Enterprise Identity Management – Towards a Decision Support Framework Based on the Balanced Scorecard Approach

Enterprise Identity Management can be found in a variety of today's organizational processes. Being costly when introduced into an organization, adequate assessments of the costs, benefits, and the organizational settings are required. Today's methods for the evaluation and decision support of new IT (including EIdMS) are typically based on single dimensions (e. g. financial or technology aspects). This paper proposes a multidimensional decision support framework, based on the Balanced Scorecard concept.

DOI 10.1007/s12599-009-0052-5

The Authors

Dipl.-Wirt.-Inf. Denis Royer
Goethe University Frankfurt
Chair for M-Business and
Multilateral Security
Grüneburgplatz 1
60629 Frankfurt
Germany
denis.royer@m-chair.net

Dr. Martin Meints
Independent Centre for Privacy
Protection Schleswig-Holstein
PO Box 7116
24171 Kiel
Germany
ULD61@datenschutzzentrum.de

Received: 2008-08-07
Accepted: 2009-02-27
Accepted after one revision by
the editors of the special focus.

This article is also available in German in print and via http://www.wirtschaftsinformatik.de: Royer D, Meints M (2009) Betriebliches Identitätsmanagement – Ein Rahmenwerk zur Entscheidungsunterstützung auf Basis des Balanced-Scorecard-Konzepts. doi: 10.1007s11576-009-0174-x.

1 Introduction

1.1 Description of the problem domain

In today's organizations, business processes are increasingly facilitated by a variety of information systems (IS). In order to accelerate the handling of user accounts and to protect such systems and other organizational assets (e. g. customer data) from unauthorized access, enterprises have the need to invest in technologies that can be integrated into their processes, allowing for automated and accelerated handling of access control related identity data. Without the introduction of appropriate technologies, organizations may face issues such as productivity losses, various risks, and lack of compliance (Royer 2008a, p. 780). *Enterprise Identity Management Systems* (EIdMS) can offer such supportive and protective measures. This class of identity management systems helps to facilitate the handling of identity data and access permissions in organizations (Mezler-Andelberg 2008, pp. 7 ff; Windley 2005, pp. 3 ff).

Questions regarding the value of Information Technology (IT) and the investment in related technologies are becoming increasingly important for organizational decision making (Hitt and Brynjolfsson 1996, pp. 121 ff; Martinsons et al. 1999, pp. 71 ff). Accordingly, the evaluation of IT security investments (and IT investments in general) is a subject which has been widely and controversially discussed in the domains of scientific and practitioners' literature for the past two decades (Cavusoglu et al. 2004, pp. 87 ff; Magnusson et al. 2007, p. 25; Sonnenreich et al. 2006, p. 45; Walter and Spitta 2004, pp. 171 ff). A large number of contributions in this field focus on the establishment of approaches helping to facilitate the decision making process for investments in IT security technologies. Even though decision making is a core management activity, the challenge lies within the collection and analysis of the data and decision parameters. This becomes even more problematic when we consider the vast amount of data available and the general impact of new infrastructural IT systems on an organization, resulting in an even more complex decision situation (Jonen et al. 2004, p. 196; Benamati and Lederer 2001, pp. 95 ff).

Despite investing a significant amount of their budgets in various information systems, studies indicate that organizations seem to fail to achieve their objectives within a set timeframe (Brynjolfsson 1993, pp. 67 ff; Dos Santos and Sussman 2000, p. 430; Wan et al. 2007). One of the stated reasons is the fact that current accounting models can only capture the increase of efficiency ("doing things right"), but fail to recognize the benefits from increasing effectiveness ("doing the right things") enabled through IS (Martinsons and Martinsons 2002, p. 72). In this context the *IT productivity paradox* is a widely and controversially discussed theory towards IS (Wan et al. 2007). Apart from the inherited problems of general IT investments, IT security investments suffer from additional problems (Magnusson et al. 2007, pp. 26 ff). These include the identification of (possible) revenues generated by an IT security investment and of the optimal level of security investments that depend on the results of a risk assessment, a process that is highly context-sensitive. Furthermore, IT security investments are carried out to mitigate risks and to prevent possible losses (Sonnenreich et al. 2006, p. 45). As risks

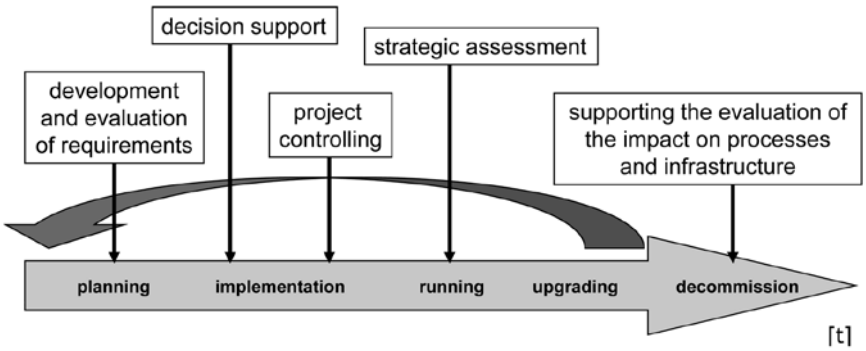

Fig. 1 Potential application area and purpose of the researched artifact

depend on the likeliness that an incident may occur and incidents may be of a non-monetary nature (e. g. negative impact on reputation), it is difficult to quantify them in monetary terms, due to the preventive nature of IT security investments.

