

# **Konzeption einer VOFI-basierten Methode zur Entscheidungsunterstützung für IS-Sicherheitsinvestitionen**

Heinz Lothar Grob, Gereon Strauch, Christian Buddendick

European Research Center for Information Systems  
Westfälische Wilhelms-Universität Münster  
Leonardo-Campus 3  
49149 Münster, Deutschland  
grob@ercis.de  
gereon.strauch@ercis.de  
christian.buddendick@ercis.de

## **Abstract:**

Die Sicherheit von Informationssystemen ist heutzutage ein vitaler Faktor für viele Unternehmen. Um eine adäquate Sicherheit zu erreichen, stehen eine Vielzahl unterschiedlicher Maßnahmen zur Verfügung, die von technischen Maßnahmen (z. B. Einsatz einer Firewall) bis hin zu organisatorischen Maßnahmen (z. B. Implementierung eines Security Awareness Management) reichen. Die Umsetzung dieser Maßnahmen erfordert Investitionen, deren Return wie bei sämtlichen IT-bezogenen Investitionen unsicher und schwer bestimmbar ist. Der Erfolg der Maßnahmen in einem Unternehmen ist nur indirekt über eine Verringerung eines zukünftigen Risikos und damit der verbundenen Auszahlungen wahrnehmbar. Eine angemessene Methode zur Beurteilung der Vorteilhaftigkeit alternativer IS-Sicherheitsmaßnahmen liegt bislang nicht vor. Bisherige Methoden zur Entscheidungsunterstützung weisen entweder den Mangel auf, dass sie aus theoretischer Sicht unbefriedigend (z. B. der weit rezipierte Return of Security Investment (ROSI)-Ansatz) darstellen oder sich als nicht praxistauglich erwiesen haben. In dem vorliegenden Beitrag wird eine Konzeption für eine Methode vorgeschlagen, bei der der Erfolg alternativer Sicherheitsinvestitionen auf Basis einer prozessorientierten Sichtweise ermittelt werden kann. Die Konzeption basiert hierbei auf einer umfassenden Analyse des State-of-the-Art im Bereich des IS-Sicherheitsmanagements sowie aktuellen Konzepten zum Geschäftsprozessmanagement und -controlling. Diese Methode bildet die langfristigen Entscheidungskonsequenzen unter Berücksichtigung der Unsicherheit ab und ermöglicht einen direkten Vergleich des Returns alternativer Maßnahmen. Entscheidungsträger werden somit in die Lage versetzt, Investitionen in bestimmte IS-Sicherheitsmaßnahmen zu priorisieren.

## 1 Einleitung

Die Notwendigkeit von Informationssystem-Sicherheitsmaßnahmen ist angesichts der steigenden Bedeutung betrieblicher Informationssysteme (IS) und der stetigen Zunahme von Sicherheitsvorfällen unumstritten. Ein Beleg hierfür ist das in der Vergangenheit überdurchschnittliche Wachstum der IS-Sicherheits-Budgets im Vergleich zu den Gesamt-IS-Budgets [BSI00]. Bei der Planung und Umsetzung von IS-Sicherheitsmaßnahmen wurden Fragen der Wirtschaftlichkeit zunächst kaum beachtet [BSI00]. Inzwischen wird in neueren Arbeiten jedoch die grundsätzliche Notwendigkeit von Wirtschaftlichkeitsanalysen hervorgehoben [Fe06], allerdings werden die vorliegenden Erkenntnisse in diesem Forschungsgebiet bislang als „vage“, „unbrauchbar“ oder ohne Bezug zu konkreten Handlungsempfehlungen charakterisiert [Kü05; Po06; Pe01]. Bei der Messung der Wirtschaftlichkeit von IS-Sicherheitsmaßnahmen stellen sich ähnliche Herausforderungen, wie sie bereits im Bereich von allgemeinen IT-Investitionen anzutreffen sind. Obwohl das IT-Produktivitätsparadoxon seit Jahren als überholt angesehen wird [BH96; BH03], zeigen aktuelle Studien, dass Führungskräfte immer noch skeptisch sind, ob IT-Investitionen einen adäquaten Wertbeitrag liefern können [Ca03; Lu04]. Verschärft wird diese Problematik bei IS-Sicherheitsinvestitionen zudem durch den Umstand, dass die Erfolgswirkungen von Maßnahmen ausschließlich indirekt sind, da sie zur Verringerung eines zukünftigen Risikos beitragen [Vo02; Ro05; Mc05]. Die Aussage: „IS-Sicherheitsfunktionen sind immer dann nützlich gewesen, wenn nichts passiert ist.“ [Fe06] unterstreicht diese Beobachtung. Zudem sind die Abhängigkeiten zwischen verschiedenen IS-Sicherheitsmaßnahmen zu berücksichtigen, da oftmals nur der Erfolg von Maßnahmenbündeln ermittelt werden kann [So00]. Ein Ansatz zur notwendigen Quantifizierung muss daher über differenzierte Gestaltungsparameter verfügen, um der inhärenten Komplexität gerecht zu werden. Erschwerend kommt hinzu, dass in der eher technisch geprägten Domäne des Sicherheitsmanagements bei Fragen der Wirtschaftlichkeitsbetrachtung von technischen Maßnahmen reziproke Experten-Laien-Beziehungen bestehen, die besonders nach transparenter Darstellung verlangen [BJR03]. Dabei dürfen insbesondere bei einer Verdichtung zu einer Entscheidungsempfehlung keine elementaren wirtschaftswissenschaftlichen Anforderungen missachtet werden.

