Enterprise Identity Management

What's in it for Organisations?

Denis Royer

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

Abstract. When introducing enterprise identity management systems (EIMS), organisations have to face various costs for the planning, the implementation, and the operation of such systems. Besides the technological issues, it is important that organisational aspects are incorporated into the development of an enterprise identity management (EIdM) solution as well. Indeed, without a proper assessment of the costs and the organisational settings (e.g. stakeholders, processes), companies will not see the benefit for introducing EIdM into their IT infrastructure and their business processes. This paper proposes initial ideas for a generic approach for assessing the value of investing in the introduction of EIMS (Type 1 IMS), which can be used for decision support purposes and the planning phase. Furthermore, the organisational aspects are discussed and possible solutions for integrating all relevant parties into the planning process are presented.

1 Introduction

Enterprise Identity Management (EIdM) is becoming an increasingly important issue for companies and corporations [7]. 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 (involving security and privacy implications) and to lower their overall costs (e.g. for keeping account data up-to-date or for helpdesk activities). This is especially so, given the diverse IT infrastructures being used in everyday transactions (e.g. enterprise resource planning (ERP), document management (DMS), human resources management (HR)).

Furthermore, the *identity lifecycle* needs to be managed, since employees change departments or get promoted. Therefore, the following process steps need to be handled as well [12, 27]:

- ***Enrolment - creation of accounts for new employees:*** issuance of the credentials and setting of the access permissions needed by the new employee
- ***Management - maintenance of accounts:*** in a changing working environment (promotions, changes of departments) the "*user and access management*" needs to handle the changing access permissions for the enrolled users (in order to minimise liabilities)

Please use the following format when citing this chapter:

Royer, D., 2008, in IFIP International Federation for Information Processing, Volume 262; The Future of Identity in the Information Society; Simone Fischer-Hübner, Penny Duquenoy, Albin Zuccato, Leonardo Martucci; (Boston: Springer), pp. 433–446.

- ***Support - password management:*** issue new passwords or reset passwords that are "lost"
- ***Deletion - end of lifecycle:*** revoke or freeze user-accounts or entitlements

Based on the IMS categorisation presented by Bauer, Meints and Hansen [1], organisations use so-called *type 1* identity management systems (IMS). Supporting the lifecycle of identities on the organisational level, this group of systems fulfils the functions of authorisation, authentication, administration, and audit of the user accounts that need to be managed.