1.2 Goal of this paper

The issue to be dealt with in this paper is the design of an artifact that serves as a starting point for developing a decision support instrument for the introduction of EIdMS into an organization (March and Smith 1995; Hevner et al. 2004, pp. 75 ff; Royer 2008a, pp. 780 ff). The artifact itself uses the Balanced Scorecard (BSC) concept as a foundation for the derivation of a decision support approach. The resulting *Enterprise Identity Management (EIdM) Decision Matrix* is intended for the planning phase of EIdMS, having a more tactical scope. However, a derived BSC well may serve different purposes and have a different, e. g. strategic, scope (**Fig. 1**).

By introducing relevant decision parameters and indicators from different perspectives, a more transparent decision making process concerning the benefits of investments in EIdMS can be achieved. Furthermore, the resulting approach needs to address the initially stated challenges. This paper will derive requirements on how such a decision support approach needs to be constructed, based on relevant literature and the results of a qualitative expert interview study[1]. Finally, while a significant amount of IT security related literature focuses primarily on technical issues (Gordon and Loeb 2002, pp. 439 ff; Siponen and Oinas-Kukkonen 2007, pp. 71 ff), this paper follows an interdisciplinary approach to analyze the organizational implications and impacts resulting from the introduction of EIdMS, whilst integrating the business and IS research perspective.

1.3 Structure of this paper

The remainder of this paper is structured as follows: The basic concepts and organizational challenges of EIdM are summarized in the second section, providing insights into the diverse and complex nature of the introduction of such technologies into organizations. In the following, theoretical foundations for this research and literature that deals with the evaluation of EIdM and IT security investments in general are presented (Section 3). Based on the previous sections, the fourth section presents the derived approach, showing its application in three scenarios. The last section (5) summarizes the findings and gives an outlook on further research.

2 Organizational challenges of EIdM

2.1 What is enterprise identity management?

EIdM is one of the major challenges for organizations in the coming years. This is due to the fact that more and more access control related identity data is processed and needs to be handled adequately. At the technological level, a variety of technologies which belong to the cluster of EIdM technologies can be identified. Among others, these include single-sign-on solutions, directory services, public-key infrastructures, and identity and access management systems (Mezler-Andelberg 2008; Windley 2005). Contrary to the information given by the majority of vendors, EIdM can be considered a framework of different technologies and functions, rather than a simple out-of-the-box solution. Moreover, EIdM is a potential core element in the IS infrastructure of an organization, integrating the assets, users, and systems in an organization (**Fig. 2**). Lastly, EIdMS are used to manage identity data and the identity lifecycle within an organization. In this regard, EIdM can be considered the *missing link*, enabling a variety of services (e. g. for eCommerce, eGovernment, eServices).

The need for EIdM is owed to the fact that entitlements of users (e. g. their roles and access permissions) change due to organizational changes. These changes in users' (partial-) identities[2] need to be handled in a centralized way (Windley 2005, pp. 29 ff), taking into consideration the changes over time, being referred to as the identity lifecycle (e. g. Meints and Royer 2008, p. 201). Supporting the lifecycle of identities on the organizational level, EIdM fulfills the functions of authentication, authorization, administration, and audit of the user accounts that need to be managed in an organization (Bauer et al. 2005, pp. 19 ff).

2.2 Aspects of EIdM introductions

The topic of EIdM gains increased importance when organizations have to face legal obligations, such as laws and regulatory frameworks (e. g. Sarbanes-Oxley Act (SOX), Basel II). Besides these compliance goals, other aspects, such as risk/security goals and value creation goals, play important roles (KPMG 2008; Royer 2008a, p. 780). Nevertheless, these goals are not mutually exclusive.

Recent studies also show that the introduction of EIdMS is coupled with significant costs (Deron GmbH 2007; KPMG 2008) and therefore requires thorough

[1] This study was conducted among 11 experts (users, vendors, and integrators) in the domain of EIdM, especially focusing on the decision parameters and their linkages. The interviews used semi-structured interview guidelines. The results were aggregated, using the qualitative content analysis as described by Miles and Huberman (1994). The complete results of the expert study have been finalized and are currently in the publication/review process.

[2] Partial identities are subsets of attributes of a complete identity. Each identity of a person comprises many partial identities of which each represents the person in a specific context or role (cf. Nabeth and Hildebrandt 2005, pp. 27 ff; Hansen and Meints 2006, pp. 544 ff).

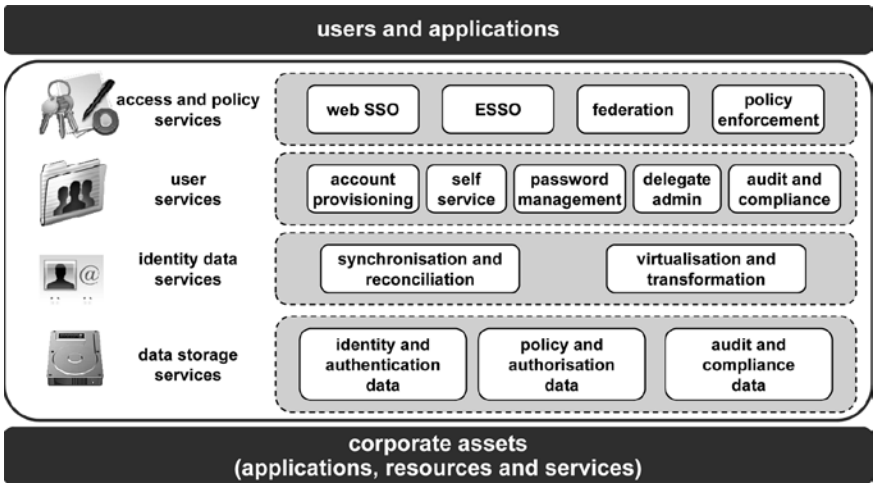

Fig. 2 EIdM technology framework based on Flynn (2007)

