Ganzheitliche Bewertung von Enterprise Identity Management Systemen – Der Ansatz der Balanced Scorecard als taktisches Entscheidungsunterstützungsinstrument

Denis Royer

Lehrstuhl M-Business und Mehrseitige Sicherheit
Universität Frankfurt am Main
Gräfstraße 78
60054 Frankfurt/Main
denis.royer@m-lehrstuhl.de

Abstract: Bei der Einführung von Enterprise Identity Management Systemen (EIdMS) müssen sich Organisationen mit einer Reihe von Problemen auseinandersetzen. Insbesondere in der Entscheidungs- und Planungsphase ist es wichtig, dass Organisationen ihre internen Dimensionen (z.B. Prozesse, Strukturen) und deren Wechselwirkungen untereinander in der Planungsphase von Enterprise Identitätsmanagement (EIdM) Lösungen berücksichtigen und sich nicht ausschließlich auf rein technologische oder finanzielle Aspekte fokussieren. Eine Organisation kann demzufolge die Nutzenpotentiale von EIdM nur dann erkennen, wenn im Vorfeld eine hinreichende Bewertung der anfallenden Kosten und der organisatorischen Aspekte vorgenommen wurde. Im vorliegenden Artikel wird ein Bewertungsansatz auf Basis der „*Balanced Scorecard (BSC)*“ zur Bewertung des Nutzens von EIdM-Investitionen vorgestellt, der in der Planungs- und Entscheidungsphase als Hilfsmittel zur übergreifenden Bewertung des materiellen und immateriellen Nutzens herangezogen werden kann. Im Rahmen dieses Artikels werden dafür notwendigen Vorrausetzungen und organisatorischen Faktoren vorgestellt und diskutiert.

1 Einleitung

In den heutigen, durch Informationstechnologien (IT) unterstützten Arbeitsumgebungen sind Organisationen mit der Bewältigung von vielschichtigen (Geschäfts-) Prozessen konfrontiert. Dabei werden verschiedene IT-Infrastrukturen und -Systeme parallel genutzt, um die diversen betrieblichen Aktivitäten und Transaktionen wie z.B. Personalwirtschaft, Dokumentenmanagement oder Enterprise Resource Planning (ERP) zu unterstützen. In diesem Kontext müssen sich Organisationen mit dem Thema der Nutzer- und Zugangsverwaltung, dem sogenannten *„Identity and Access Management (IAM)“,* auseinandersetzen, um bestehende IT-Infrastrukturen und Systeme vor unbefugten Zugriffen zu schützen und um Datenschutz- und Datensicherheitsanforderungen gerecht zu werden. Weiterhin können durch ihren

Einsatz Kostensenkungspotentiale, z.B. durch die Zentralisierung von Zugangsdatenbeständen oder Helpdesk Aktivitäten, realisiert werden.

1.1 Ziele und Gang der Untersuchung

In der unternehmerischen Praxis setzt eine Entscheidung für oder gegen eine Investition in IT-Sicherheitssysteme wie das hier behandelte Enterprise Identity Management (EIdM) eine fundierte Kosten-Nutzen-Analyse voraus. Um eine adäquate Entscheidungsgrundlage zu schaffen müssen die aus der EIdM-Systemeinführung resultierenden Vor- und Nachteile mit Hilfe geeigneter Methoden identifiziert und bewertet werden. Die Einführung von Enterprise Identity Management Systemen (EIdMS) betrifft verschiedenste Bereiche/Dimensionen der Organisation (Strukturen, Prozesse, Mitarbeiter, etc.), daher ist eine rein finanzielle Betrachtung/Bewertung nicht ausreichend und es bedarf einer geeigneten Vorgehensweise zur ganzheitlichen Bewertung von EIdMS. Eine solche Vorgehensweise wird in dieser Arbeit auf Basis der „*Balanced Scorecard (BSC)*“ von Kaplan und Norton [KN96] entwickelt und erörtert. Damit ist es möglich, neben finanziellen Kennzahlen noch weitere Dimensionen (z.B. Risiken, Prozesse, etc.) mit in der Bewertung zu berücksichtigt. Der vorgestellte Ansatz soll dabei vorrangig als Unterstützungsinstrument in der taktischen Planung mit einem Zeithorizont von einem bis drei Jahren dienen.

Der Artikel gliedert sich wie folgt: Im Anschluss an die Darstellung und Einführung in die vorliegenden Thematik (Kapitel 1) widmet sich Kapitel 2 den verschiedenen Treibern für die Einführung von EIdM-Lösungen. Weitergehend wird in Kapitel 3 der Prozess zur Erhebung der relevanten Faktoren für die Bewertung von EIdM-Projekten vorgestellt. Hier werden auch die Hintergründe im Zusammenhang mit IT-Sicherheitsinvestitionen dargelegt. Kapitel 4 stellt darauf aufbauend den Entwurf für eine EIdM BSC als taktisches Entscheidungsunterstützungsinstrument vor. Kapitel 5 schließt diesen Artikel mit einer Zusammenfassung und dem Ausblick auf den weiteren Forschungsbedarf ab.