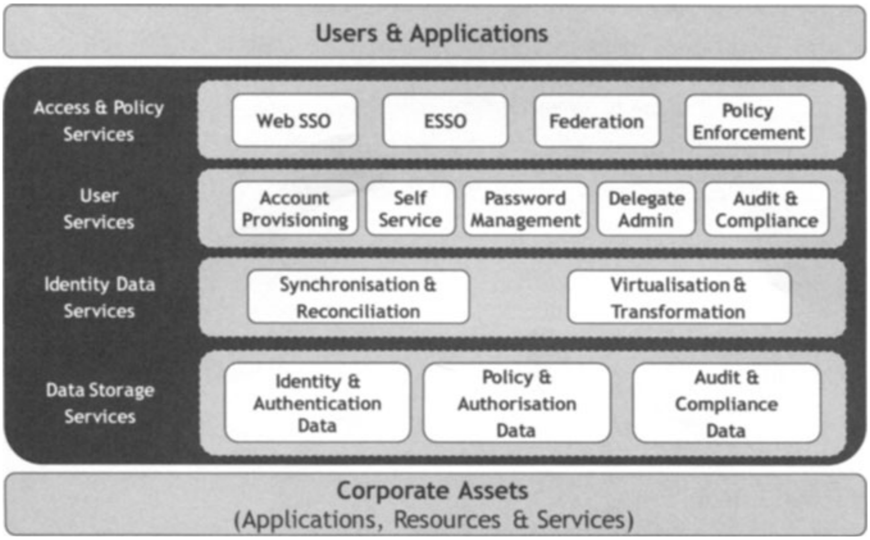


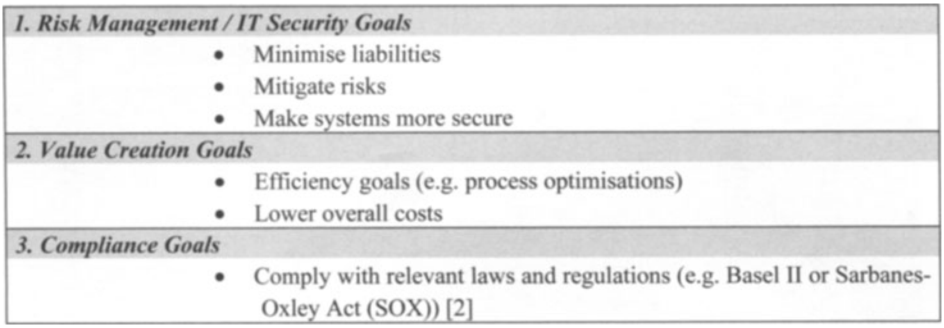
Fig. 1. EIdM technology framework based on Flynn [9].

At the technological level, a variety of technologies can be identified, belonging to the cluster of EIdM technologies, for example single-sign-on (SSO), meta-directories, public-key infrastructures (PKI), and IAM systems [9, 27]. Therefore, EIdM can be considered a framework of different technologies, rather than a product or an out-of-the-box solution (cp. Figure 1).

1.1 Driving Factors for EIdM

There are a variety of driving factors for introducing enterprise identity management systems (EIMS) into an organisation. Based on an explorative study (expert interviews), conducted by the author, the most prevalent factors appear to be (1) value creation goals, (2) IT risk management goals, and (3) compliance goals[1] (cp. Table 1). Without proper management of the identity lifecycle, companies may face losses in their productivity (increased costs for managing their IT infrastructure), risks associated with potential security leaks (resulting from incoherently managed user accounts) or ramifications for non-compliance against relevant laws and regulations [2]. However, the presented goals are not mutually exclusive. Table 1 gives an overview of the driving factors identified so far:

Table 1. Most prevalent factors for implementing IdM in organisations[2].



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 Sarbanes-Oxley Act (SOX)) [2]

1.2 Goal of this paper

Without a thorough cost-benefit analysis, no decision maker will invest in IT security related technologies such as EIdM. The question "*What's in it for Organisations*?" needs to be answered, using concrete methodologies that serve as a decision support instrument for the decision makers in an organisation. Consequently, the question "*How can investments into EIdM be evaluated?*" needs to be researched and answered as well. This paper strives to present initial ideas on how a generic approach can be constructed, which should help to consistently assess the value (including risks, costs, and benefits) of EIdM in organisations.

This paper is structured as follows: Following the introduction (1), the second section (2) discusses the underlying research approach needed to carry out the research in this field. The third section (3) introduces general cost and benefit aspects for the introduction of EIdM and some of the general problems encountered in EIdM projects. Next, the fourth section (4) describes the proposed evaluation process as a starting point for assessing the costs and benefits 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 section (5) summarises the findings and gives an outlook on further research questions.

[1] In this context, ***compliance*** refers to corporations and public agencies needs to ensure that personnel are aware of, and take steps to comply with relevant laws and regulations (e.g. Basel II or Sarbanes-Oxley Act (SOX)) [2].

[2] These factors are based on an explorative expert interview conducted by the author.

2 Research Approach

In order to answer the posed research question, a self-developed, 3-staged research approach, based on the design science framework by Hevner et al. [13], will be used. The (primary) artefact to be designed is a framework for assessing the value of EIdM in organisations (including its requirements and properties), including the approach described in this paper. The constructed design process itself is divided in 4 *sub-questions*, which are used to further structure the different stages:

- ***Sub-Question 1:*** Which are the methods that can be used to assess the value of EIdM?
- ***Sub-Question 2:*** Which of these methods applied in practice (that is, in the corporate field for decision support) and how?
- ***Sub-Question 3:*** What are the actual requirements and properties that are needed to assess the value of EIdM and how can they be formalised into a framework?
- ***Sub-Question 4:*** How can the framework (including its requirements and properties) be applied into a decision support instrument for the assessment of EIdM?

The individual stages and sub-questions are visualised in Figure 2. The *first stage* of the designed research approach deals with the problem identification and the analysis of the problem relevance of the presented research questions. Here the foundations for the further research will be laid out and discussed, including the hypotheses building.

