Enterprise Identity Management – What's in for Organisations

Denis Royer (denis.royer@m-chair.net)
Johann Wolfgang Goethe University Frankfurt
Institute of Business Informatics
Chair of Mobile Business & Multilateral Security

Abstract: When introducing identity management systems (IMS), organisations have to face various costs for the actual planning, the implementation, and the operation of such systems. Besides the technological issues, organisational aspects have to be incorporated as well. Without a proper assessment of the costs and the organisational settings, companies will be less willing to introduce identity management (IdM) into their IT infrastructure and their business processes. This paper proposes a generic approach for assessing the costs and benefits related to the introduction of enterprise IMS (Type 1 IMS [1]), which can be used for decision support purposes in the planning phase. Furthermore, the organisational aspects are discussed and possible solutions are presented.

1. Introduction

Identity Management (IdM) with all its facets is becoming a more and more important issue for today's companies and corporations [3]. Especially with a diverse IT infrastructure being used in everyday's transactions (e.g. enterprise resource planning (ERP), document management (DMS), human resources management (HR)), organisations have to take care of their user and access management (identity and access management (IAM)), in order to protect their systems from unauthorised access (security) and to lower their overall costs (e.g. for keeping account data up-to-date or for helpdesk activities).

Furthermore, the *identity lifecycle* has to be managed, since employees change departments or get promoted. Therefore, the following process steps need to be handled as well [8, 14]:

- ***Enrolment - Creation of accounts for new employees:*** issuance of the credentials and setting of the access permissions.

- ***Management - Maintenance of accounts:*** in changing working environment (promotions, change of departments, etc,) the user and access management needs to handle the access permission (e.g. for minimising liabilities).
- ***Support - Password management:*** issue new passwords or reset passwords that are “lost”.
- ***Deletion - End of lifecycle:*** revoke or freeze accounts or entitlements.

In order to support this lifecycle, organisations use so called type 1 identity management systems (IMS), which fulfil the function of the authorisation, the authentication, the administration, and the audit of the user accounts that need to be managed [1].

Moreover, the driving factors for introducing IMS into an organisation can be found in (1) value creation, (2) IT risk management, or (3) compliance goals[1] (see also Table 1). Without a proper management of the identity lifecycle, companies have to face losses in their productivity (e.g. increasing costs for managing their IT infrastructure), the risks associated with potential security leaks, such as incoherently managed user accounts, or the issue of not being compliant with relevant laws and regulations.

Table 1. Driving Factors for IdM in Organisations

1. Risk Management / IT Security Goals
• Minimise liabilities • Mitigate risks • Make systems more secure
2. Value Creation Goals
• Efficiency goals (e.g. process optimisations) • Lower overall costs
3. Compliance Goals
• Comply with relevant laws and regulations (e.g. Basel II or SOX)

However, without a thorough cost-benefit analyses, no decision maker will invest into IT security related topics, such as IdM. Therefore, concrete methodologies are needed to serve as a decision support instrument for the decision makers in an organisation. A generic approach to tackle this is presented in this paper.

This paper is structured as follows: The second section describes the general cost situation for the introduction of IdM. Ongoing some of the general problems for IdM projects are described. The third section describes the evaluation process for the return of such projects as a means for decision support. Here, the general prerequisites and the stakeholders are described as well. Furthermore, some of the organisational aspects are presented and discussed. The last chapter summarises the findings and gives an outlook on further research questions.

[1] In IdM, ***compliance*** refers to corporations and public agencies to ensure that personnel are aware of and take steps to comply with relevant laws and regulations (e.g. Basel II or SOX).

2. The Cost for Introducing IdM

According to a recent study conducted by Deron, the costs for creating or deleting users/employees are reduced by 50% when using an IdM solution. The total costs for the user management are even reduced by 63%, compared to a manual management of the user accounts and the related transactions [4].

However, when introducing IdM solutions, companies have to face significant costs. According to a recent survey on 3.500 German companies by Deron [4], IdM projects can easily exceed costs of 100.000€ and more for the actual IdM solution being used and the consulting necessary to implement and introduce such systems into a company. Furthermore, there are additional factors that have to be taken into consideration:

- IdM itself is not a purely technology driven topic, since it directly intervenes with the everyday processes, workflows, and the organisational structure of a company. So, when introducing IMS, organisational factors have to be recognised as well:
  - Who is responsible for maintaining the accounts?
  - Who defines the necessary processes?
  - Who enforces the policies being set?
- The nature of IdM projects is diverse and there are various goals for introducing this technology (cp. Table 1). While the requirements for one project include the increase of the overall security, other projects deal with issues such as compliance or provisioning as driving factors. Here, the project inherent requirements have to be gathered and analysed to come up with a more generalised view, as projects are not alike.
- Moreover, IMS are not products, but frameworks of different technologies (meta-directories, SSO, workflow management, etc.). Therefore all projects are unique, which makes it difficult to come up with a general cost assessment for the implementation and introduction of IdM [14].
- Last but not least, the costs associated with the lifecycle of an IdM solution (lifecycle costs) need to be gathered. These costs include items such as training, migration of legacy systems, etc [13].