Bei der Konzeption einer Methode zur Entscheidungsunterstützung für IS-Sicherheitsinvestitionen sind diese besonderen Herausforderungen zu berücksichtigen. Dem vorliegenden Beitrag liegt ein gestaltungsorientiertes Forschungsdesign zugrunde, wobei eine konzeptionell-deduktive-Forschungsmethode gewählt wurde. Eine Analyse des aktuellen State-of-the-Art im Bereich des IS-Sicherheitsmanagements zeigt, dass die vorgeschlagenen Methoden entweder theoretisch nicht exakt oder praxisuntauglich sind. Ausgehend von den bestehenden Anforderungen wird in diesem Beitrag somit eine Methode vorgeschlagen, die eine Beurteilung der Wirtschaftlichkeit alternativer IS-Sicherheitsinvestitionen ermöglicht. Hierbei wird dem Umstand Rechnung getragen, dass die Auswirkungen von IT-Investitionen zunächst auf Prozessebene beobachtet werden können [Ta08]. Die Methode unterstützt die Berechnung der Ein- und Auszahlungen für sämtliche Prozesse, auf die IS-Sicherheitsmaßnahmen Einfluss haben und verdichtet diese im Rahmen einer mehrperiodigen Investitionsrechnung. Um der Unsicherheit gerecht zu werden, sind in der Methode zudem Aspekte der Monte-Carlo-

Simulation vorgesehen, die es ermöglicht, unsichere Parameter über Verteilungsannahmen bei der IS-Sicherheitsinvestitionsentscheidung abzubilden. Der Beitrag endet mit einer kurzen Zusammenfassung und einem Ausblick auf zukünftige Forschungsarbeiten.

## **2 State-of-the-Art der Entscheidungsunterstützung für IS-Sicherheitsinvestitionen**

Im Folgenden werden die in der Literatur identifizierten Ansätze hinsichtlich der dargestellten Anforderungen untersucht. Da Investitionen in IS-Sicherheit in der Regel keinen unmittelbaren Ertrag mit sich bringen, sondern dazu beitragen, unerwünschte Ereignisse abzuwenden und so Schäden zu verhindern, ist ein etablierter Ansatz, sie zu bewerten, die Verringerung des Erwartungsschadens zu ermitteln. Einer der ersten und wichtigsten Ansätze hierzu ist die im Jahr 1979 vom National Bureau of Standards veröffentlichte Richtlinie zur Messung von IS-Sicherheitsrisiken („Guideline for Automatic Data Processing Risk Analysis“) [NBS79]. Die Spitzenkennzahl Annual Loss Expectancy (ALE) wird aus der Summe der zu erwartenden jährlichen Schäden gebildet, die auf Sicherheitslücken zurückzuführen sind [Me03]. Das ALE-Konzept ist in den 80-er Jahren in Amerika vor allem auf Grund der Förderung durch das National Institute of Standards and Technology (NIST) verstärkt zum Einsatz gekommen. Mit dem Auslaufen dieser Projekte war das Konzept aber fast vollständig in Vergessenheit geraten [No05]. Als Hauptgründe für das Scheitern des ALE-Konzepts in der Praxis nennt Soo Hoo den hohen Detaillierungsgrad und die hohe Kompliziertheit des Modells, die starke Abhängigkeit des Modells von einer vollständigen Datenbasis und die inhärente Annahme, dass sämtliche Größen deterministisch und im Voraus bekannt sind [So00]. Daneben wurde oft der Mangel an notwendigen empirischen Daten bemängelt [Me03].