The *second stage* depicts the actual design process and the creation of the researched artefact(s). Within this stage, the first 3 sub-questions (1-3) will be discussed. Sub-question 1 will begin with a literature review of the available methods to assess the value of EIdM and IT security investments in general (assessment of the "state-of-the-art"). This will help to identify the available methods and to assess their advantages and disadvantages. The next sub-question (2) will be answered by using expert interviews. The targeted experts will be practitioners in the field of EIdM, who will be asked which methods are actually used in real-life, and why certain methods are (not) used. Based on these results, the requirements for a framework to assess the value of investments into EIdM will be derived (based on the framework by Lee [16]). The synthesis of the results of the first 2 sub-questions is discussed in the 3rd sub-question. Here, the framework (the primary artefact), its requirements, and its properties for assessing the value of EIdM will be derived (representing the research contribution). Furthermore, a generalised outline for how the framework can be used in practice and design recommendations will be presented (secondary artefacts). The search process for the artefacts will be iterative, coupling feedback loops to the 1st and 2nd sub-question.

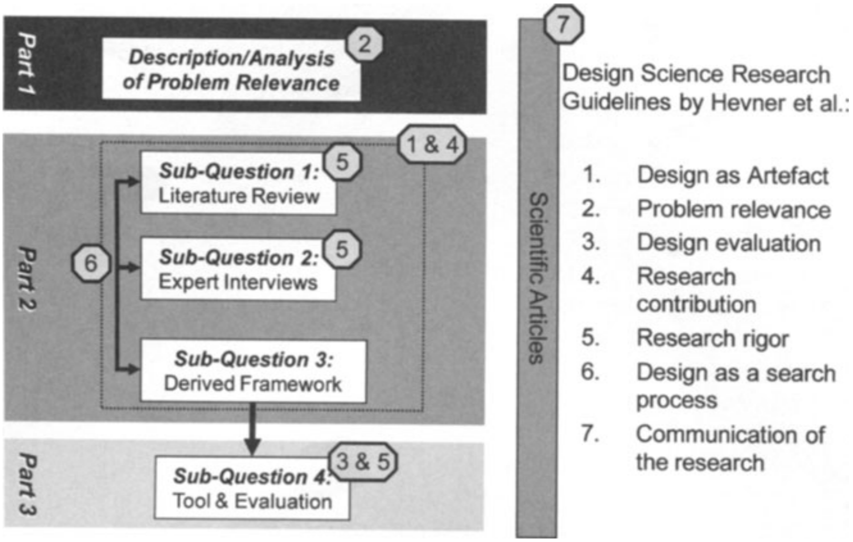

Part 1
Description/Analysis of Problem Relevance
2
1 & 4
Sub-Question 1: Literature Review
5
6
Sub-Question 2: Expert Interviews
5
Sub-Question 3: Derived Framework
Part 2
Sub-Question 4: Tool & Evaluation
3 & 5
Part 3
Scientific Articles
7
Design Science Research Guidelines by Hevner et al.:
1. Design as Artefact
2. Problem relevance
3. Design evaluation
4. Research contribution
5. Research rigor
6. Design as a search process
7. Communication of the research

Fig. 2. Research approach based on the design science framework by Hevner et al. [13].

In order to validate the designed artefacts (design evaluation), the 4th sub-question (*3rd stage*) of the presented research approach will test the framework in practice. In order to do this, a prototypic decision support instrument for the assessment of the value for introducing EIdM will be implemented (instantiation of the framework). For the actual evaluation of the design, a combination of case study research and expert interviews is planned, analysing how the proposed evaluation framework improves the decision making process in practice.

The paper at hand discusses the *first stage*, including the analysis of the problem and its relevance. Furthermore, initial ideas and requirements (based on the initial literature review) for an evaluation process will be presented, which serve as a component of the evaluation framework.

3 Cost and Benefit Aspects for Introducing EIdM

According to an explorative study conducted by Deron, the costs for creating or deleting users-accounts are reduced by 50% when using an EIdM solution. The total costs for the user management are reduced by up to 63%, compared to manual management of the user accounts and the related transactions [6].