1.2 Klassifikation von Enterprise Identity Management (EIdM)

Vor dem Hintergrund steigender Digitalisierung von Geschäfts- und Hilfsprozessen stellt das Thema EIdM eine zunehmende Herausforderung für Unternehmen und Organisationen dar [DD07]. Ein Grund hierfür ist u.a. die sich über den Zeitverlauf ändernden Nutzerberechtigungen (Rollen und Rechte), welche bspw. aus einem Arbeitsstellenwechsel (z.B. Beförderungen) resultieren können. Die Änderungen in den (partiellen) Identitäten[1] der Nutzer müssen möglichst zeitnah und sicher angepasst werden [Wi05] und können dem sogenannten Identitätslebenszyklus zugeordnet werden (siehe Tabelle 1), der aus folgenden vier Prozessschritten besteht: (1.) Einschreibung

[1] Partielle Identitäten sind Untermengen von Attributen einer vollständigen Identität (bspw. einer Person). Jede Identität einer Person besteht aus vielen partiellen Identitäten, wobei jede von ihnen eine Person in einer spezifischen Rolle darstellt (basierend auf den Arbeiten von [Fi07]).

(das sog. Enrolement), (2.) Management, (3.) Unterstützung und (4.) die Löschung der Identitätsdaten [HM06] [Wi05].

In Anlehnung an das Rahmenwerk von Bauer, Meints und Hansen [BMH05] kann man EIdMS den sog. *Typ 1 Identitätsmanagementsystemen* zuordnen, welche der Zuweisung von Identitäten an einen Nutzer dienen. Sie grenzen sich insofern von den sog. *Profiling Systemen* (*Typ 2* – Abstraktion/Ableitung von Identitäten) oder *nutzerzentrierten Identitätsmanagementsystemen* (*Typ3* – Steuerung der „eigenen" Identität) ab, als das sie in einer Organisation Nutzerkonten zentral verwalten.

Weiterhin können die EIdMS hinsichtlich der organisatorischen und technologischen Ebene unterschieden werden. Auf der *organisatorischen Ebene* unterstützen EIdMS die Prozessschritte des Identitätslebenszyklus, in dem sie die Authentifizierung, die Autorisation, die Administration und das Audit (die sogenannten 4 As) der zu verwalteten Nutzerkonten ermöglichen.

Tabelle 1: Schritte im Lebenszyklus von Identitäten (basierend auf [HM06] und [Wi05]).

Einschreibung / Enrolement – Erzeugung eines Nutzerkontos:
Initiale Ausgabe der Credentials und setzen der Zugangsberechtigungen, welche von einem neuen Mitarbeiter benötigt werden.
Management – Pflege der Nutzerkonten:
In sich verändernden Arbeitsumgebungen (z.B. durch Beförderungen oder den Wechsel in andere Abteilungen) muss das „Nutzer und Zugangsmanagement" die Nutzerkonten und die verbundenen Berechtigungen zeitnah handhaben.
Unterstützung – Anpassung von bestehenden Autorisierungen:
Neu-Ausgabe von Credentials (z.B. Zurücksetzung von Passwörtern).
Löschung – Ende des Lebenszyklus:
Entzug oder Sperrung von Nutzerkonten oder Berechtigungen.

Hinsichtlich der technologischen Ebene lässt sich eine Vielzahl von Technologien identifizieren und in die verschiedenen (Dienst-)Bereiche (Nutzerdienste, Identitätsdienste, etc.) des EIdM zuordnen. Hierzu gehören bspw. Single-Sign-On (SSO) Lösungen, Verzeichnisdienste, Public-Key-Infrastrukturen (PKI) und IAM Systeme [Fl07] [Wi05]. Das EIdM ist dabei als eine Unterstützungsfunktion anzusehen, welche sich als zusätzliche Schicht in eine bestehende IT-Infrastruktur einer Organisation als Schnittstelle zwischen Nutzern, Diensten und Applikationen integriert [Fl07].

Entgegen der von vielen (Technologie-) Hersteller kommunizierten Meinung und publizierten Informationen handelt es sich beim EIdM um ein Technologierahmenwerk verschiedener Technologien und Funktionen und *nicht* um ein einzelnes Software-Produkte, welches alle Unternehmensbereiche ohne Anpassungen abdeckt. Die Realität sieht oftmals eher so aus, dass bei der Einführung von EIdM Lösungen in eine Organisation umfangreiche, unternehmensspezifische Anpassungen notwendig sind.