Nachdem sich das ALE-Konzept als impraktikabel erwiesen hat, wurden weitere Anstrengungen unternommen, um einen tragfähigen Ansatz zur Beurteilung der Wirtschaftlichkeit von Sicherheitsinvestitionen zu entwickeln. Daraus resultieren die Ansätze der zweiten Generation [So00]. Diese charakterisieren sich durch eine Komplexitätsreduktion im Vergleich zum ALE-Konzept. Exemplarisch seien das Integrated Business-Risk Management Framework, rein wertorientierte Methodologien, Szenario-Analysen und Best Practice Ansätze genannt. Beim Integrated Business-Risk Management Framework, einem nicht-technischen Modell, werden die IS-Sicherheitsrisiken analog zu den üblichen Business-Risiken (operative, finanzielle, etc.) und damit den Spezifika der Problemstellung unangemessen behandelt. Wertorientierte Methodologien fokussieren nur die mögliche Schadenshöhe eines Ereignisses unter Ausblendung der Eintrittswahrscheinlichkeiten und erlauben so keine vollständige Quantifizierung des Risikos. Bei Szenario-Analysen liegt der Fokus auf einem oder einigen wenigen Bedrohungsszenarien und erlauben somit nicht die Beurteilung umfassender Investitionen. Best Practice Ansätze gestatten als standardisierte Vorgehensempfehlungen keine Berücksichtigung individueller Spezifika.

Da bei diesen Ansätzen der Nutzen einer IS-Sicherheitsinvestition nicht quantifiziert wird und wesentliche Größen ausgeklammert werden, sind sie nicht zur

Entscheidungsunterstützung geeignet [Wa05]. Viel der im Folgenden entwickelten so genannten Ansätze der „Dritten Generation“ [So00], wie z. B. die von Gordon/Loeb, Cavusoglu/Mishra/Raghunathan oder Cremoni/Martini [GL02; CMR04, CM05], fokussieren eher auf die Erklärung der ökonomischen Wirkungszusammenhänge im Kontext von IS-Sicherheitsmaßnahmen. Sie liefern damit einen wesentlichen Erklärungsbeitrag, durch die eher theoretische Natur der Modelle, bei denen wesentliche Aspekte ausgeblendet werden oder die notwendigen Parameter nicht mit vertretbarem Aufwand zu bestimmen wären [So00], sind diese jedoch nicht zur Entscheidungsunterstützung geeignet. Daher ist der Bedarf nach einer angemessenen und praktikablen Methode zur Wirtschaftlichkeitsbeurteilung weiterhin ungebrochen [No05].

Eine Kennzahl zur Wirtschaftlichkeitsbetrachtung, die hingegen einige Verbreitung in der Praxis erlangt hat, ist der Return on Security Investment (ROSI), mit dem die Wirtschaftlichkeit einer Sicherheitsmaßnahme beurteilt werden soll. Der Ansatz stieß aus zwei Gründen auf großes Interesse: Zum einen soll der ROSI durch eine vorgebliche Analogie zum Return on Investment (ROI) eine solide und anerkannte Basis für Investitionsentscheidungen bieten [Ma04; Pe01]. Zum anderen wird die scheinbar klare Aussage und Einfachheit der Kennzahl betont [No05]. In der Literatur gibt es noch keine einheitliche Definition des ROSI: Neben der Verwendung unterschiedlicher Variablenbezeichnungen und der Verwendung unterschiedlicher Ausgangsgrößen wird der ROSI einerseits als Absolutwert [Be02; Po06], andererseits als Quotient [Ma04; SAS05] dargestellt [No05]. In der Regel wird die Darstellung als Absolutwert bevorzugt:

$$R - S + T = ALE \Leftrightarrow R - ALE = S - T = ROSI^1$$

An anderer Stelle findet sich dagegen der ROSI in der Quotientenschreibweise [Ma04; SAS05]:

$$ROSI = \frac{R - ALE}{T} = \frac{S - T}{T}$$

Beiden Varianten des ROSI-Konzeptes ist zu Eigen, dass das ALE-Konzept mit dem klassischen Total Cost of Ownership-Konzept (TCO) für IS-Sicherheitsinvestitionen kombiniert wird. Damit werden allerdings auch die kritischen Aspekte dieser Konzepte übernommen. Dies sind einerseits die schon oben diskutierten Kritikpunkte des ALE-Ansatzes. Außerdem werden wesentliche Nachteile der klassischen TCO-Methode übernommen, in der z. B. auch nicht die für eine mehrperiodige Betrachtung notwendigen Zins- und Steuerzahlungen eingehen [vB07a]. Zudem wird dabei in der Regel nur auf die direkten Veränderungen des Erwartungsschadens und die reinen Maßnahmenkosten fokussiert, indirekte Zahlungen werden nicht berücksichtigt.

---

<sup>1</sup> Mit *ALE* (*Annual Loss Expectancy*) dem jährlichen Erwartungsschaden nach dem ALE-Konzept; *R* (*Recovery Cost*) als den jährlichen Kosten zur Beseitigung der Schäden von Sicherheitsvorfällen; *S* (*Savings*) Summe der jährlich durch die Maßnahmen verhinderten Schäden; *T* (*Tool Cost*) als Kosten für Sicherheitsmaßnahmen, in der Regel berechnet nach dem Konzept Total Cost of Ownership.

Soo Hoo geht eine wesentliche Einschränkung der herkömmlichen Darstellungen des ROSI-Ansatzes an, indem er Investitionsentscheidungen betrachtet, bei denen verschiedene Sicherheitsrichtlinien als Bündel mehrerer Sicherheitsmaßnahmen bezüglich ihres „Net Benefit“ verglichen werden [So00]. Mit dem „Net Benefit“ soll eine quantitative Bewertung einer Sicherheitsinvestition unter Berücksichtigung aller auf die Investition zurückzuführenden zusätzlichen Kosten, Leistungen und der veränderten ALE erreicht werden. Bei allen bisher dargestellten Ansätzen wird ebenso wie bei den meisten anderen Ansätzen eine einperiodige Betrachtung vorgenommen [So00; GL02; Ma04]. Dabei werden entweder Durchschnittsgrößen verwendet oder es wird die problematische Annahme der Konstanz der Parameter zu Grunde gelegt. Damit ist es unmöglich, mit diesen Ansätzen die Komplexität der Entscheidungssituation adäquat abzubilden. Wird dennoch eine explizite mehrperiodige Betrachtung vorgenommen, so erfolgt dies teilweise ohne Berücksichtigung von Zinsen [so bei Po06]. Die Annahme dieser gehört aber zu einer der wesentlichen Anforderungen, die an Instrumente zur Beurteilung von IT-Sicherheitsmaßnahmen gestellt werden [FPW07].