planning. Considering this, decision makers should debate whether investments into EIdM make sense for every type of organization. This is due to the fact that specific organizational aspects, such as the size and the importance of the IT used in an organization as well as the number of users, also need to be taken into consideration.

In the planning phase it is important that organizational aspects are incorporated into the development of an enterprise identity management (EIdM) solution, instead of purely focusing on the *technological* or *financial* aspects. Indeed, without a proper assessment of the *costs*, *benefits*, and the *organizational settings* (such as stakeholders or processes), companies will not be able to see the full potential of introducing EIdM as an additional layer into their IT infrastructure (e. g. faster process cycles, ID data quality, etc.) and their business processes, besides fulfilling constraints, such as compliance. Moreover, while IT changes (or can be changed) rapidly, the stakeholders, such as the IT department, management, and the users (operating departments and application administrators), need to be taken into consideration as well (Royer 2008a, p. 782). Without proper change management and the involvement of these stakeholders, it is unlikely that the strategic goals and potentials of expenditures for introducing IS (and EIdMS) can be achieved within a set timeframe (Dos Santos and Sussman 2000, p. 430; Magnusson et al. 2007, p.27).

Considering the aforementioned aspects, organizations tend to have difficulties in demonstrating tangible returns of EIdM investments, as they are not yet capable of capturing their enhanced value and returns. One of the reasons can be found in the complex and diverse nature of IT security investments and IT investments in general. Moreover, EIdM and its introduction touch on many different aspects within an organization (operational and organizational structure, such as processes, structure, and task), which are discussed in the following sections.

Additionally, EIdM is not a purely technology driven topic. As shown before, this type of technology creates an interface between the users and assets. Consequently, interference with the processes of an organization exists. Accordingly, the resulting process changes, which result from the introduction of EIdM, add to the complexity for the organization (Benamati and Lederer 2001, pp. 96 ff; Schumann 1993, pp. 168 ff).

3 How to support decision making for EIdM – foundations and concepts

3.1 Evaluation methods for EIdM and IT security investments and IT security risks

The origin of the discussion concerning the evaluation of IT investments goes back to the late 1980s, and it has been addressed consequently ever since. Several methods and frameworks have been presented for assessing the economic impacts and the value of IT (security) investments. Prominent examples are the commonly used *return on investment* (ROI) or the *return on security investments* (ROSI). A selected literature sample and a summary of its findings and results are listed in **Tab. 1**.

Whereas several different approaches have been proposed to evaluate IT and IT security investments, further difficulties can be observed with regard to evaluation methods, metrics, and data collection.

The evaluation methods based on financial measures are not well-suited for IT security investments as they do not reflect the wide range of potential benefits, such as intangible aspects (Magnusson et al. 2007, pp. 26 ff; Martinsons et al. 1999, pp. 72 ff) and the interconnectedness of the different aspects. An example is the achievement of compliance to relevant laws and regulations by executing an EIdM project.

The metrics used are often single-dimensional, only taking a specific point of view, such as that of financial aspects. One example for this is ROSI, which is limited to the monetarization of IT security investments (e. g. by analyzing productivity losses associated with security breaches). As a result, decisions are made on a limited amount of information which could lead to suboptimal results, as only a narrow and incomplete picture of the impact of IT security investments is considered.

Finally, the majority of the methods presented in the related literature do not tackle the problem of *data collection* and the identification of the relevant data for analysis. Also, a lack of empirical data as a basis for analyses limits the significance (Purser 2004, p. 543).

Therefore, while currently accepted methods try to tackle the stated additional problems of IT (security) investments, (so far) no approach is capable of integrating all the aspects into one approach. Thus, extended metrics and adequate methods seem necessary in order to evaluate the potential return on EIdM and ultimately to support the decision making process.

3.2 The Balanced Scorecard concept (BSC)

During the early 1990s, Kaplan and Norton introduced the BSC concept as a performance measurement system for organizations, addressing shortcomings of traditional performance measurement systems (Kaplan and Norton 1996). Arguing that financial accounting measures are too narrow in scope, the BSC does not rely *only* on financial outcomes (Martinsons et al. 1999, p. 72), but is supplemented with additional organizational measures that

complement past and future performance indicators in a holistic way (Martinsons et al. 1999, p. 73).

The resulting scorecard translates additional measures into four perspectives: financial, customer, internal business processes, and learning & growth (Kaplan and Norton 1996). The perspectives are derived from the *visions & strategies* of an organization. Also, they represent the three major stakeholder groups of an organization: shareholders, customers, and employees (Mooraj and Oyon 1999, p. 482). The term "balanced" reflects the intent to maintain a balance between the perspectives and their contained performance indicators, i.e., the balance is kept between short- and long-term objectives, lagging and leading indicators, and financial and non-financial measures. Further research extended the BSC concept by forming causal chains and causal networks among the perspectives' indicators, also referred to as *strategic maps* (Kaplan and Norton 2004, pp. 55 ff).