So, while IMS offer high cost saving potentials, they also have high investment costs associated with the planning, the implementation, and the operation.

3. The Evaluation Process

In order to perform a cost-benefit analysis, decision maker need concrete methodologies to assess the overall return on investment (ROI), which need to fulfil several prerequisites. This includes e.g. the incorporation of the driving factors for introducing IdM.

Besides its many different technical and financial definitions, the term *return on investment (ROI)* generally refers to the degree of how efficient the capital invested into a project is used to generate profit [12, 13]. Looking at this, it is reasonable to expect that the higher the actual ROI of a project is, the higher will be its competitivity and its likelihood to be executed by the decision makers in an organisation.

From the viewpoint of the investment process, ROI analyses are performed for two general purposes:

1. For determining the degree of fulfilment after a project was executed. This is especially used as a measure for project performance.
2. As a decision support tool for comparing similar investment opportunities or the question whether a project should be generally executed.

The article at hand will focus on the latter point, of using ROI analyses as a decision support instrument.

3.1 The Paradox of the return of IdM Investments

One of the starting points for analysing the ROI of IT security related projects is the structure of the project itself. Having a huge strategic impact on the whole organisation and its structure (changes in processes, etc.), IdM projects need to be analysed in a holistic way, including factors like people, structure, task, and technology.

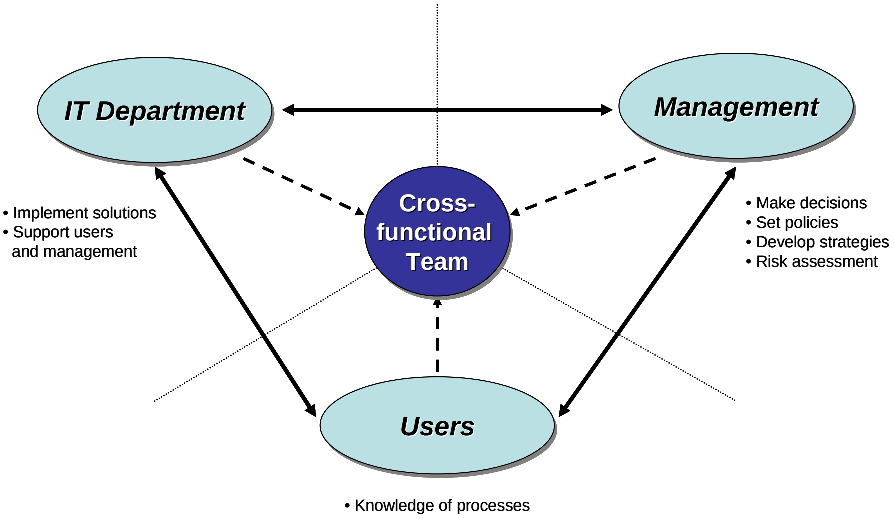

Fig. 1. Stakeholders model for introducing IdM in an organisation.

So, while technology changes (or can be changed) rapidly, the organisational factors need to be taken into consideration as well. Without a proper change management and an involvement of all stakeholders, it is unlikely that the strategic goals set (cp. Table 1) for introducing IdM into an organisation can be achieved and that the benefits and potentials of the expenditures into IdM can be achieved within a set time-frame [5]. Literally speaking, even though companies invest in IdM solution to achieve the presented goals, they fail to see the "big picture" and therefore cannot achieve the return aimed at, which leads to a productivity paradox.

One of the possible ways to overcome this paradox is to build *cross-functional teams*, integrating all the stakeholders into the process of introducing IdM into an organisation. By doing this, strategic thinking throughout the organisation can be enabled, helping to get all the aspects and requirements, reframing the role of IdM in the organisation, and to overcome possible language barriers in the communication between the stakeholders [5, 12]. The different groups and their roles/tasks are presented in Figure 1.

Moreover, having a general overview of all the affected processes and stakeholder groups, it is easier to identify the possible costs and benefits, which can be achieved by this type of technology. Therefore, it is beneficial when a cross-functional team is working on a cost-benefit analysis, so all factors can be identified sufficiently.