Bei anderen Ansätzen der „dritten Generation“ wird auf klassische Methoden der Investitionsrechnung zur Verdichtung der Daten zu einer Entscheidungsempfehlung zurückgegriffen, wie der Kapitalwertmethode oder der internen Zinsfußmethode [Bu02; Me03; GL05; GL06; La06; FPW07]. Da diese Ansätze sich durch rigide Prämissen z.B. hinsichtlich der Finanzierung auszeichnen, kann der Forderung einer transparenten und komplexitätsadäquaten Abbildung der Entscheidungssituation damit nicht entsprochen werden. Viel mehr wird in der Regel nicht expliziert, wie die entsprechenden Größen, deren Bestimmung vor allem im Zentrum Bemühungen stehen sollte, erfasst werden können. Dabei wird bei der Erfassung der relevanten Größen auf Verfahren (Nutzwertanalyse, Analytical Hierachy Process etc.) zurückgegriffen [Lo00; Bu02; Co05; BGL05], bei denen relevante Daten teilweise intransparent und methodisch fragwürdig verdichtet werden. Die wesentliche Problemstellung liegt in diesem Anwendungskontext nicht in der Berechnung einer finanzmathematischen Größe, sondern in der Erfassung aller relevanten Zahlungsströme, wobei wie bereits ausgeführt insbesondere in diesem Kontext unterschiedlichen Domänenwissens auf jeder Stufe der Entscheidungsfindung und –verdichtung Transparenz herrschen.

Das bedingt vor allem die vollständige Erfassung aller relevanten Zahlungsströme unter Berücksichtigung aller potentiellen direkten, indirekten und derivativen Größen, die in diesem Kontext besonders wichtig sind, wie z.B. auch Steuern oder relevante Eigenkapitalunterlegung. So ist z. B. die bei Informationssystemen besonders wichtige Entscheidung zwischen Anschaffung oder Leasing, Eigenerstellung und Fremdbezug bzw. Outsourcing ohne Zinsen und Steuern nicht zu beurteilen, weil zeitlichen Effekten und Steueraspekten dabei besondere Bedeutung zukommt. Die Kritik an der Vernachlässigung solcher Größen ist gerade im Bereich des IS-Controllings nicht neu [Ka86]. Im Folgenden wird eine Methode eingeführt, die eine umfassende und integrierte Erfassung aller relevanten Daten unterstützt und eine komplexitätsadäquate Verdichtung zu einer Empfehlung im dargestellten Entscheidungskontext erlaubt.

### 3 Konzeption einer Methode zur Entscheidungsunterstützung

#### 3.1 Prozesse als Basis der Entscheidungsunterstützung

Da die Auswirkungen von IS-Sicherheitsmaßnahmen, wie bei sämtlichen IT-Investitionen, zunächst in den Prozessen zu beobachten sind [Ta08], sollten diese auch – in Analogie zum Business Management im Mittelpunkt des Sicherheitsmanagements stehen [SN06; Ko98; Rö03; JTQ07]. Für die Prozessorientierung spricht im Kontext des Sicherheitsmanagements vor allem, dass die Prozesssicht wie in Abbildung 1 dargestellt die Integration unterschiedlicher relevanter Perspektiven des Sicherheitsmanagement wie der Organisationsstruktur, Raumpläne, Rechtekonzepte etc. in den Prozessmodellen erlaubt. Andererseits können anhand der Prozesse über die Analyse des Gefährdungspotentials von Ereignissen auf die wertschöpfenden Aktivitäten die potentiellen Verluste ermittelt werden. Dazu sind die Auswirkungen auf die Sicherheitsqualität der Prozesse hinsichtlich Vertraulichkeit, Verfügbarkeit und Integrität durch die Gefährdungen und möglichen Gegenmaßnahmen abzubilden. Dazu kann wie in Abbildung 1 exemplarisch dargestellt z.B. auf die Grundschutzkataloge zurückgegriffen werden.