In summary, the integration of the BSC's perspectives allows for a more comprehensive view on the organization itself (e. g. history and trends). Also, the BSC enables an active management of an organization down to the project level, helping to act in the best long-term interests (Martinsons et al. 1999, p. 73; Jonen et al. 2004, pp. 196 ff).

3.3 Preliminary assessment

Based on the previously analyzed literature, we argue that there is no decision support approach yet which is capable of supporting decision makers when investing in EIdM projects. As shown, this is due to the facts that:

- EIdM projects have a high level of complexity with regard to the operational and organizational structure. In order to obtain *the big picture*, further aspects of the EIdM introduction need to be observed.
- The presented approaches are too narrow in scope and focus on single dimensions (e. g. financial measures or technical issues).
- Moreover, no approach has so far been capable of capturing the potential benefits resulting from increased effectiveness through the introduction of EIdMS, which may occur in different aspects.

Tab. 1 Selected literature on the evaluation of IT security investments and IT security risks

Author	Evaluation approach / Results
Cavusoglu et al. 2004	The model described employs a *game theory* based approach, supporting the choice for a security technology. The estimated parameters are used to determine potential cost savings implied by a security technology. The technology yielding the maximum savings is chosen.
Farahmand et al. 2005	In their approach, Farahmand et al. assess IT security risks, based on the analysis and evaluation of qualitative risks. The risks are translated into monetary values, representing the expected losses of a security incident.
Magnusson et al. 2007	Analysis of different ROSI approaches with regard to their theoretical foundation and their value for the measurement of value creation. The authors conclude that ROSI is not sufficiently utilizable in value creation (Net Present Value, ROI) calculations.
Gordon and Loeb 2002	This paper presents a conceptual economic model to derive the optimal level of information security investment decisions. The presented approach is based on a mathematical risk-model, which is described in theory.
Purser 2004	Purser proposes a ROI measure for security managing, incorporating the value of changed risks. The author argues that by incorporating such measure into the control framework cost savings can be achieved.
Riepl 1998	The author gives a critical assessment of the Total Cost of Ownership (TCO) and the ROI approach for the evaluation of general IT investments. As a result the author advises decision makers to challenge such methods and to thoroughly assess IT infrastructures based on extended methods.
Sonnenreich et al. 2006	Sonnenreich et al. analyze the ROSI and the problems related to acquiring the necessary data (e. g. risk exposure, risk mitigation, solution costs) to actually calculate a "meaningful" ROSI. Furthermore, they suggest the usage of the NPV to factor in the time-value of money. Their result is a ROSI calculation scheme, focusing on lost productivity, risk exposure and risk mitigation.
vom Brocke et al. 2007	A framework based on a capital budgeting (VOFI – Visualization of Financial Implications) approach to calculate the ROSI is proposed. Potential cash inflows are simulated on the basis of capital risk investments.

However, an approach based on the BSC concept, combined with the aspects described by other evaluation methods seems appropriate in order to embrace the presented challenges of EIdM introductions in general. Such an approach would allow executives to overcome complex decision-making situations by bridging the gap between the different impacting fields and decision parameters.

4 Proposal of an EIdM Decision Matrix

In order to build a decision support framework for the introduction of EIdMS, substantial modifications to the original perspectives of the BSC concept are necessary. This is due to the fact that we intend to use the derived framework for *decision making*. Therefore, several prerequisites need to be taken into consideration when building an *EIdM Decision Matrix (EDM)*.

The presented EDM focuses on the tactical level of decision making (0.5–3 years), while the underlying BSC concept is aimed towards the strategic area. The reason is that the resulting effects of EIdM projects tend to emerge short to mid-term after such systems have been introduced (e. g. process or quality improvements). However, for IT projects it is also important to include strategic implications linked to the overall IT strategy. Based on the scope of an EIdM project, strategic implications can be translated into target settings for the EDM, such as long-term process improvements, improvement of data quality, or user satisfaction.

When building an EDM, it is essential to focus on specific decision variables and the most commonly used key performance indicators as subsets. Although the original BSC requires a periodical review of the perspectives, we argue that a limited subset of decision variables suitable for generalization are sufficient for the majority of decision making processes. The resulting framework should, however, allow for the possibility of extending the used metrics and decision parameters according to specific cases and application areas.

For decision support it is not always possible to determine all data with 100% accuracy within an acceptable timeframe (Purser 2004, pp. 543–544) and some data may even be probabilistic. Therefore some degree of compromise is necessary. When preparing the data, one has to keep in mind that (most of the time) the results