However, when introducing EIdM solutions, companies have to face significant costs. According to Deron's survey of 3,500 German small to mid-sized companies [6], EIdM projects can easily exceed €100,000 and more in total cost (for the actual EIdM solution being used, and the consulting necessary to implement and introduce such systems into the company).

From the author's point of view and based on the conducted literature review, there are additional factors that have to be taken into consideration as well. These include:

- EIdM itself is not a purely technology-driven topic since it directly intervenes with everyday processes, workflows, and the organisational structure of a company. So, when introducing EIMS, organisational factors have to be recognised as well:
  - Who is responsible for maintaining the accounts?
  - Who defines the necessary policies, and on what basis?
  - Who defines the necessary processes for managing the identity lifecycle?
  - Who enforces the policies being set?
- The nature of EIdM projects is diverse and there are various goals for introducing this technology (cp. Table 1). While the requirements for one project may include the overall increase of security, other projects are driven by issues such as compliance or provisioning. The projects' inherent requirements have to be gathered and analysed to come up with a more generalised view to cope with this variation.
- As stated before, EIMS are not products, but frameworks of different technologies (meta-directories, SSO, workflow management, etc.) that can be integrated into an (existing) IT infrastructure (cp. Figure 1). Therefore all projects are unique, which makes it difficult to come up with a general cost assessment for the implementation and introduction of EIdM [27].
- Last but not least, the costs associated with the lifecycle of an EIdM solution (lifecycle costs) need to be considered. These costs include items such as training, upgrading and integrating existing EIdM infrastructures, and migration of legacy systems, etc. [23].

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

4 Development of the proposed Evaluation Process

In order to perform a cost-benefit analysis, decision makers need concrete methodologies and evaluation processes to assess the value of EIdM investments (based on the widely used *return on investment (ROI)* business ration). Such methodologies need to fulfil several prerequisites. These include the incorporation of the driving factors for introducing EIdM (cp. Table 1).

Besides its many different technical and financial definitions, the ROI generally refers to the degree of how efficiency by which the capital invested into a project is used to generate profit [21, 23]. Looking at this, it is reasonable to expect that the higher the actual ROI of a project is, the higher will be its competitiveness (compared to other investment alternatives). The same applies to the likelihood that the project will actually 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 or not.

Here, we will focus on the latter point, of using ROI analyses as a decision support instrument.

4.1 EIdM, the IT Productivity Paradox, and the Return on EIdM Investments

One of the starting points for analysing the ROI of IT security related projects is the structure of the project itself. As shown initially, EIdM technologies need to be integrated on the process level of an organisation. The introduction of an EIMS will most likely have a huge impact on the whole organisation and its structure (changes in processes, etc.). Therefore, EIdM projects need to be analysed in a holistic manner, including factors such as people, structure, task, and technology.

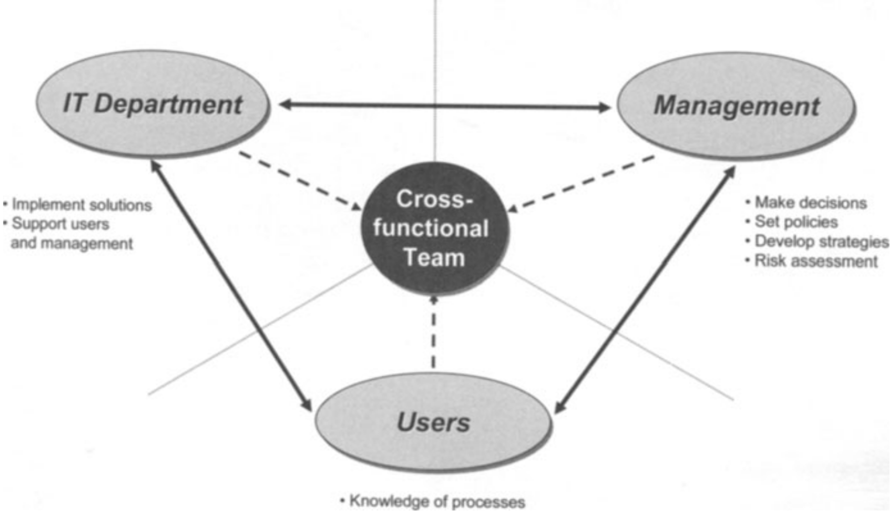


Fig. 3. Stakeholders involved in the process for introducing EIdM into an organisation and their roles (own representation based on Dos Santos [8]).