3.2 Prerequisites for an Evaluation Scheme

Generally, when analysing IT investments, the evaluation scheme must fulfil several prerequisites in order to produce an adequately complete and thorough analysis of the subject's matter [9]. The presented prerequisites should help a cross-functional team to adequately build a decision support instrument:

- First, the underlying assumptions taken as basis for an analysis need to be realistic. This can be achieved by analysing other IdM projects, using their results as reference/benchmark object for deducting the related costs.
- The modelling of the underlying environment should also take additional cost factors into account, such as development costs, migration costs, and other costs related to the lifecycle of an investment.
- Based upon the gathered data, it is important to determine the impact and interaction of the different parameters to get a complete picture of the cost effects being present in the analysed case.
- Evaluations, using static finance-mathematical methods, should be avoided. A better way of determining the worth of an investment is to use dynamic methods, such as the internal rate of return (IRR) or the net present value (NPV) [6]. While the static methods work with periodic mean values, the dynamic methods examine the actual present value over the complete runtime of an investment. The main difference is the consideration of the cash in- and outflows and their present value over time. This gives a more accurate view upon the development of the investment than just an average value [2].
- Although a thorough collection and analysis of the present data is a good foundation for an evaluation, one has to deal with uncertainties in the development of the parameters [11]. In order to adequately forecast such effects, methods such as the scenario technique presented by Geschka and Hammer offer a good method to asses them [7].
- For the decision support, most often it is not possible to determine all data with a 100% accuracy within an acceptable timeframe. Therefore some degree of

compromise is necessary. So, when preparing the data, one has to keep in mind that most of the time the results only need to be sufficiently accurate for decision making processes. Also, the methods used should incorporate into existing approaches, in order to minimise potential incompatibilities when building the evaluation scheme [12].

- Finally, the results have to be comprehensible for third parties, in order to allow the validation of the initial assumptions [6] and to support the decision making process.

3.3 Operationalise IdM Projects

One of the initial steps of a cross-functional team is the operationalisation of the overall plan for introducing of IdM into an organisation. This is needed to cut down on complexity, as this approach helps to analyse the costs and benefits of manageable sub-projects. Moreover, a step-by-step introduction helps to minimise potential failures [12]. For this purpose, the author proposes the following steps to be taken for an analysis:

1. Analyse organisational environment in order to derive strategic goals for the introduction of IdM and IMS (cp. Table 1).
2. Build holistic view on organisation based on the derived strategic goals, building a global plan for introducing IdM.
3. Divide the global plan into smaller *sub-projects*, which can be executed step-by-step.
4. *Evaluate the sub-projects (see next section).*
5. Determine the sequence of the *sub-projects* based-on their return for the later execution of the plans.

3.4 Structure of the actual Evaluation Process

As a next step, the actual analysis for the sub-projects is prepared. The proposed process is build upon the prerequisites and the operationalisation presented earlier. For the actual evaluation process, an extended model of the evaluation process proposed by Pisello was used [10], dividing it in 7 steps:

- ***Step 1:*** assessment of the organisational view on IdM in order to derive strategic goals for its introduction. What should be achieved by introducing IdM?
- ***Step 2:*** define and document the project's scope (what should be analysed) based on the strategic determinates set earlier.
- ***Step 3:*** define all project costs including all investments into hardware & software, license fees, and labour (e.g. consulting).
- ***Step 4:*** document and estimate potential *tangible benefits* including all direct (budgeted) and indirect (unbudgeted) savings and gains. Examples are potential saving in optimised processes that lead to less support requests.
- ***Step 5:*** document intangible benefits. What else does the project help to achieve (e.g. being compliant with laws, offering interoperability, extensibility)?

- ***Step 6:*** document the possible risks such as resources, schedule, staffing, or legal and determine what *tangible and intangible impacts* they may have on the analysed case.
- ***Step 7:*** calculation of the potential return, based on the tangible benefits *and* the potential impacts of the risks.

One of the modifications being introduced into this process was the incorporation of the potential risks being associated to IdM. This is necessary, as IT security investments, such as IdM, help to reduce/mitigate potential risks. Furthermore, this helps to get a more accurate view on the benefits, which can be derived from this kind of technologies [12].

Moreover, the presented process heavily relies on the documentation of the performed steps and the evaluation of the benefits (tangible, intangible) and the costs. In the opinion of the author, this helps third parties to comprehend and validate the results more easily.