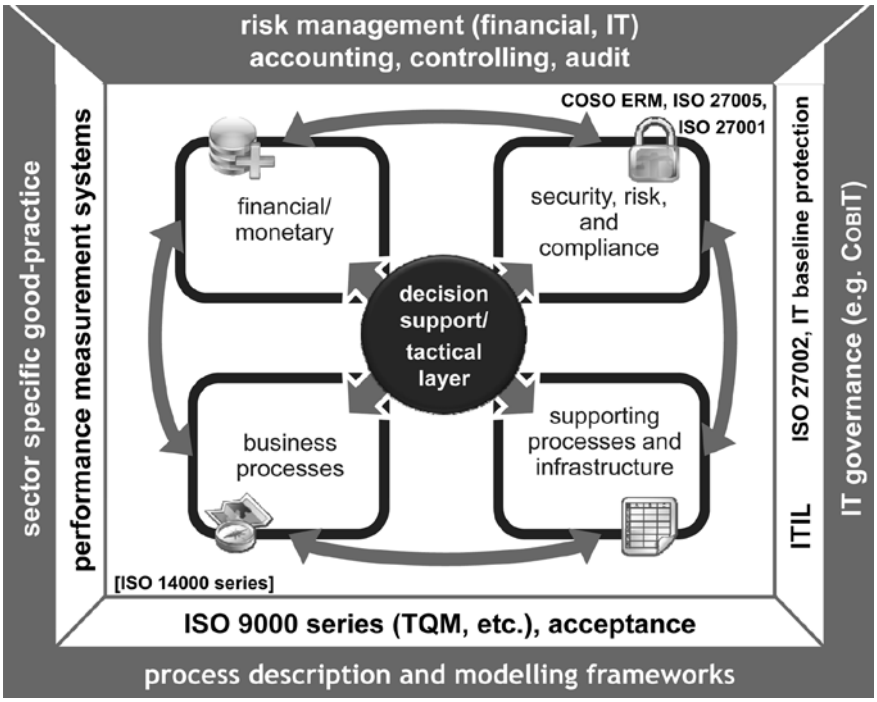

Fig. 3 Initial design of the derived EIdM Decision Matrix (EDM), incorporating the relevant standards and best-practice frameworks (based on Royer and Meints 2008, p. 191)

need to be only sufficiently accurate for decision making processes.

4.1 The perspectives of the EIdM Decision Matrix

Based on an initial literature review (Royer 2008a), adapted on the basis of an expert interview study, four perspectives and corresponding indicators for an EDM were derived: financial/monetary, security/risk/compliance, business process, and supporting processes/infrastructure. Moreover, these can be further classified into two superordinate objectives: the business objectives (financial/budget and business processes), and the objectives driven by compliance – compliance objectives (security/risk-management and supporting processes). By using the BSC approach, these two objectives can be brought together in a coherent and comprehensive way to facilitate the decision making process (Royer 2008b). The resulting EDM based on the four perspectives is presented in **Fig. 3**.

Each of the perspective should be translated into corresponding metrics and decision parameters that reflect the goals of the introduction of EIdMS into organizations. In this context, an overview of the organization and solution specific requirements is necessary as a source for the development of performance indicators since (at least in the perspectives of business processes) supporting processes and security requirements of organizations and solutions may show a wide range.

The following sections will further describe the four perspectives of the EDM and potential measures that can serve as an initial set of decision parameters for an average organization whose security requirements can be satisfied by the described standard and best-practice. The mapping towards the objectives of each perspective is also further elaborated. As there are no specific guidelines for the derivation of measures, the authors extracted the proposed metrics from the mainstream IS management literature as well as from best practice and standards in the field of information security techniques and management, such as the ISO/IEC 9000, ISO/IEC 27000 series or ISO/IEC 15408 (Common Criteria). Linking these approaches allows a multidimensional analysis within the perspectives already presented.

It is definitely important to note again that due to the differences with respect to the requirements of each individual EIdM solution, careful checking and adjustment of the decision parameters proposed in this paper is necessary.

4.1.1 Financial/monetary perspective

This perspective focuses on the monetary aspects of EIdMS projects. Accordingly, it includes factors such as financial information, budgets, and the costs associated with an EIdM project. This helps to give an overview of the (prospective) savings/cash in- (e. g. process induced savings) and out-flows (e. g. costs of security incidents) of an EIdM project by mapping them to the other perspectives and their key performance indicators, allowing for an analysis of the impacts induced by the other three perspectives. Examples are cost savings induced by using EIdM for role-specific or function based software delivery in an organization. Based on the number of existing software packages, the estimated number of packages after the EIdM introduction and EIdM process reengineering, and the costs per software package, the resulting cost reduction for software licenses can be calculated.

Another important aspect is the monitoring of IT budgets, in order to not limit possible growth potentials (Baschin and Steffen 2001, p. 368), which is considered to be one of the main obstacles to achieving a sufficient security level (Yue et al. 2007, p. 3). Consequently, by monitoring the budgets related to an EIdM project, this effect can be avoided. **Tab. 2** lists examples for measures employed in this context.

4.1.2 Business process perspective

The argument of Martinsson et al. can be followed, as IS and therefore also EIdMS are more organization-based than customer-focused (Martinsons et al. 1999, pp. 79-80). However, when integrating stakeholders, such as users and customers, EIdM does also have an impact on the current business process of an organization (**Tab. 3**).

Analyzing the business processes, this perspective looks into the core processes of an organization. By evaluating the integration of the EIdM and the IS in an organization, the prospects of higher efficiency and productivity can be made measurable (Jonen et al. 2004, p. 199).

4.1.3 Supporting process and infrastructure perspective

This perspective involves evaluating the supporting processes in an organization

(e. g. HR, organizational management) and the IT infrastructure. For the impact of EIdM, this perspective offers the possibility to assess the alignment of supporting and business processes with regard to their targets and the structure and inventory of the existing IS and its users (**Tab. 4**).

Potential decision parameters are heavily dependent on the supporting processes applied. In some cases good practice processes as described in the IT Infrastructure Library (ITIL) may be referenced or used.