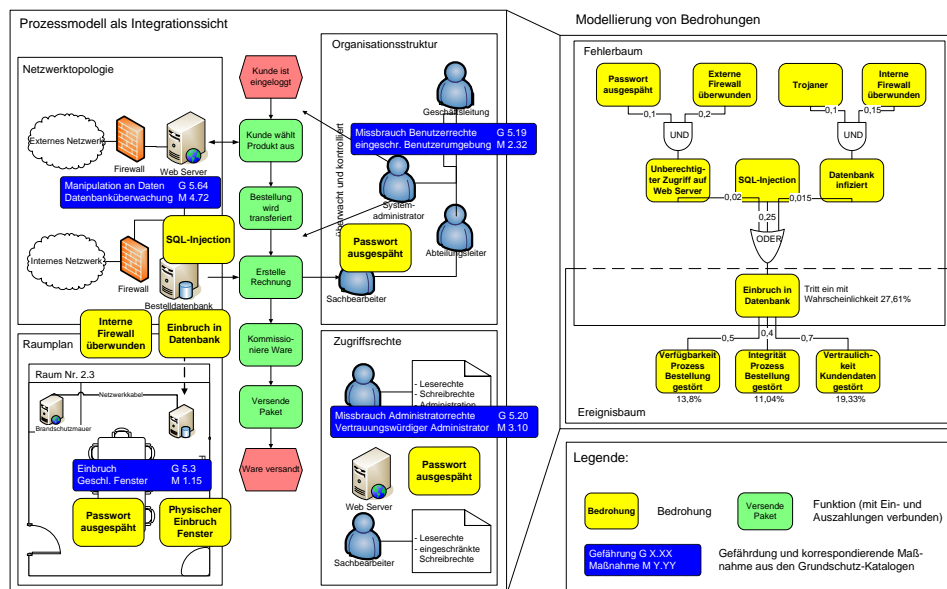


Abbildung 1: Prozesse als Integrations-sicht von Bedrohungen, Sicherheitsmaßnahmen und Ein- und Auszahlungen

Maßnahmen und Schäden etc. lassen sich dabei auch stochastisch in einer geeigneten Kombination von Fehler- und Ereignisbaumanalyse einbringen, bei der Fehlerbaumanalyse Schadenereignisse modelliert werden, deren Auswirkungen auf die Prozesse mittels einer Ereignisbaumanalyse dargestellt wird [K05]. Dieses Vorgehen ist in anderen Kontexten z.B. im Rahmen von Möglichkeits- und Einfluss-Analysen

(FMEA) oder der Hazard Analysis Critical Control Point Methode (HACCP) bekannt [Fr89; Sc99; Pi97]. Das Vorgehen kann hier aus Platzgründen nicht detailliert beschrieben werden, zumal hinsichtlich der expliziten Ausgestaltung auch noch weiterer Forschungsbedarf besteht.

Daneben lassen sich anhand der Prozessmodelle über die entsprechenden Leistungsbeiträge und Ressourcenbeanspruchung auch die finanzielle Auswirkungen der Maßnahmen abbilden. Dieses Vorgehen findet analog in der Prozesskostenrechnung statt, hier sollen wegen des Investitionscharakters allerdings Ein- und Auszahlungen anstelle von Kosten- und Leistungen als periodisierte Größen im Vordergrund stehen. Dieses Vorgehen ist bereits auch in anderen Kontexten in Form einer prozessorientierten Investitionsrechnung dargestellt worden [KH99; MTS04; KSW06]. Die Entscheidungssituation einer IS-Sicherheitsinvestition ist dadurch geprägt, dass neben den direkten Ein- und Auszahlungen, wie der Veränderung des Erwartungsschadens, auch sämtliche indirekten Zahlungen erfasst werden müssen, die durch die Durchführung der Investition verursacht werden [NKB05]. Durch Sicherheitsmaßnahmen können z.B. auch Auszahlungen im Bereich des 1st Level-Supports durch Einführung zertifikatsbasierter Mitarbeiterausweise reduziert werden [Ma04]. Daneben sollten auch zusätzliche Einnahmen berücksichtigt werden, wie sie z. B. aus einem Anstieg der Neukunden-Akquirierung durch ein sichtbar höheres Sicherheitsniveau (z. B. eine SSL-Verschlüsselung für einen Online-Shop) resultieren können. Unterschiedliche Prozessdesigns verursachen ebenso unterschiedliche Zahlungsfolgen. So können z. B. Kunden durch umständliche Bestellprozesse auch von einem Kauf abgehalten werden. Diesem kommt bei dem vorgestellten Vorgehen entgegen, dass neben unterschiedlichen Maßnahmenbündeln auch weitergehende Auswirkungen wie Produktivitätsveränderungen anhand verschiedener Prozessdesigns untersucht werden können.