2 Treiber für EIdM Projekte

Es gibt eine Vielzahl von Gründen, welche für die Einführung von EIdMS in eine Organisation sprechend. Eine auf Experteninterviews basierende, explorative Studie konnte (1) IT-Risikomanagement Ziele, (2) Wertschöpfungsziele und (3) Compliance[2] Ziele als die am häufigsten genannten Treiber identifizieren (vgl. Tabelle 2)

Eine falsche oder fehlende Berücksichtigung dieser Aspekte und ein mangelhaftes oder fehlendes Management des Identitätslebenszyklus können erhebliche negative Konsequenzen für die Organisation nach sich ziehen. Dazu zählen bspw. Produktivitätseinbußen und erhöhte Kosten für das Management der Nutzerkonten, Risiken welche mit möglichen Sicherheitslücken einhergehen (resultierend aus schlecht verwalteten Nutzerkonten) oder Sanktionen aufgrund der Nichteinhaltung von relevanten Gesetzen und Regelungen [Be05]. Weiterhin bleibt anzumerken, dass die genannten Treiber für die Einführung von EIdM-Lösungen in keinem Zielkonflikt zueinander stehen, sondern teilweise sogar Synergien aufweisen. Weiterhin resultiert aus der Einführung eines EIdM-Systems eine Vielzahl von Vorteilen. Studien aus dem Bereich der Anwendung von EIdM-Lösungen belegen Kosteneinsparungspotentiale von bis zu 50% beim Anlegen und Administrieren von Nutzerkonten im Vergleich zur manuellen Verwaltung [De07]. Demgegenüber stehen jedoch signifikante Kosten für die Einführung und den Betrieb von EIdM-Systemen. So verursachen EIdM-Projekte schnell Kosten von über 100.000 Euro, die für die Hard- und Software, die Beratungsleistung und andere Kostenfaktoren aufgebracht werden müssen.

Tabelle 2: Treiber für die Einführung von EIdM in Organisationen.

IT-Risikomanagement Ziele:	
	• Minimierung von Haftung • Abwälzung von Risiken des IT-Einsatzes • Erhöhung der IT-Sicherheit
Wertschöpfungsziele:	
	• Effizienzziele (z.B. Prozessoptimierungen) • Generelle Kosteneinsparungen
Compliance Ziele:	
	• Befolgung von relevanten Gesetzen und Regelungen, wie bspw. Basel II, KonTraG oder Sarbanes-Oxley Act (SOX)

Die Auswertung der wissenschaftlichen Literatur zeigt weitere Aspekte und Herausforderungen auf, die neben den Kosten für die Einführung eines EIdM-Systems berücksichtigt werden müssen:

[2] Im hier betrachteten Kontext bezieht sich *Compliance* auf die Verpflichtung für Firmen und öffentliche Einrichtungen dafür Sorge zu tragen, dass ihre Angestellten über relevant Gesetze und Regelungen (z.B. Basel II, Sarbanes-Oxley Act (SOX) oder KonTraG) informiert sind, entsprechende Maßnahmen in der Organisation verankert sind und somit den Gesetzen und Regelungen entsprochen wird (vgl. auch [Be05], [HL07], [Da05]).

- ***Technologie vs. Prozesse:*** Bei der Einführung von EIdM handelt es sich *nicht* um ein vollkommen technologiegetriebenes Thema. Vielmehr entstehen Wechselwirkungen mit den Prozessen, Arbeitsabläufen und der Struktur einer Organisation und der jeweils eingeführten EIdM Technologie. Dementsprechend müssen die daraus resultierenden organisatorischen Aspekte (Zuständigkeiten, Policies, Prozesse) mit in die Analyse einbezogen werden.

- ***Beachtung von projektinhärenten Faktoren:*** Wie bereits beschrieben, werden bei der Einführung von EIdM-Projekten verschiedene Ziele verfolgt (vgl. Tabelle 2). Während bspw. bei einem Projekt der Fokus auf der Erhöhung des IT-Sicherheitsniveaus liegt, stehen in anderen Projekten die Erfüllung der Compliance Anforderungen im Vordergrund. Folglich müssen diese projektinhärenten Faktoren mit erfasst und in die Analyse eingebracht werden, um generalisierbare Aussagen treffen zu können [RR05].

- ***Verallgemeinerung der Kosten:*** Es handelt sich beim EIdMS um ein Technologierahmenwerk (Abschnitt 1.2) welches in existierende IT-Infrastrukturen integriert wird. Projektspezifische EIdM-Lösungen können mit verschiedenen Produktbündeln umgesetzt werden, die sich hinsichtlich ihres Umfangs erheblich unterscheiden können. Zusätzlich sind EIdM-Projekte und die mit ihnen einhergehenden Anpassungen einzigartig, was eine Verallgemeinerung der Kosten für die Implementierung und Einführung erschweren kann. Hier sollten dementsprechend Referenzprojekte als Vergleichbasis herangezogen werden, um eine Abschätzung ermöglichen zu können.

- ***Lebenszykluskosten – Total Costs of Ownership (TCO):*** Letztlich sollten möglichst die zu erwartenden Kosten über den gesamten Einsatzzeitraum einer EIdM-Lösung, die sog. Lebenszykluskosten, berücksichtigt werden. Hier sind die Kostenanteile für Training, Support, wiederkehrende Wartungsmaßnahmen und die Integration in eine bestehende IT-Infrastruktur zu nennen [SU06].