However, important aspects in this perspective are the integration of relevant supporting processes into the EIdM, and coverage of the phases of the life cycle of identities managed in the EIdM (complete coverage almost automatically requires integration with HR).

4.1.4 Security, risk and compliance perspective

This perspective of the BSC deals with the associated risks and the security management of EIdM projects. Here, factors resulting from compliance mandates (e. g. SOX), data security (e. g. roles, access permissions), and security standards (if required) play a major role in the evaluation.

A set of requirements for the solution can be developed based on a risk assessment and standard security functions and measures described in ISO/IEC 15408 (Common Criteria, especially class "Authentication and Authorization (FIA)") or ISO/IEC 27002 (Code of practice for information security management, various chapters). An overview of potentially relevant requirements for EIdM solutions and resulting performance indicators, from a security point of view, was already developed in Royer and Meints 2008. The decision parameters which the authors believe most relevant for an organization are described in **Tab. 5**.

4.1.5 Mapping / linkage of the four perspectives

The decision parameters proposed clearly show overlap. One example is *coverage/integration* in the perspective supporting processes, *coverage* in the security perspective and *savings/cash flow generated* in the financial perspective. While *coverage/integration* in the perspective supporting processes show overlap with *coverage* in the security perspective due to the fact that supporting processes also may deal with protecting worthy information, both may cause a change in the *savings/cash flow generated*.

Tab. 2 Exemplary measurements and decision parameters for the financial/budget perspective

Cash Outflows / Budget Overall EIdM project budget and degree of target achievement with regard to budget Aggregated costs of the project Process incidents costs (help desk activity, issued software licenses, etc.)
Negative effects/ Risks Estimated costs for security incidents (e. g. based on historic or benchmark data) Potential costs caused by operational risks (e. g. resulting from the unwillingness to use a system) based on incident metrics (e. g. derived from ITIL or audit logs), operational pilots, or by using benchmark data.
Savings/Cash Inflows generated Classical financial measures, based on traditional measures such as static measures (e. g. ROI, payback period) or dynamic measures (e. g. NPV, DCF) Business evaluations, identifying cash inflows resulting from causal effects related to other perspectives, such as improved service quality (indirectly quantifiable), reduced risk (qualitative/intangible), or process cost savings (quantitative/tangible).

Tab. 3 Exemplary measurements and decision parameters for the business process perspective

Coverage / Integration Alignment of EIdM processes and business processes
Process quality related measures Overall process maturity (documentation of the operational and organizational structure of an organization), limiting the maximum maturity of the EIdM processes (e. g. by employing the capability maturity model) Overall adaptability of processes (qualitative measurement)
Operations Number and average time needed to handle EIdM influenced business cases Changes in process cycle time as target-performance comparison in [%] Number of IT systems requiring authentication, involved in a business

4.2 Outputs and implications of the EIdM Decision Matrix – possible application scenarios

The presented EDM can serve a variety of application scenarios, which are discussed in the following subchapters.

4.2.1 Determination of organizational state-of-the-art

First of all, the framework can be used to determine the state-of-the-art of an organization, focusing on the decision for or against an introduction of EIdM. The actual implementation could be in the form of a *decision support system* (DSS), allowing decision makers to aggregate and analyze the relevant data, in order to structure the complex decision problem (Power 2004; Sprague 1980). Furthermore, possible returns from the introduction of EIdM could be calculated on the basis of the acquired data. These include aspects such as cost-savings from EIdM supported software license management, reduced help-desk incidents, or enhanced productivity by reducing media break in provisioning processes.

4.2.2 Comparison of solutions

Moreover and combined with supplementing methods (e. g. portfolio analysis, simulation techniques, scenario technique), the framework can be used to compare different EIdM solutions. By visualizing the resulting data for each of the potential EIdM, decision makers obtain a better assessment of the future development of the decision parameters.

In this connection, the presented approach can be used in early project stages (**Fig. 1**), such as the requirements specification or the support of procurement processes. Here, the relevant requirements of the four perspectives can be taken into consideration. This may, in addition to technical requirements and costs, lead to an integration of the EIdM with a list of enterprise applications and the fulfillment of specific security requirements, such as enforcement of password policies, the support for different levels of (user) authentication, etc.

In a later step, the technical specifications of potential solutions offered by the

Tab. 4 Exemplary measurements and decision parameters for the supporting process perspective

Coverage / integration
Supporting processes (and related applications) integrated into the EIdM vs. total supporting processes with authentication/authorization requirements
Overall (EIdM) integration level, (EIdM) process automation level, media breaks, or integration level
Process alignment or integration maturity between the supporting and the business processes (qualitative measurement)
Time, priority, and resources needed to integrate an EIdM solution into an organization
Infrastructure
Number and type of existing IT systems (e. g. platforms, applications, number of identified interfaces between systems/applications)
User management: amount of users, issued credentials
Operations and workflow related measurements
EIdM process cycle time as target-performance for (de-) provisioning or changes in ID attributes
Phases of the life cycle of identities supported by the EIdM solution vs. total phases
Expertise and training needed to operate the EIdMS by IT specialists (qualitative measure)

Tab. 5 Exemplary measurements and decision parameters for the security / risk-management perspective