Basierend auf den dargestellten Erkenntnissen soll im Folgenden ein Vorgehensmodell vorgestellt werden, mit dem Investitionsalternativen in IS-Sicherheitsmaßnahmen bewertet werden können. Dabei werden nicht einzelne Maßnahmen oder Investitionen isoliert betrachtet, sondern Investitionsalternativen als unterschiedliche Bündel von Maßnahmen [So00]. Damit existieren wenigstens zwei Alternativen, die verglichen werden können, der Fall **mit** einer Sicherheitsinvestition (With-Fall) und der Fall **ohne** (Without-Fall). Für diese konkurrierenden Investitionen werden die entsprechenden vollständigen Zahlungsfolgen ermittelt, das heißt, es werden auch die indirekten Auswirkungen der Maßnahmen wie Produktivitätsveränderungen berücksichtigt, um anschließend unter Ableitung derivativer Zahlungen wie Zinsen und Steuern die Alternativen zu Zielwerten zu verdichten, die einen Vergleich erlauben. Im Folgenden soll ein Ansatz dargestellt werden, mit dem die gewonnenen Daten zur Entscheidungsunterstützung so verdichtet werden können, dass die notwendige Transparenz nicht verloren geht.

### 3.2 Verdichtung zur Entscheidungsempfehlung

Wesentliches Anliegen einer weiteren Verdichtung zu Zielgrößen, die eine Entscheidungsunterstützung in der Auswahl der relevanten Alternative bieten, sollte sein, dass die Transparenz und Flexibilität für eine komplexitätsadäquate Abbildung der Entscheidungssituation gewährleistet werden. Dabei bietet sich aus dem Instrumentarium der dynamischen Investitionsrechnung hier insbesondere das der vollständigen Finanzpläne (VOFI) an [Gr89]. Diese Methode wird hier im Gegensatz zu anderen Ansätzen verwendet, da neben der Berücksichtigung von Zinsen und Steuern insbesondere die durch den tabellenorientierten Aufbau die notwendige Transparenz und Ausbaufähigkeit einer Kommunikation zwischen den beteiligten Akteuren unterschiedlicher Domänen bei der Risikoanalyse und -bewertung entgegen kommt. Damit ist eine Abbildung unterschiedlicher relevanter Spezifika der einzelnen Alternativen ohne großen Aufwand möglich. In Abbildung 2 ist hierzu das Grundschemata eines vollständigen Finanzplanes mit Steuern dargestellt.

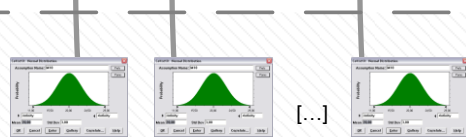
Berechnung des Endwertes einer Investitionsalternative

Vollständiger Finanzplan

VOFI der Investition				
Zeitpunkt	t=0	t=1	...	t=n
Zahlungsfolge				
<b>Eigenkapital</b>				
<b>Kredit</b>				
+ Aufnahme				
- Tilgung				
- Solzzinsen				
<b>Standardanleihe</b>				
- Anlage				
+ Auflösung				
+ Habenzinsen				
<b>Steuerzahlungen</b>				
- Auszahlungen				
+ Erstattung				
<b>Finanzierungssaldo</b>				
<b>Bestandsgrößen</b>				
Kontokorrentkredit				
Guthabensaldo				
<b>Bestandsaldo</b>				

Nebenrechnungen, z.B. Steuern

Abschreibungen			
Zeitpunkt	t=1	...	t=n
Buchwert Jahresbeginn			
Abschreibungen			
Buchwert Jahresende			
Berechnung der Steuerzahlungen			
Zeitpunkt	t=1	...	t=n
Einzahlungsüberschuss			
- Zinsaufwand			
+ Zinsertrag			
- Abschreibungen			
<b>Steuerbemessungsgrundlage</b>			
Erstattung			
Auszahlung			



Verteilungsannahmen

Erweiterung um stochastische Inputgrößen

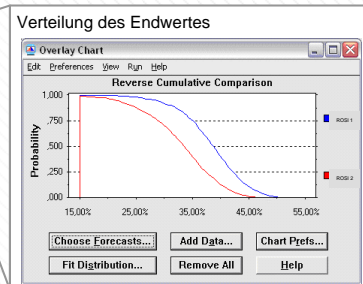


Abbildung 2: VOFI einer Alternative mit Nebenrechnung und Erweiterung durch stochastische Größen (Risiko-Chancen-Analyse)