Die Einführung von EIdM-Lösungen stellt eine komplexe und zeitintensive Unternehmung dar Dies bietet einerseits eine Vielzahl von Einsparungspotentialen, auf der anderen Seite sind aber auch eine Reihe von Kosten für die Planung, die Implementierung und den Betrieb zu berücksichtigen.

3 Entwicklung eines Evaluationsprozesses

Die Durchführung einer problemadäquaten Kosten-Nutzen-Analyse bedarf geeigneter Werkzeuge und Bewertungsansätze, die eine Vergleichbarkeit der Ergebnisse für verschiedene Projektalternativen sicherstellen. Dafür sind bei der Gestaltung von Bewertungsansätzen zur Entscheidungsunterstützung auf einige grundsätzliche Anforderungen, wie die Transparenz der Datenerhebung und die methodische Genauigkeit zu achten um eine konsistente Datenbasis zu gewährleisten [RR05]. Dabei ist bei der Erhebung der entscheidungsrelevanten Daten das Aufwand-Nutzen-Verhältnis

zu berücksichtigen. Für die meisten Entscheidungen sind hinreichend genaue Daten ausreichend [Pu04].

Für die Bestimmung des Nutzens von EIdM werden oftmals Metriken mit limitierter Geltungsbereich, wie bspw. die Kapitalverzinsung (ROI)[3], als Bewertungskriterium herangezogen, um die Treiber des EIdM und ihre Auswirkungen (z.B. das Maß der Prozessintegration oder die Einbeziehung aller relevanten Parteien) beurteilen zu können. Im Folgenden wird nun ein generalisierter Bewertungsansatz mit der Zielsetzung der Entscheidungsunterstützung beschrieben.

3.1 EIdM und die Hintergründe von Investitionen im Bereich der IT-Sicherheit

Die Bewertung von Investitionen im Bereich der IT-Sicherheit ist ein vielfach (kontrovers) diskutiertes Themengebiet (vgl. [CMR04], [MMZ07] und [SAS06]). Neben den verschiedenen Problemen von „*klassischen*“ IT-Investitionen, wie dem IT-Produktivitäts-Paradoxon ([Br93], [WFW07]), steht auch die Bewertung von Investitionen im Bereich der IT-Sicherheit und insbesondere des EIdM vor einer Vielzahl von Herausforderungen [MMZ07] [SAS06].

Problematisch erweist sich dabei häufig die Identifikation der potentiellen Einnahmen (die sog. Cash-Inflows), welche durch IT-Sicherheitsinvestitionen generiert werden. Zusätzlich stellt sich die Bestimmung des optimalen Mitteleinsatzes für die gesamte IT-Sicherheit als eine Herausforderung dar. So werden Investitionen in die IT-Sicherheit getätigt um Risiken abzuwenden und mögliche Verluste (finanziell, immateriell, etc.) zu verhindern [SAS06]. Die Abwendung dieser Verluste und Risiken macht es jedoch schwierig oder sogar unmöglich, die relevanten Kosten zu spezifizieren und zu bemessen, da unerwünschte Vorfälle aufgrund dieser Präventivmaßnahmen weitestgehend verhindert werden. In diesem Zusammenhang werden in der Literatur verschiedene Ansätze und Rahmenwerke zur Bewertung der ökonomischen Auswirkungen und Nutzen von IT-Sicherheitsinvestitionen diskutiert. Ein sehr verbreiteter Ansatz stellt dabei der sog. „Return on Security Investments (ROSI)“ dar, welcher zur Monetarisierung von IT-Sicherheitsinvestitionen herangezogen werden kann [CMR04] [MMZ07] [SAS06]. Aufbauend auf dem ROI, ist der ROSI auf die Analyse und Monetarisierung von Produktivitätseinbußen oder potentiellen Verlusten durch Sicherheitslücken ausgerichtet. Neben dieser rein finanziell ausgerichteten Kennzahl bedarf es weiterreichender Metriken, welche auch immaterielle und organisatorische Faktoren zum Zweck der ganzheitlichen Bewertung von EIdM-Investitionen mit in die Analyse einfließen lassen. Dies wird im Folgenden analysiert.

3.2 Strukturelles Vorgehen für die Erhebung der relevanten Daten

Zwecks Komplexitätreduzierung und Problemstrukturierung sowie zur Sicherstellung der systematischen und vollständigen Berücksichtigung aller relevanten Faktoren erfolgt

[3] Die Kapitalverzinsung oder auch „Return on Investment (ROI)“ gibt den Effizienzgrad einer Investition, basierend auf den erwirtschafteten Profit an (vgl. [Pu04] oder [EFS04]).

die Erhebung der Daten von EIdM-Projekten schrittweise. Basierend auf der analysierten wissenschaftlichen Literatur unterteilt sich der hier vorgestellte Prozess in sechs Schritte. Diese lassen sich in die Bereiche Definition, Bewertung und Kalkulation unterteilen (siehe Abbildung 1):