Environmental and information access control
Physical access areas integrated into the EIdM vs. physical access areas existent in the organization
Accounts managed by an EIdMS vs. total accounts
Mapping of users and accounts in the different systems to indicate "account density"
Privileged accounts managed with the EIdM solution vs. total privileged accounts
Accounts with specific authentication requirements (such as a password of a certain quality, a token, quality of the encryption of authentication data transferred via networks etc.) managed with the EIdM vs. total number of accounts with specific authentication requirements
Accounts with specific authorization requirements (such as session time outs, login time frames etc.) managed with the EIdM vs. total number of accounts with specific authorization requirements
Audit logging
Achievable quality of audit logs (content, time frame covered, revision process, evaluation support) vs. required quality of audit logs
Coverage
Information and communication sources used by the EIdM vs. total available information and communication sources

solution providers are documented, leading to at least one possible scenario per solution provider for the future EIdM solution. Each of the requirements fulfilled by the solution analyzed in the next step can then be evaluated using the selected decision parameter and performance indicators. The analysis of the relevancy and interconnection of the performance indicators allows a more in-depth analysis and comparison of the scenarios.

4.2.3 Project controlling

Finally, IS need adequate mechanisms and processes for their control as they represent an interface in an organization. In this regard our framework can be extended to serve as an integrated IT (project) controlling tool (**Fig. 1**) – e. g. as discussed by Krcmar or Schumann (Krcmar 1990; Schumann 1993). However, being out of scope of the ex-ante nature of the presented approach, this topic is beyond decision support and will be subject of further work in this field.

4.3 Limitations of the framework

Although the EDM offers a vehicle to analyze EIdM projects beyond single dimensional metrics, it has high demands with regard to complexity and aggregation of data. However, EIdM is complex, as its introduction has numerous impacts on the operational and organizational structure of an organization. Therefore, a thorough analysis of the effects in the presented four perspectives seems feasible. Moreover, even though data might not be available at the initial setup of the EDM, they can still be fed into later stages to improve calculations. With regard to the data, the setup and customization of the presented approach is a necessary step, which depends on the EIdM project's scope. Accordingly, the aggregation of analysis data is a task that needs to be tightly integrated into the project planning phase and the analysis of the requirements (e. g. based on Royer 2008a, pp. 783 ff).

Furthermore, at this early stage of our work, the perspectives and their contained decision parameters represent a first framework rather than a complete DSS. Nevertheless, the presented framework can serve as an initial starting point to develop a complete, software-based decision support tool. A more in-depth analysis and modeling of the relationships between the derived *decision parameters* will be subject of future research endeavors. Based on case study research, instantiations of the EDM will be used to further validate the presented linkages and to improve the framework itself.

5 Conclusions

In this paper a systematic decision support framework for the introduction of EIdMS into organizations was proposed. Starting with a comprehensive analysis of EIdM technology, its application fields, and problems, a framework considering the BSC concept for the measurement and the incorporation of relevant decision parameters in the decision making process was presented. By integrating additional perspectives besides the technological or financial point of view, the resulting EIdM Decision Matrix allows support of decision making in a holistic way. The considered four perspectives and the contained decision parameters were extracted from the relevant literature and expert interviews. Furthermore, existing best-practice and standardized approaches were incorporated as well. Finally, when implemented into a software-based DSS, the presented framework will allow decision makers to better observe and understand positive and negative impacts when introducing EIdM technologies into an organization. However, this will be the subject of our upcoming research.

References

Baschin A, Steffen A (2001) IT-Controlling mit der Balanced Scorecard. ZfCM 45(6):367–371

Bauer M, Meints M, Hansen M (2005) Deliverable D3.1: Structured overview on prototypes and concepts of identity management systems. http://www.fidis.net/fileadmin/fidis/deliverables/fidis-wp3-del3.1.overview_on_IMS.final.pdf. Accessed 2009-02-27

Benamati J, Lederer AL (2001) How IT organizations handle rapid IT change: five coping mechanisms. Inf Technol Manag 2(1):95–112

Brynjolfsson E (1993) The productivity paradox of information technology. Communications of the ACM 36(12):67–77

Cavusoglu H, Mishra B, Raghunathan S (2004) A model for evaluating it security investments.