So while technology changes (or can be changed) rapidly, the organisational factors need to be taken into consideration as well. Without proper change management and the involvement of the stakeholders, it is unlikely that the strategic goals (cp. Table 1) and potentials of the expenditures for introducing EIdM can be achieved within a set time-frame [8, 17]. Even though companies invest in EIdM solutions to achieve the presented goals (e.g. risk mitigation), they may fail to see the "*big picture*" and therefore will not achieve the returns they aimed for. This leads to the effect referred to as the *IT productivity paradox* [4, 14, 26].

One of the ways to ameliorate the negative consequences of introducing EIdM is by *cross-functional teams*, integrating all the stakeholders into the process of introducing EIdM into an organisation. By doing this, strategic thinking throughout the organisation can be enabled, including all aspects and requirements, reframing the role of EIdM in the organisation, and overcoming possible language barriers in the communication between the stakeholders [8, 21]. The different groups and their roles/tasks are presented in Figure 3. Moreover, by having a general overview of all the affected processes and stakeholder groups, it is easier to identify the possible costs and benefits [24] which can be achieved by this type of technology.

Similar to the IT productivity paradox, the evaluation of IT security investments is also discussed widely in scientific literature [5, 17, 25]. Besides the various inherited problems of general IT investments, such as the described productivity paradox [4, 26], EIdM and IT security investments suffer from additional problems [17, 25]. These include the identification of (possible) revenues generated by an IT security investment or the optimal level of the total security investments. Furthermore, IT security investments are carried out to mitigate risks and to prevent possible losses [25]. If indeed the risks are mitigated and occurrences of security incidents and potential losses are prevented, it is difficult to assess whether an investment can be established cost-effective, due to the preventive nature of IT security investments.

In scientific literature several methods and frameworks are discussed that should help to assess the economic impact and the value of IT security investments, such as the return on security investments (ROSI) [5, 17, 25]. Depending on the taken approach, ROSI tries to monetarise IT security investments, for example by analysing the productivity losses associated to security breaches. However, extended metrics incorporating organisational settings and intangible factors seem necessary, in order to evaluate the return on EIDM investments. As laid out in the research approach, the analysis of these methods and frameworks will be subject of the future research in this field.

4.2 Prerequisites for an Evaluation Scheme/Process

Generally, when analysing IT investments, an evaluation scheme must fulfil several prerequisites in order to produce a sufficiently complete and thorough analysis of the subject's matter [22]. Based on the literature research, the presented prerequisites should help a cross-functional team to adequately build a decision support instrument:

- First, the underlying assumptions taken as a basis for an analysis need to be realistic. This can be achieved by analysing other EIdM projects in the same industry, using their results as a reference/benchmark for deducing 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 the 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 (e.g. ROI) 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) [10, 14]. 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 [3, 25].
- 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 [20]. In order to adequately forecast such effects, methods, such as the scenario technique presented by Geschka and Hammer, offer a good way to assess them [11], as they give a possible range for the actual outcome of an investment.
- For decision support, it is not possible to determine all data with 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 an evaluation scheme [21].
- Finally, the results have to be comprehensible for third parties, in order to allow the validation of the initial assumptions[10] and to support the decision making process. In order to achieve this, the methods for the assessment of the risks, the costs, and the benefits, need to be consistent/ standardised [21, 25].

4.3 Operationalisation of EIdM Projects

One of the initial steps of a cross-functional team is the operationalisation of the overall plan for introducing EIdM 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 [21]. For this purpose, the author proposes the following steps to be taken for (preparing) an analysis:

1. Analyse the organisational environment in order to derive strategic goals for the introduction of EIdM (cp. Table 1).
2. Build a holistic view of the organisation based on the derived strategic goals, deriving a global plan for introducing EIdM.
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.

The described process is visualised in Figure 4. The feedback loops introduced in steps 1 to 3 help to improve the results of the process itself.