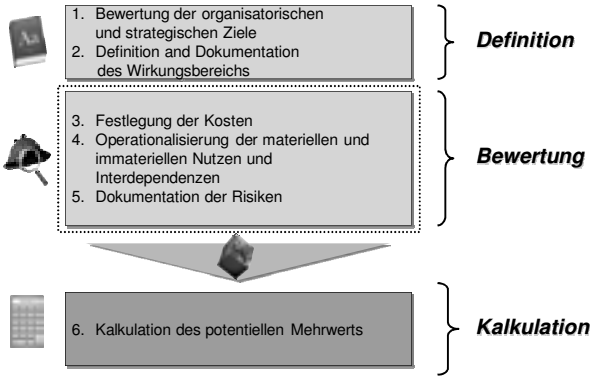

Abbildung 1: Aufbau des Prozesses zur Erhebung der relevanten Faktoren.

- ***Schritt 1:*** Im ersten Schritt werden die strategischen Ziele des EIdM hinsichtlich der strategischen Ziele der Organisation verglichen und bewertet. Zweck ist hierbei die Präzisierung der Zielsetzungen des EIdM (vgl. Tabelle 2).

- ***Schritt 2:*** Basierend auf den festgelegten strategischen Determinanten aus Schritt 1 wird der Wirkungsbereich der EIdM-Lösung definiert und dokumentiert. Um keine wichtigen Informationen außer Acht zu lassen, sollte eine Rückkopplung zu *Schritt 1* erfolgen.

- ***Schritt 3:*** Im dritten Schritt werden die Kosten erfasst, welche im direkten Zusammenhang mit dem EIdM-Projekt stehen. Als geeignete Methoden bieten sich hier die *Total Costs of Ownership (TCO)* oder die *Lebenszykluskostenrechnung (LCC)* an.

- ***Schritt 4:*** Weitergehend werden in Schritt 4 die *materiellen und immateriellen* Nutzenpotentiale erfasst und dokumentiert. Beim materiellen Nutzen wird zwischen direkten und indirekt (über Umrechnungen) erfassbaren Kosteneinsparungen unterschieden. Ein Beispiel für indirekt erfassbare Nutzen sind Prozessverbesserungen in der Unterstützung des Lebenszyklus von Identitäten, die in weniger Support-Anfragen resultieren. Weiterhin müssen auch negative Kosteneffekte mit in die Betrachtung einbezogen werden. Dies ist darin begründet, da IT-Sicherheitsmaßnahmen wie EIdM auch zu Lasten der Produktivität und Bequemlichkeit gehen können [SAS06]. Letztlich müssen die rein qualitativ erfassbaren Nutzen (z.B. höhere Interoperabilität, höhere Prozessreife zwischen Geschäfts- und Hilfsprozessen) erfasst und ihre Wechselwirkungen analysiert werden.

- ***Schritt 5:*** Neben den in Schritt 5 erfassten Nutzenpotentialen müssen auch die mit einem Projekt *verbundenen Risiken* dokumentiert werden (Ressourcen, Zeitplanung, rechtliche Rahmenbedingungen, etc.). Weiterhin sollten die sich ergebenen Auswirkungen der Risiken beschrieben werden, wenn diese eintreten. Risikoanalyseverfahren könne hier helfen die Auswirkungen der relevanten Risiken transparent darzustellen (vgl. [Ke98]). Die verfügbaren Verfahren müssen allerdings um die Risiken der Einführung von EIdM erweitert werden.

- ***Schritt 6:*** Abschließend wird auf Basis der in den vorherigen Schritten erhobenen Daten die Berechnung des Gesamtnutzens durchgeführt.

Durch eine stringente und konsistente Einbindung von Dokumentationszyklen in die einzelnen Analyseschritte ist es weiterhin möglich die Zusammenhänge zwischen den einzelnen materiellen und immateriellen Faktoren besser verstehen zu können. Da EIdM-Projekte verschiedenste Zielsetzungen und Ausrichtungen haben können, ermöglicht eine solche standardisierte Datenerfassung eine transparente Darstellung projektinhärenter Faktoren für die Entscheidungsträger.

4 Vorschlag für eine taktische EIdM Balanced Scorecard (BSC)

Neben einem formalisierten Ablauf für die Bewertung und Aggregation der Daten werden zusätzlich Rahmenwerke für die Entscheidungsunterstützung und Bewertung von EIdM-Lösungen benötigt, um den Gesamtnutzen einer EIdM-Investition besser bestimmen zu können. Ein solches Rahmenwerk muss über die eingeschränkte Sichtweise von rein finanziellen Kennzahlen (bspw. Kapitalwert, ROI, ROSI) hinausgehen (vgl. [JLM04] und [Ma97]) und andere materiellen sowie immateriellen Faktoren und Entscheidungsdeterminanten mit in die Bewertung einfließen lassen. Einen möglichen Lösungsansatz bietet hier eine taktische EIdM BSC, welche an die klassischen BSC von Kaplan und Norton angelehnt ist ([KN96], [Ba01], [BS01]). Durch die Einbeziehung von materiellen und immateriellen Bewertungsfaktoren bietet die BSC einen adäquaten Ansatz um ein integriertes Bewertungsrahmenwerk für die Entscheidungsunterstützung (und weitergehend den Betrieb einer EIdM-Lösung) ableiten zu können.

