model is only as good as the input data provided by the customer. The ROI model calculates all the results based on the reference values or the ones provided by the customer. Therefore the results can be very unrealistic if the assumptions have not been taken into consideration and input values do not reflect reality. It is important to keep in mind that the ROI model is intended to be only a guideline for evaluating possible cost savings.

The ROI model assumes that the cost savings are generated evenly throughout the year. In reality cost savings are not probably divided evenly throughout the year. Furthermore, the

ROI model shows only yearly cash flows. Some customers might want to see monthly or half yearly cash flows.

As mentioned before the ROI model will not take into account intangible benefits that identity management solution can deliver. Identity management solution can deliver many intangible benefits, such as improved business agility and personnel satisfaction. These intangible benefits are hard to convert into monetary values and therefore they are excluded from the ROI model. Because the ROI model considers the most important tangible benefits, it will not provide the full truth about the profitability of an identity management solution

As I described in earlier paragraphs, this study has many limitations and therefore I will now present suggestions for further research. First, it would be interesting to study more carefully intangible benefits related to the identity management solutions. Furthermore, a model could be constructed to convert these intangible benefits into monetary values. This way the whole value of an identity management solution could be calculated. Second, the ROI model's attributes could be examined in several real life companies in order to gain justified reference values which in turn would enhance model's credibility. SSO time savings, for example, could be easily calculated by comparing time used for logins before implementing identity management solution and after the implementation. Third, it would be interesting to investigate how the ROI model's results correlate with realized returns. This could be done by evaluating the customer company's realized savings against the forecasted ones. However, it might be hard to determine which savings are cumulated as a result of identity management solution implementation.

References

A10 Networks. (2006). *Identity management ROI calculation case study*. A10 Networks.

Alinean. (2002). *Tivoli ROI analyst methodology*. IBM Corporation.

Benantar, M. (2006). *Access control systems: Security, identity management and trust models*. USA: Springer.

Buecker, A., Filip, W., Dr., Palacios, J. C., & Parker, A. (2009). *Identity management design guide with IBM tivoli identity manager.* IBM Corporation.

Buecker, A., Karl, W., & Perttilä, J. (2008). *Deployment guide series: IBM tivoli identity manager 5.0* (Third Edition (December 2008) ed.) IBM Corporation.

Cronkhite, C., & McCullough, J. (2001). *Access denied: The complete guide to protecting your business online.* McGraw-Hill Professional.

Cser, A., & Penn, J. (2008). *Identity management market forecast: 2007 to 2014*. Forrester.

Florencio, D., & Herley, C. (2007). A large-scale study of web password habits. *WWW '07: Proceedings of the 16th International Conference on World Wide Web,* Banff, Alberta, Canada. 657-666.

Hewlett-Packard. (2004). *HP identity management – faster time to revenue and lower costs.* Hewlett-Packard

IBM. *Parsers.* Retrieved 14.12, 2010, from http://publib.boulder.ibm.com/infocenter/tivihelp/v2r1/index.jsp?topic=%2Fcom.ibm.IBMDI.doc%2Freferenceguide259.htm

IBM. (2007). *Identity and access management: Uncovering the secrets to successful implementations.* IBM Corporation.

The identity project. (2007). Retrieved 24.01, 2011, from http://www.angel.ac.uk/identity-project/Reports/WP7-FutureDevelopments.pdf

Jaferian, P., Botta, D., Hawkey, K., & Beznosov, K. (2009). A case study of enterprise identity management system adoption in an insurance organization. 7:46-7:55.

Jøsang, A., Zomai, M. A., & Suriadi, S. (2007). Usability and privacy in identity management architectures. *ACSW '07: Proceedings of the Fifth Australasian Symposium on ACSW Frontiers,* Ballarat, Australia. 143-152.

Kasanen, E., Lukka, K., & Siitonen, A. (1993). The constructive approach in management accounting research. *Journal of Management Accounting Research, 5*, 243-264.

Kho, N. D. (2009). THE changing face OF IDENTITY MANAGEMENT. *EContent, 32*(3), 20.

Lakner, G., Bobak, G., Cifka, J., Greene, K., Lachman, A., Taylor, J., et al. (2004). *Windows-based single signon and the EIM framework on the IBM eserver iSeries server.* IBM Corporation.

Molloy, I., Chen, H., Li, T., Wang, Q., Li, N., Bertino, E., et al. (2008). Mining roles with semantic meanings. *SACMAT '08: Proceedings of the 13th ACM Symposium on Access Control Models and Technologies,* Estes Park, CO, USA. 21-30.

OSM. (2005). *A CIO's guide to the return on investment (RoI) achievable through the implementation of user provisioning*. Open Systems Management.

Paavilainen, J. (1998). *Tietoturva*. Jyväskylä: Gummerus Kirjapaino Oy.

Peterson, B. H., Smedegaard, P., Heninger, W. G., & Romney, M. B. (2008). Managing multiple identities. *Journal of Accountancy, 206*(3), 38.

Pohlman, M. B. (2008,). *Oracle identity management: Governance, risk, and compliance architecture; 3rd ed.* Hoboken, NJ: Taylor & Francis Ltd.

RIMA. Retrieved 24.01, 2011, from http://www.logica.fi/we-are-logica/media-centre/articles/rima---identiteetin-hallintaa-palveluna/

Sarbanes-Oxley Act of 2002, (2002).

Sarbanes-oxley essential information. Retrieved 23.12, 2010, from http://www.sox-online.com/basics.html

STEPPING INTO identity management.(2006). *Computerworld, 40*(47), 22.

Summers, W. C., & Bosworth, E. (2004). Password policy: The good, the bad, and the ugly. *WISICT '04: Proceedings of the Winter International Synposium on Information and Communication Technologies,* Cancun, Mexico. 1-6.

Sun Microsystems. (2004). *The role of identity management in sarbanes-oxley compliance*. Sun Microsystems.

Viega, J., & Messier, M. (2004). Security is harder than you think. *Queue, 2*(5), 60-65.

Windley, P. (2005). *Digital identity.* O'Reilly Media, Inc.