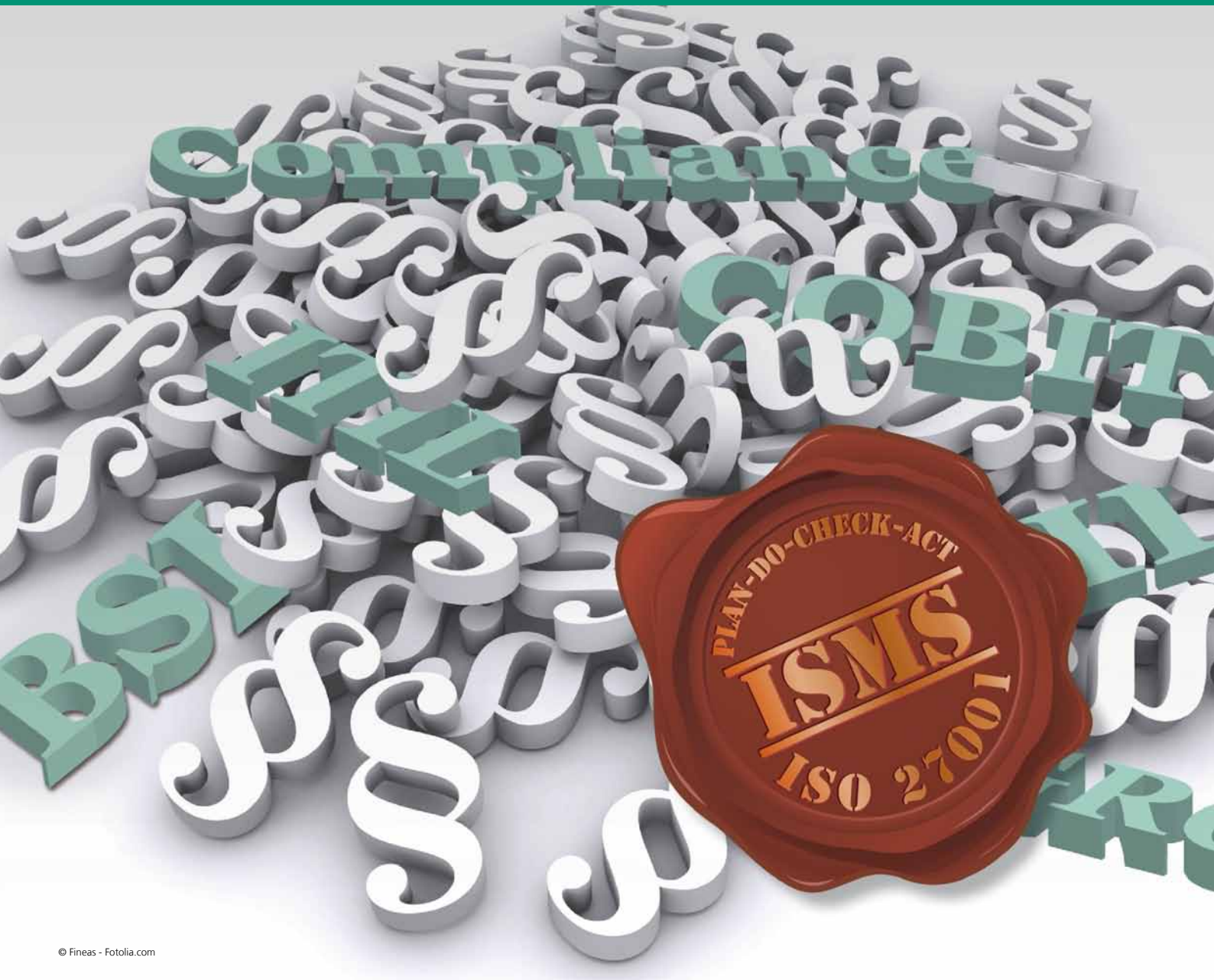
Fraunhofer
AISEC

FRAUNHOFER RESEARCH INSTITUTION AISEC

MANAGEMENTSYSTEME FÜR INFORMATIONSSICHERHEIT:
Marktübersicht. Vorgehensmodell. Handlungsempfehlungen.