4.1 Die originäre Balanced Scorecard nach Kaplan und Norton

Die klassische BSC wurde 1992 von Kaplan und Norton als ein *ausbalanciertes Kennzahlensystem* für Unternehmen und Organisationen entwickelt [KN96]. Die BSC ist in vier übergreifende Perspektiven aufgeteilt, welche sich aus der „*Vision und Strategie*“ einer Organisation ableiten. Die vier Perspektiven der BSC umfassen (1.) die Finanzperspektive, (2.) die Prozessperspektive, (3.) die Interne- oder Potentialperspektive und (4.) die Kundenperspektive, welche jeweils spezifische Kennzahlen für die jeweilige Perspektive enthalten.

Die BSC hat das Bestreben die zurückliegenden Erfolge aufzuzeigen und zukünftige Trends abzubilden, indem die einzelnen Perspektiven mit der „*Vision & Strategie*“ einer Organisation verknüpft werden. Die BSC greift dabei nicht nur auf finanzielle Kennzahlen zurückgreift, sondern bezieht auch immaterielle Kennzahlen, wie bspw. die Kundenzufriedenheit, mit ein. So lassen sich umfassendere Erkenntnisse über die Organisation gewinnen und ein nachhaltigeres Handeln im Interesse der Organisation ableiten, als es mit rein finanziellen Kennzahlen möglich wäre. Um die Zusammenhänge und Verknüpfungen zwischen den einzelnen Perspektiven und den darin enthaltenen Kennzahlen aufzeigen zu können werden Kausalketten und kausale Netzwerke für deren Analyse verwendet [JLM04].

4.2 Generischer Entwurf einer taktischen EIdM Balanced Scorecard

Im Gegensatz zur klassischen, strategischen BSC, hat die hier präsentierte BSC einen taktischen Fokus mit einem Zeithorizont von ein bis drei Jahren, wo sie als Entscheidungsunterstützungsinstrument für die Einführung von EIdM genutzt werden kann. Darüber hinaus kann die EIdM BSC in der Implementierungsphase als Steuerungsinstrument zur Messung der Zielerreichung dienen. Basierend auf den bereits beschriebenen Zusammenhängen, umfasst die hier vorgeschlagene BSC folgende vier Perspektiven:

- ***Finanz-Perspektive:*** Diese Perspektive enthält die klassischen finanziellen Kennzahlen. Dazu gehören bspw. die generellen Finanzinformationen und die Kosten, welche mit einem EIdM-Projekt einhergehen (basierend auf TCO, LCC, etc.). Dies hilft eine Übersicht über die potentiellen Zahlungsflüsse zu erhalten.

- ***Geschäftsprozess-Perspektive:*** Hier werden die Kern-Prozesse einer Organisation betrachtet und analysiert. Mit den hier enthaltenen Kennzahlen lassen sich bspw. der Grad der Integration von IS und EIdM in die Geschäftsprozesse einer Organisation und die potentiellen Effizienzsteigerungen quantifizieren [JLM04], bzw. die Prozessreife innerhalb der Organisation, bestimmen.

- ***Risiko-Management und Sicherheits-Perspektive:*** In diesem Bereich werden die potentiellen Risiken (z.B. Projektrisiken, Sicherheitsrisiken) und das Sicherheitsmanagement analysiert, die im Rahmen eines EIdM-Projektes auftreten können. Hierbei lassen sich schwerpunkmäßig Kennzahlen aus den Bereichen Compliance (z.B. Basel II, KonTraG oder SOX), Best-Practice (ITIL, etc.) oder generellen Standards (ISO 27001, etc.) ableiten.

- ***Unterstützungsprozess-Perspektive:*** Die letztgenannte Perspektive untersucht die Unterstützungsprozesse in einer Organisation (Personalwirtschaft, IT, Management, etc.), welche indirekt an der Wertschöpfung des Unternehmens beteiligt sind. Im Zusammenhang mit dem EIdM erlaubt diese Perspektive eine

weitergehende Analyse der Prozessreife zwischen den Geschäfts- und Unterstützungsprozessen.

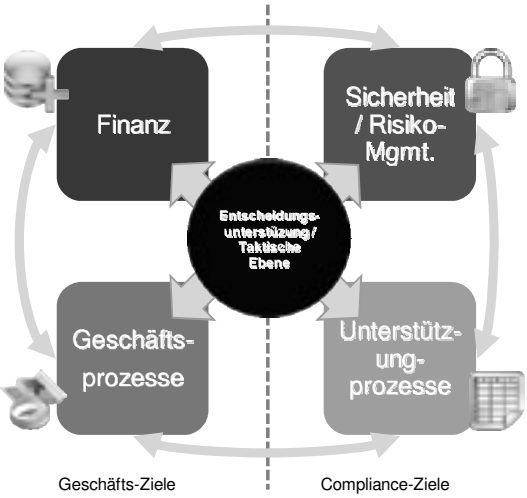

Abbildung 2:Initialer Entwurf einer EIdM Balanced Scorecard (eigene Darstellung basierend auf [BS01], [JLM04] und [KN96]).