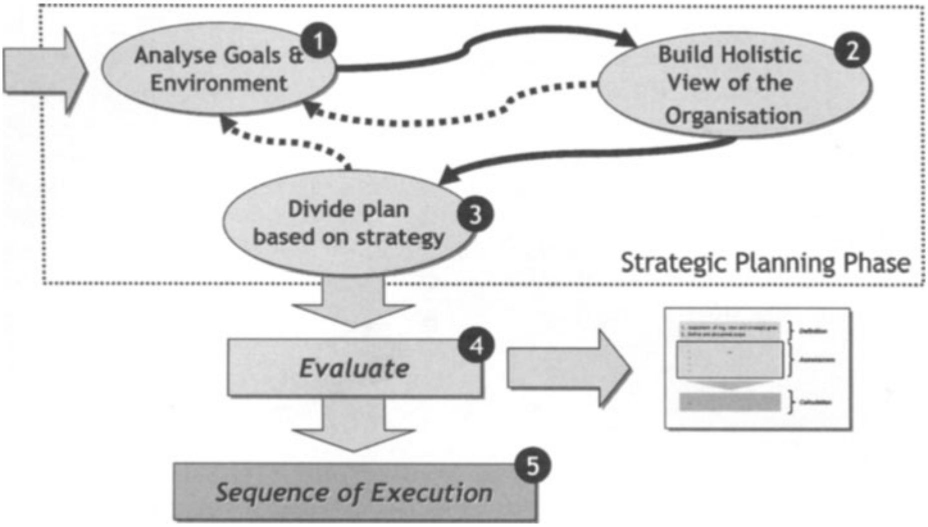

Analyse Goals & Environment
1
Build Holistic View of the Organisation
2
Divide plan based on strategy
3
Strategic Planning Phase
Evaluate
4
Sequence of Execution
5

Fig. 4. Proposed process for an initial operationalisation of the project's structure.

4.4 Structure of the proposed Evaluation Process

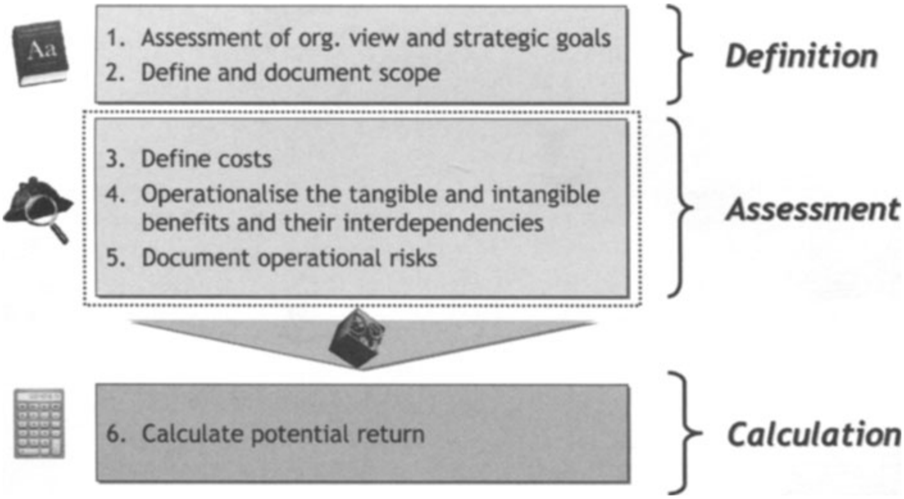
As a next step, the actual analysis for the sub-projects is prepared. The proposed process is built upon the prerequisites and the operationalisation presented earlier (literature review), dividing it into 6 steps (cp. Figure 5):

- ***Step 1:*** assessment of the organisational view on EIdM in order to derive strategic goals for its introduction. What should be achieved by introducing EIdM?
- ***Step 2:*** define and document the project's scope (what should be analysed) based on the strategic determinates set earlier. (In order to avoid important facets being missed, this step should be used in a cycle with Step 1).
- ***Step 3:*** define all project costs including all investments in hardware and software, license fees, and labour (e.g. consulting).
- ***Step 4:*** document and estimate potential *tangible and intangible benefits*. For the tangible benefits, this includes all direct (budgeted) and indirect (unbudgeted) savings and gains. Examples are potential saving in optimised processes that lead to less support requests. Furthermore negative productivity needs to be included, especially since security measures could come at the cost of convenience [25]. For the intangible benefits, the question "*What else does the project help to achieve*?" needs to be answered as well. Possible aspects include being compliant with laws, offering interoperability, and extensibility. In either case, it is important to analyse the interdependencies between the

tangible and intangible benefits. Here, standardised methods are needed to determine the costs accordingly [25].