Communications of the ACM 47(7):87–92
Deron GmbH (2007) Identity Management Studie 2006/2007. Deron, Stuttgart
Dos Santos BL, Sussman L (2000) Improving the return on IT investment: the productivity paradox. IJIM 20(6):429–440
Farahmand F, Navathe SB, Sharp GP, Enslow PH (2005) A management perspective on risk of security threats to information systems. Inf Technol Manag 6(2–3):203–225
Flynn MJ (2007) Enterprise identity services. http://360tek.blogspot.com/2006/07/enterprise-identity-services.html. Accessed 2009-02-27
Gordon LA, Loeb MP (2002) The economics of information security investment. ACM TISSEC 5(4):438–457
Hansen M, Meints M (2006) Digitale Identitäten – Überblick und aktuelle Trends. Datenschutz und Datensicherheit 30(9):571–575
Hevner AR, March ST, Park J (2004) Design science in information systems research. MIS Quarterly 28(1):75–105
Hitt LM, Brynjolfsson E (1996) Productivity, business profitability, and customer surplus: three different measures of technology value. MIS Quarterly 20(2):121–142
Jonen A, Lingnau V, Müller J, Müller P (2004) Balanced IT-Decision-Card, Ein Instrument für das Investitionscontrolling von IT-Projekten. WIRTSCHAFTSINFORMATIK 46(3):196–203
Kaplan RS, Norton DP (1996) The balanced scorecard. Translating strategy into action. Random House, Boston
Kaplan RS, Norton DP (2004) Strategy maps. Harvard Business School Press, Boston
KPMG (2008) KPMG's 2008 European identity & access management survey
Krcmar H (1990) Informationsverarbeitungs-Controlling – Zielsetzung und Erfolgsfaktoren. Information Management 5(3):6–15
Magnusson C, Molvidsson J, Zetterqvist S (2007) Value creation and return on security investments (ROSI). In: Venter H, Labuschagne L, Eloff J, von Solms R (eds) IFIP SEC 2007: New approaches for security, privacy and trust in complex environments. Springer, Boston
March ST, Smith GF (1995) Design and natural science research on information technology. Decision Support Systems 15(4):251–266
Martinsons M, Davidson R, Tse D (1999) The balanced scorecard: a foundation for the strategic management of information systems. Decision Support Systems 25(1):71–88
Martinsons MG, Martinsons V (2002) Rethinking the value of IT, again. Communications of the ACM 45(7):25–26
Meints M, Royer D (2008) Der Lebenszyklus von Identitäten. Datenschutz und Datensicherheit 32(3):201
Mezler-Andelberg C (2008) Identity Management – eine Einführung. dpunkt, Heidelberg
Miles MB, Huberman AM (1994) Qualitative data analysis. Sage, Thousand Oaks
Mooraj S, Oyon DHD (1999) The balanced scorecard: a necessary good or an unnecessary evil? EMJ 17(5):481–491
Nabeth T, Hildebrandt M (2005) D2.1: Inventory of topics and clusters. http://www.fidis.net/fileadmin/fidis/deliverables/fidis-wp2-del2.1_Inventory_of_topics_and_clusters.pdf. Accessed 2009-02-27
Power DJ (2004) Specifying an expanded framework for classifying and describing decision support systems. CAIS 13(13):158–166
Purser SA (2004) Improving the ROI of the security management process. Computers & Security 23(7):542–546
Riepl L (1998) TCO versus ROI. Information Management 13(2):7–12
Royer D (2008a) Assessing the value of enterprise identity management (EIdM) – towards a generic evaluation approach. In: Weippl ER, Quirchmyr G, Slya J (eds) Proceedings of the 3rd international conference on availability, reliability and security (ARES 2008). IEEE Press, Barcelona
Royer D (2008b) Ganzheitliche Bewertung von Enterprise Identity Management Systemen – Der Ansatz der Balanced Scorecard als taktisches Entscheidungsunterstützungsinstrument. In: Alkassar A, Siekmann J (eds) Sicherheit 2008 – 4. Jahrestagung Fachbereich Sicherheit der Gesellschaft für Informatik. LNI, Saarbrücken
Royer D, Meints M (2008) Planung und Bewertung von Enterprise Identity Managementsystemen. Datenschutz und Datensicherheit 32(3):189–193
Schumann M (1993) Wirtschaftlichkeitsbeurteilung für IV-Systeme. WIRTSCHAFTSINFORMATIK 35(2):167–178
Siponen MT, Oinas-Kukkonen H (2007) A review of information security issues and respective research contributions. The DATA BASE for Advances in Information Systems 38(1):60–80
Sonnenreich W, Albanese J, Stout B (2006) Return on security investment (ROSI) – A practical quantitative model. Journal of Research and Practice in Information Technology 38(1):45–56
Sprague RHJ (1980) A framework for the development of decision support systems. MIS Quarterly 4(4):1–26
vom Brocke J, Strauch G, Buddendick C (2007) Return on security investments – towards a methodological foundation of measurement systems. In: Proceedings of the 13th AMCIS. AIS, Keystone
Walter SG, Spitta T (2004) Approaches to the exante evaluation of investments into information systems. WIRTSCHAFTSINFORMATIK 46(3):171–180
Wan Z, Fang Y, Wade M (2007) A ten-year odyssey of the "IS productivity paradox" – a citation analysis (1996–2006). Proceedings of the 13th AMCIS. AIS, Keystone
Windley PJ (2005) Digital identity. O'Reilly, Sebastopol
Yue WT, Çakanyildirim M, Ryu YU, Liu Dengpan (2007) Network externalities, layered protection and IT security risk management. DSS 44(1):1–16

Abstract

Denis Royer, Martin Meints

Enterprise Identity Management – Towards a Decision Support Framework Based on the Balanced Scorecard Approach

Enterprise Identity Management Systems (EIdMS) are an IT-based infrastructure that needs to be integrated into various business processes and related infrastructures. Assessment and preparation of decisions for the introduction need to take the costs, benefits, and the organizational settings into consideration. A variety of methods for the evaluation and decision support of new IT (e. g. EIdMS) are discussed in the literature – however, these are typically based on single dimensions (e. g. financial or technology aspects). This paper proposes a multidimensional decision support framework, based on the Balanced Scorecard concept. The presented approach introduces four perspectives and a related set of initial decision parameters to support decision making. The perspectives are (a) financial/monetary, (b) business processes, (c) supporting processes and (ICT) infrastructure and (d) information security, risks and compliance. Perspectives and adaptable sets of decision parameters also may serve as foundation for software-based decision support instruments.

Keywords: Balanced scorecard, Enterprise identity management, Decision support, IT security