IRYNA WINDHORST UND BENEDIKT PIRZER

09/2012



Executive Summary

Die Gewährleistung eines sicheren und zuverlässigen IT-Betriebs im Rahmen des Risikomanagements wird in vielen Branchen durch zahlreiche Vorschriften und Gesetze, wie z.B. dem Gesetz zur Kontrolle und Transparenz im Unternehmensbereich (KonTraG) [1, 2, 21] oder Sarbanes-Oxley Act (SOX) gefordert. Gerade in größeren Organisationen können unkoordinierte Einzelmaßnahmen einen ausreichend sicheren IT-Betrieb nicht gewährleisten und sind nicht geeignet, die eigenen Bemühungen um einen sicheren IT-Betrieb gegenüber Kunden oder dem Gesetzgeber nachzuweisen. Ein strukturiertes Vorgehen mit definierten Prozessen und die Dokumentation dieses Vorgehens ist daher erforderlich. Standardisierte Verfahren erleichtern eine solche Herangehensweise und ermöglichen die Bemühungen unterschiedlicher Organisationen zu vergleichen und zu bewerten.

Im deutschsprachigen Raum sind mit der Norm ISO/IEC 27001 und dem Grundschutz des Bundesamts für Sicherheit in der Informationstechnik (BSI) zwei Standards weit verbreitet, die den Aufbau eines Managementsystems für Informationssicherheit (ISMS) in Organisationen beschreiben. Der Aufbau und Betrieb eines solchen Managementsystems ist aufwendig und komplex, so dass hier eine Unterstützung durch spezialisierte Softwaresysteme wünschenswert ist.

Das vorliegende Whitepaper gibt einen Überblick über geeignete Softwaresysteme und klassifiziert die am Markt verfügbaren Lösungen. Neben Spezialsoftware zur Unterstützung des Betriebs eines ISMS auf Basis einer Norm sind Multinormensysteme verfügbar, die teilweise auch gängige Standards, die über den Fokus der IT-Sicherheit hinausgehen, wie z.B. ITIL oder COBIT, unterstützen. Der Betrieb eines ISMS kann auch im Rahmen einer IT-fokussierten oder unternehmensweit ausgerichteten Governance, Risk Management and Compliance (GRC) Strategie verstanden werden, so dass auch integrierte GRC-Softwaresysteme Unterstützung beim Betrieb eines ISMS bieten können.

Das Ergebnis der Studie zeigt, dass viele Unternehmen bisher noch keine Softwareunterstützung für Informationssicherheitsmanagement (ISM) nutzen [38, 19]. Da jedes System seine Existenzberechtigung hat, müssen interessierte Unternehmen aus einer Vielzahl von ISMS-Softwaresystemen das für ihren individuellen Anwendungsfall geeignete auswählen. Die Studie bietet ein Best Practice Vorgehensmodell und Handlungsempfehlungen bei der Auswahl und Einführung eines ISMS-Softwaresystems und somit erleichtet den Einstieg in den ISMS/GRC-Themenkomplex.