- ***Step 5:*** document the possible operational risks such as resources, schedule, staffing, and legal and determine what *tangible and intangible impacts* they may have on the analysed case.
- ***Step 6:*** calculation of the potential return, based on the tangible benefits *and* the potential impacts of the risks (e.g. by using metrics and models such as ROI or ROSI).

The proposed evaluation process is visualised in Figure 5. Compared to other models such as Pisello [19], it strives to offer the following enhancements: First of all, the *potential operational risks* associated to EIdM are incorporated. This is necessary, as *IT security investments*, such as EIdM, help to reduce/mitigate potential risks. This result is a more accurate view of the benefits which can be derived from these kinds of technologies [21].



1. Assessment of org. view and strategic goals
2. Define and document scope
Definition
3. Define costs
4. Operationalise the tangible and intangible benefits and their interdependencies
5. Document operational risks
Assessment
6. Calculate potential return
Calculation

Fig. 5. Visualisation of the proposed evaluation process

Moreover, the presented process heavily relies on the documentation of the performed steps and the evaluation of the related operational risks, benefits, and the costs. Furthermore, this helps to identify the interdependencies between these aspects more easily and in a more consistent manner.

The documentation needs to be written in such a way that *all* involved parties can understand the used terminology and concepts. Common knowledge bases and glossaries are helpful to fulfil this requirement. In the opinion of the author, this helps 3rd parties not involved in the evaluation process (such as top level management) to comprehend and validate the results more easily.

4.5 Discussion

As part of the research approach outlined in section 2, the proposed evaluation process should help to assess the benefits and costs related to EIdM in a structured and standardised way (cp. [25]), 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 EIdM technologies in a more transparent manner.

As previously indicated, the decisions made by a cross-functional team need to be made on the basis of the organisational overview, in order to determine the actions to be taken on the strategic, the tactical, and the operational levels of the organisation. Therefore all relevant stakeholders need to be involved as all groups play a vital role for assessing the overall EIdM strategy. Here, the affected (business) processes that interfere with the EIdM in an organisation are the focal point for examination. They need to be acknowledged, analysed, formalised and documented in an appropriate way to get an overview on what is needed and where.

It seems clear that formalised process models are needed, in order to support the decision makers when planning the EIdM strategy for an organisation. Such process models need to address the special requirements for EIdM 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 EIdM.

Besides formalised process models, evaluation frameworks are needed that help to assess the overall value of investments into EIdM. Also it is important that such a framework is extending the limited view of financial metrics (e.g. NPV, ROI, or ROSI) [14, 18], taking tangible and intangible factors and associated operational risks into consideration. Here, an IT Security/EIdM Balance Scorecard (BSC), derived from the classical BSC by Kaplan and Norton [15] may be an appropriate approach to develop an integrated evaluation framework.

5 Summary and Outlook

When introducing EIMS, organisations incur a variety of costs for the implementation and the related organisational aspects. This paper presents initial ideas for a formalised process for assessing and considering the associated operational risks, costs, and benefits related to EIdM projects in an organisation.

Based on the presented research approach (section 2), the evaluation process at hand is a first step to achieve this. However, future research needs to extend the work presented here. This especially includes concepts, such as an IT Security/EIdM BSC, which integrate tangible and intangible factors into the decision making process. Furthermore, such an instrument could be used to execute an EIdM project on the tactical level, bringing together the strategic and the operational perspectives.

Acknowledgements

The research at hand was funded by the European (6th Framework Program) Network of Excellence (NoE) FIDIS (Future of Identity in the Information Society). The author wants to thank all people that helped to improve the contents of this paper with their comments, their contributions, and their reviews.