Ausgangspunkt eines VOFIs ist die Zahlungsfolge der Investitionsalternative. Davon ausgehend können unterschiedliche Kredit- und Anlagekonditionen mit unterschiedlichen Zinssätzen, Laufzeiten und Tilgungsformen bei der Berechnung eines periodenindividuell ausgeglichenen Finanzierungssaldos berücksichtigt werden. In Nebenrechnungen können der Ausgestaltung der Gesellschaftsform entsprechend z.B.

unterschiedliche Aufschüttungs- und Steuermodelle berücksichtigt werden. Damit ist auch eine Abbildung z.B. der Konsequenzen von Outsourcingentscheidungen möglich. Für jede Periode werden im unteren Teil für die unterschiedlichen Anlage- und Finanzierungsformen die aktuellen Bestände erfasst und in einem Saldo konsolidiert. Damit ist es auch möglich, unterschiedliche Eigenkapitalunterlegungen oder Entnahmekonzepte abzubilden, denen im Kontext des Risikomanagements eine besondere Bedeutung zukommt [FKW07].

Der Bestandssaldo am Ende der letzten Periode stellt den Endwert der Investition dar, der bei Annahme der restriktiven Prämissen der klassischen Methoden mit diesen übereinstimmt [Gr89]. Diesem ist der Endwert der VOFIs aller anderen Investitionsalternativen gegenüber zu stellen. Wenn nur eine Investitionsalternative vorliegt, ist der Endwert des VOFIs der Investition (With-Fall) mit dem Endwert des VOFIs für den Fall des Beibehaltens des Status Quo (Without-Fall) zu vergleichen. Dafür wird ein VOFI aufgestellt, in der durch keine Maßnahmen beeinflusste Erwartungsschaden und die alternative Verwendung des Eigenkapitals über die Verzinsung zum Opportunitätskostensatz dargestellt werden. Der zusätzliche Endwert der Investition ergibt sich als Differenz zwischen dem Endwert der Investition und dem Endwert der Opportunität (der „zweit-besten“ Lösung) [Gr89]. Bei einem positiven zusätzlichen Endwert ist es sinnvoll, die Investition durchzuführen. Ein Anwendungsbeispiel im Kontext von IS-Sicherheitsinvestitionen findet sich bei vom Brocke et al. [vB07b].

Vollständige Finanzpläne können mit herkömmlicher Tabellenkalkulationssoftware umgesetzt werden und sind damit auch Akteuren mit nicht-ökonomischer Ausbildung durch die Explikation aller originären und derivativen Zahlungen transparent. Dadurch können auch die Zahlungsfolgen hinsichtlich ihrer Zusammensetzung leicht von heterogenen Anwenderkreisen in herkömmlichen Office-Lösungen programmiert werden. Dadurch sind Anpassungen leicht realisierbar, z. B. ist es möglich, mittels einer handelsüblichen Erweiterung über Monte Carlo-Simulationen die in diesem Kontext besonders relevanten stochastischen Größen abzubilden und ein Risiko-Chancen-Profil der Investition zu berechnen [He64]. Damit ist einer Risikobetrachtung inhärente Unsicherheit einfach und umfassend abzubilden. Wie in Abbildung 2 dargestellt, wird dazu die Zahlungsfolge mit Verteilungsannahmen unterlegt. Dies kann direkt oder über Nebenrechnungen erfolgen oder aus den Ergebnissen eingangs getätigter Prozesssimulationen. Über die Simulation können so Verteilungen des Endwertes ermittelt werden, mit denen sich über die verschiedenen Alternativen Risiko-Chancen-Profile ermitteln lassen, die eine Steuerung der Disposition der operativen Risiken im Bereich der Informationssysteme entsprechend der gewünschten Risikodisposition für das Unternehmen erlauben.

## **Zusammenfassung und Ausblick**

In dem vorliegenden Beitrag wurde eine Methode zur Entscheidungsunterstützung für IS-Sicherheitsinvestitionen eingeführt. Die Forschungsarbeiten orientieren sich hierbei an einem konstruktiven Forschungsdesign, wobei eine konzeptionell-deduktive Analyse