Die für den Anwendungsbereich von EIdM abgeleitet BSC ist in Abbildung 2 dargestellt. Im Weiteren lassen sich die vier Perspektiven den Geschäftszielen (Finanz und Geschäftsprozesse) oder den Compliance-Zielen (Sicherheit / Risiko-Management und Unterstützungsprozesse) zuordnen. Durch den Einsatz der hier vorgestellten EIdM BSC lassen sich diese zwei Zielsetzungen übergreifend gegenüberstellen. Weiterhin können die so gewonnen Informationen für den weiteren Entscheidungsprozess genutzt werden.

Die einzelnen Perspektiven und deren Kombinationen lassen sich auf taktischer Ebene größtenteils mit bereits existierenden Best-Practice Ansätzen und relevanten Standards (z.B. ISO 9001, ISO 27001) abdecken oder verknüpfen. Ferner kann durch die Zusammenführung von Best-Practice-Ansätzen und Standards eine integrierte und detaillierte Analyse der einzelnen Perspektiven ermöglicht werden.

Wie auch bei der klassischen BSC gilt es zu bedenken, dass die in den vier Perspektiven enthaltenen Kennzahlen Vernetzungen aufweisen können. Diese Vernetzungen und ihre Wechselwirkungen sollen im Rahmen der weiteren Forschung in diesem Gebiet analysiert und mit Hilfe von Experteninterviews erhoben werden. Einen ersten systematischen Ansatz zur Erfassung, Analyse und Ableitung der Kennzahlen wurde in Abschnitt 3 vorgestellt.

4.3 Einschränkungen der EIdM Balanced Scorecard

Analog zur klassischen BSC unterliegt auch die EIdM BSC einigen Schwierigkeiten. Dazu zählen z.B. ihre Komplexität und die benötigte Zeit zu ihrer Einführung. Da die

EIdM BSC bereits in einer komplexen Entscheidungssituation eingesetzt wird, ermöglicht ihre Strukturierung der in der Organisation verfügbaren Informationen eine transparentere Entscheidungsfindung, da alle Entscheidungsrelevanten Faktoren miteinander in Beziehung gestellt werden können. Weiterhin stellen die eingeschränkte Verfügbarkeit und Unsicherheiten der benötigten Informationen eine Herausforderung für die Erstellung von Prognosen dar. Hier können Verfahren wie die Szenario-Technik [GH97] oder Risikoabschätzungsverfahren mögliche Hilfsmittel und Lösungsmöglichkeiten sein.

5 Zusammenfassung und Ausblick

Bei der Einführung von EIdMS sind Organisationen mit einer Vielzahl von Kosten, internen Dimensionen und deren Wechselwirkungen untereinander konfrontiert, die bei der Realisierung von EIdM-Projekte beachtet werden müssen. Dieser Artikel präsentiert einen Ansatz für die Erfassung und Gestaltung der nötigen Entscheidungsdeterminanten. Weiterhin wird die Überführung in ein Kennzahlensystem, die EIdM BSC, beschrieben. Die dargestellte BSC erlaubt es, Geschäftsziele und Compliance-Ziele miteinander in Beziehung setzen zu können und so eine ganzheitliche Bewertung zu ermöglichen.

Die EIdM BSC unterstützt den Entscheidungsprozess in einer Organisation auf der taktischen Managementebene. Jedoch besteht weiterer Forschungsbedarf, um die Wechselwirkungen der in der EIdM BSC enthaltenen materiellen und immateriellen Kenzahlen in der Praxis besser verstehen zu können. Der Nutzen des vorgestellten Ansatzes für die taktische Entscheidungsfindung in Organisationen soll zukünftig in der Praxis weiter analysiert und evaluiert werden. Die hier gewonnen Erkenntnisse sollen dabei in die Weiterentwicklung der EIdM BSC einfließen.

6 Danksagungen

Die vorliegende Forschung wurde durch das EU Exzellenznetzwerk FIDIS (*Future of Identity in the Information Society*) finanziert [Fi07]. Der Autor möchte allen Personen danken, die geholfen haben diesen Artikel zu verbessern. Ein spezieller Dank gilt Meike Torney für die umfangreiche und konstruktive Kritik in der Fertigstellungsphase.

7 Literaturverzeichnis

[Ba01] Baschin, A.: Die Balanced Scorecard für Ihren IT-Bereich: ein Leitfaden für Aufbau und Einführung. Campus-Verlag, Frankfurt/Main, 2001.