References

1. Bauer, M., Meints, M. and Hansen, M., Deliverable D3.1: Structured Overview on Prototypes and Concepts of Identity Management Systems (FIDIS, 2005).
2. Berghel, H., The Two Sides of ROI: Return on Investment vs. Risk of Incarceration, Communications of the ACM, 48(4), pp. 15-20 (2005).
3. Blohm, H. and Lüder, K., Investition, Schwachstellenanalyse des Investitionsbereichs und Investitionsrechnung (Vahlen, Munich, 1995).
4. Brynjolfsson, E., The Productivity Paradox of Information Technology, Communications of the ACM, 36(12), pp. 67-77 (1993).
5. Cavusoglu, H., Mishra, B. and Raghunathan, S., A Model for Evaluating IT Security Investments, Communications of the ACM 47(7), pp. 87-92 (2004).
6. Deron GmbH, Identity Management Studie 2006/2007 (Deron, Stuttgart, 2007).
7. Dewey, B. I. and DeBlois, P. B., Current Issues Survey Report 2007, EDUCAUSE Quarterly, 30(2), pp. 12-31 (2007).
8. Dos Santos, B. L. and Sussman, L., Improving the return on IT investment: the productivity paradox, International Journal of Information Management, 20(6), pp. 429-440 (2000).
9. Flynn, M. J. (2007); http://360tek.blogspot.com/2006/07/enterprise-identity-services.html, accessed 27th of September 2007.
10. Franklin, C. J., The ABCs of ROI, Network Computing, 27th of April, pp. 93-95 (2002).
11. Geschka, H. and Hammer, R., Die Szenario Technik in der strategischen Unternehmensplanung, in: Strategische Unternehmensplanung - strategische Unternehmensführung, edited by Hahn, D. and Taylor, B. (Physica, Heidelberg, 1997), pp. 464-489.
12. Hansen, M. and Meints, M., Digitale Identitäten – Überblick und aktuelle Trends, Datenschutz und Datensicherheit (DuD), 30(9), pp. 571-575 (2006).
13. Hevner, A. R., March, S. T. and Park, J., Design Science in Information Systems Research, MIS Quarterly, 28(1), pp. 75-105 (2004).
14. Jonen, A. et al., Balanced IT-Decision-Card, Ein Instrument für das Investitionscontrolling von IT-Projekten, Wirtschaftsinformatik, 46(3), pp. 196-203 (2004).
15. Kaplan, R. S. and Norton, D. P., The Balanced Scorecard. Translating Strategy into Action (Random House, Boston, 1996).
16. Lee, A. S., Integrating Positivist and Interpretive Approaches to Organizational Research, Organisational Science, 4(2), pp. 342-365 (1991).
17. Magnusson, C., Molvidsson, J. and Zetterqvist, S., Value Creation and Return On Security Investmensts (ROSI), in: IFIP SEC 2007: New Approaches for Security, Privacy and Trust in Complex Environments, edited by Venter, H. et al. (Springer, Boston, 2007), pp. 25-35.
18. May, T. A., The death of ROI: re-thinking IT value measurement, Information Management & Computer Security, 5(3), pp. 90-92 (1997).

19. Pisello, T., Return on Investment for Information Technology Providers (Information Economics Press, New Canaan, 2001).
20. Potthof, I., Kosten und Nutzen der Informationsverarbeitung: Analyse und Beurteilung von Investitionsentscheidungen (DUV/Gabler, Wiesbaden, 1998).
21. Purser, S. A., Improving the ROI of the security management process, 23(6), pp. 542-546 (2004).
22. Rossnagel, H. and 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 (2005).
23. Schmeh, K. and Uebelacker, H. (2006); http://www.heise.de/tp/r4/artikel/18/18954/ 1.html accessed 22.10.2007.
24. Solingen, R. v., Measuring the ROI of Software Process Improvement, IEEE Software, 21(3), pp. 32-38 (2004).
25. Sonnenreich, W., Albanese, J. and Stout, B., Return On Security Investment (ROSI) – A Practical Quantitative Model, Journal of Research and Practice in Information Technology, 38(1), pp. 45-56 (2006).
26. Wan, Z., Fang, Y. and Wade, M., A Ten-Year Odyssey of the “IS Productivity Paradox” - A Citation Analysis (1996-2006), Proceedings of the 13th Americas Conference on Information Systems (AMCIS), Keystone, Colorado (2007).
27. Windley, P. J., Digital Identity (O’Reilly, Sebastopol et al., 2005).