3.5 Discussion

The proposed evaluation process should help to assess the benefits and costs related to IdM in a formalised way, introducing the associated risk into the process as an additional factor. As projects differ in their scope, a formalised process helps to keep track of the project-inherent factors, helping the decision makers to assess the introduction of IdM technology in a more transparent way.

As presented, the decisions made by a cross-functional team need to be done on the basis of the strategic overview, in order to get the correct order of actions to be taken. Therefore, all stakeholder need to be involved, as all groups play a vital role for assessing the overall IdM strategy (see Figure 1). Here, the affected (business) processes that intervene with the IdM in an organisation are the focal point to look at. They need to be acquired, analysed, formalised and documented in an appropriate way to get an overview on what is needed, where.

From the author's point of view, formalised process models are needed, in order to support the decision makers when planning the IdM strategy for an organisation. Such process models need to address the special requirements for IdM solutions, such as the roles, the access permissions, the affects business process, and the lifecycle of the identities being present in an organisation. Also, this would help to better identity the risks associated with IdM.

4. Summary and Outlook

When introducing IMS, companies have to face various costs for the implementation and the related organisational aspects. This paper presents a formalised process for assessing the costs and benefits related to IMS, taking the presented facts and prerequisites into consideration. Based on this, cost assessment, companies are offered a method for better planning the introduction of IMS and to help in their decision making process.

However, besides cost assessments, process models are necessary in the future, to streamline the development and implementation process of enterprise IMS, since there is no unified way of modelling such systems, yet.

References

[1] Bauer, M. and Meints, M. (eds.), Deliverable D3.1: Structured Overview on Prototypes and Concepts of Identity Management Systems, available at www.fidis.net (2005).

[2] Blohm, H. and Lüder, K., Investition, Schwachstellenanalyse des Investitionsbereichs und Investitionsrechnung, 8th edition (Vahlen, Munich, 1995).

[3] Camp, J.S. and DeBlois, B., Current Issues Survey Report 2007, Educause Quarterly, no. 2/2007, pp. 12-31 (2007).

[4] Deron, Identity Management Studie 2006/2007 (March 15th 2007); http://www.deron.de/studie_idm_2006.

[5] Dos Santos, B. and Sussman L., Improving the return on IT investment: the productivity paradox, International Journal of Information Management, vol. 20, pp. 429-440 (2000).

[6] Franklin jr., C. The ABCs of ROI, in: Network Computing, 29th April 2002, p.93–95 (2002).

[7] Geschka, H. and Hammer, R., Die Szenario Technik in der strategischen Unternehmensplanung, in: D. Hahn, B. Taylor, Strategische Unternehmensplanung - strategische Unternehmensführung, 7th edition (Physica , Heidelberg, 1997), pp.464-489.

[8] Hansen, M. and Meints, M., Digitale Identitäten – Überblick und aktuelle Trends, Datenschutz und Datensicherheit (DuD), vol. 30, no. 9, pp. 571 – 575 (2006).

[9] Rossnagel, H., Royer, D., Investing in Security Solutions - Can Qualified Electronic Signatures be Profitable for Mobile Operators, Proceedings of the 11th Americas Conference on Information Systems (AMCIS), Omaha, Nebraska, AIS, pp. 3248-3257 (2005).

[10] Pisello, T., Return on Investment for Information Technology Providers (Information Economics Press, New Canaan, 2001).

[11] Potthof, I., Kosten und Nutzen der Informationsverarbeitung: Analyse und Beurteilung von Investitionsentscheidungen (DUV/Gabler, Wiesbaden, 1998)

[12] Purser, S.A., Improving the ROI of the security management process, Computers & Security, vol.6, no. 23, pp. 542-546 (2004).

[13] Schmeh, K. and Uebelacker, H., Sicherheit, die sich rechnet - Return-on-Investment in der IT-Security (May 30th 2006); http://www.heise.de/tp/r4/artikel/18/18954/1.html.

[14] Windley, P.J., Digital Identity (O'Reilly, Sebastopol et.al., 2005).

Denis Royer was born in Germany in 1977. He completed his master in business informatics in 2003 at the University of Technology at Braunschweig (Germany). From 2000 to 2001 he studied information systems and business administration at the University of Nebraska @ Omaha, Nebraska (USA). Since 2004 he is a researcher and project coordinator of the FIDIS NoE (www.fidis.net) at Johann Wolfgang Goethe – Universität in Frankfurt, Germany. At the chair for Mobile Commerce and Multilateral Security, he works on the economic evaluation of identity management systems, IdM process models, and IdM meta-models in the context of the European research project FIDIS (Future of Identity in the Information Society).