[BS01] Baschin, A.; Steffen, A.: IT-Controlling mit der Balanced Scorecard. Zeitschrift für Controlling u. Management, Nr. 6 (45), 2001; S. 367-371.

[BMH05] Bauer, M.; Meints, M.; Hansen, M.: Deliverable D3.1: Structured Overview on Prototypes and Concepts of Identity Management Systems. FIDIS, 2005.

[Be05] Berghel, H.: The Two Sides of ROI: Return on Investment vs. Risk of Incarceration. Communications of the ACM, Nr. 4 (48), 2005; S. 15-20.

[Br93] Brynjolfsson, E.: The Productivity Paradox of Information Technology. Communications of the ACM, Nr. 12 (36), 1993; S. 67-77.
[CMR04] Cavusoglu, H.; Mishra, B.; Raghunathan, S.: A Model for Evaluating IT Security Investments. Communications of the ACM, Nr. 7 (47), 2004; S. 87-92.
[Da05] Damianides, M.: Sarbanes -Oxley and IT Governance: New Guidance On It Control And Compliance. Information Systems Management, Nr. 11 2005; S. 77-85.
[De07] Deron GmbH: Identity Management Studie 2006/2007. Deron, Stuttgart, 2007.
[DD07] Dewey, B.I.; DeBlois, P.B.: Current Issues Survey Report 2007. EDUCAUSE Quarterly, Nr. 2 (30), 2007; S. 12-31.
[EFS04] Erdogmus, H.; Favaro, J.; Strigel, W.: Return on Investment. IEEE Software, Nr. 3 (21), 2004; S. 18-22.
[Fi07] FIDIS NoE: Future of Identity in the Information Society (FIDIS). http://www.fidis.net, 2007.
[Fl07] Flynn, M.J.: Enterprise Identity Services. http://360tek.blogspot.com/2006/07/enterprise-identity-services.html, 2007.
[GH97] Geschka, H.; Hammer, R.: Die Szenario Technik in der strategischen Unternehmensplanung. In (Hahn, D.; Taylor, B. Hrsg.): Strategische Unternehmensplanung - strategische Unternehmensführung, Physica, Heidelberg, 1997; S. 464-489.
[HL07] Hall, J.A.; Liedtka, S.L.: The Sarbanes-Oxley Act: IMPLICATIONS for large-scale IT Outsourcing. Communications of the ACM, Nr. 3 (50), 2007; S. 95-100.
[HM06] Hansen, M.; Meints, M.: Digitale Identitäten – Überblick und aktuelle Trends. Datenschutz und Datensicherheit (DuD), Nr. 9 (30), 2006; S. 571-575.
[JLM04] Jonen, A. et al.: Balanced IT-Decision-Card, Ein Instrument für das Investitionscontrolling von IT-Projekten. Wirtschaftsinformatik, Nr. 3 (46), 2004; S. 196-203.
[KN96] Kaplan, R.S.; Norton, D.P.: The Balanced Scorecard. Translating Strategy into Action. Random House, Boston, 1996.
[Ke98] Keil, M. et al.: A Framework Identifying Software Project Risks. Communications of the ACM, Nr. 11 (41), 1998; S. 76-83.
[MMZ07] Magnusson, C.; Molvidsson, J.; Zetterqvist, S.: Value Creation and Return On Security Investmensts (ROSI). In (Venter, H. et al. Hrsg.): IFIP SEC 2007: New Approaches for Security, Privacy and Trust in Complex Environments, Springer, Boston, 2007; S. 25-35.
[Ma97] May, T.A.: The death of ROI: re-thinking IT value measurement. Information Management & Computer Security, Nr. 3 (5), 1997; S. 90-92.
[Pu04] Purser, S.A.: Improving the ROI of the security management process. Nr. 6 (23), 2004; S. 542-546.
[RR05] Rossnagel, H.; Royer, D.: Investing in Security Solutions - Can Qualified Electronic Signatures be Profitable for Mobile Operators. In (AIS Hrsg.): Proceedings of the 11th Americas Conference on Information Systems (AMCIS), Omaha, Nebraska, 2005; S. 3248-3257.
[SU06] Schmeh, K.; Uebelacker, H.: Sicherheit, die sich rechnet - Return-on-Investment in der IT-Security. http://www.heise.de/tp/r4/artikel/18/18954/1.html, 2006.
[SAS06] Sonnenreich, W.; Albanese, J.; Stout, B.: Return On Security Investment (ROSI) – A Practical Quantitative Model. Journal of Research and Practice in Information Technology, Nr. 1 (38), 2006; S. 45-56.
[WFW07] Wan, Z.; Fang, Y.; Wade, M.: A Ten-Year Odyssey of the “IS Productivity Paradox” - A Citation Analysis (1996-2006). In (AIS Hrsg.): Proceedings of the 13th Americas Conference on Information Systems (AMCIS), Keystone, Colorado, 2007.
[Wi05] Windley, P.J.: Digital Identity. O’Reilly, Sebastopol et al., 2005.