Inhaltsverzeichnis

Abkürzungsverzeichnis

BCM	Business Continuity Management
BDSG	Bundesdatenschutzgesetz
BIA	Business Impact Analysis
BITKOM	Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e.V.
BS	British Standard
BSI	Bundesamt für Sicherheit in der Informationstechnik
COBIT	Control Objectives for Information and Related Technology
DIN	Deutsches Institut für Normung
eGRC	Enterprise Governance Risk and Compliance
EN	Europäische Norm
GmbH	Gesellschaft mit beschränkter Haftung
GRC	Governance Risk and Compliance
GRC IS	Governance Risk and Compliance Information System
IEC	International Electrotechnical Commission
ISACA	Information Systems Audit and Control Association
ISM	Information Security Management
ISMS	Information Security Management System
ISO	International Organization for Standardization
ITGI	IT Governance Institute
ITIL	Information Technology Infrastructure Library
ITSM	Information Technology Service Management
KonTraG	Gesetz zur Kontrolle und Transparenz im Unternehmensbereich
NIA	Normenausschuss Informationstechnik und Anwendungen
NIST	National Institute of Standards and Technology
PDCA	Plan-Do-Check-Act
SaaS	Software-as-a-Service
UG	Unternehmergesellschaft (haftungsbeschränkt)

1 Einleitung

Die eigene IT-Infrastruktur ist heutzutage für fast alle Organisationen und Unternehmen, auch außerhalb des IT-Bereichs, von zentraler Bedeutung. Nahezu alle Geschäftsprozesse in Organisationen werden mit Informationstechnologien unterstützt. Dazu zählen sowohl die Kernprozesse, wie z.B. Fertigung, Einkauf oder Distribution, als auch unterstützende Prozesse, wie z.B. die Arbeitszeitverwaltung oder Lohnabrechnung. Auch werden in fast jeder Organisation vertrauliche Informationen, wie z.B. Mitarbeiterdaten oder geheime Konstruktionspläne, mit Hilfe von IT-Systemen verwaltet. Die Gewährleistung eines sicheren und zuverlässigen IT-Betriebs wird darüber hinaus durch zahlreiche Vorschriften und Gesetze gefordert. In vielen Branchen besteht, auch aufgrund großer Vernetzung mit Zulieferern oder Partnern, der Wunsch nach einem einheitlichen Sicherheitsniveau.

Aktuelle Bedrohungen, komplexe Spionageprogramme und Datendiebstähle, wie z.B. bei Sony, Yahoo, Visa, Deutschen Telekom, SchülerVZ oder Hotmail haben gezeigt, dass IT-Risiken zum Unternehmensrisiko geworden sind. Um den ungewollten Abfluss geschäftskritischer Informationen zu verhindern, werden nicht nur konkrete technische Maßnahmen benötigt, sondern es ist notwendig, ein Gesamtpaket an technischen, organisatorischen, physischen, prozessualen und personellen Maßnahmen zu betrachten und diese konsequent und ganzheitlich durchzuführen. Um die zahlreichen Aspekte eines solchen ganzheitlichen Schutzes der geschäftsrelevanten Informationen zu berücksichtigen und die Aktivitäten zur Wahrung der Informationssicherheit einer Organisation effizient und effektiv zu managen, bietet sich die Unterstützung durch ein Softwaresystem für das Management der Informationssicherheit (ISMS-Softwaresystem) an.

Die vorliegende Studie bietet einen Überblick bei der Vielzahl von Softwaresystemen für die Unterstützung von ISMS durch die Klassifizierung und Marktübersicht, unterstützt die Unternehmen bei der Auswahl und Einführung eines geeigneten Werkzeugs für Informationssicherheitsmanagement (ISM) durch ein Best Practice Vorgehensmodell und bietet Handlungsempfehlungen an.

2 Definition grundlegender Begriffe, Abgrenzung und Untersuchungsgegenstand

2.1 Definition und Abgrenzung grundlegender Begriffe

Informationssicherheitsmanagementsysteme

In Anlehnung an den ISO Standard 27001 [17] sowie den BSI Standard 100-1 [7] und erweitert um Aspekte nach Müller [44] lässt sich ein Informationssicherheitsmanagementsystem (ISMS) als Summe der Prozesse, Verantwortlichkeiten, Verfahren, Methodiken sowie der Ressourcen, Hilfsmittel und einer geeigneten Aufbauorganisation charakterisieren, um der Leitungsebene zu ermöglichen, alle auf Informationssicherheit ausgerichteten Aktivitäten und Aufgaben nachvollziehbar zu lenken und zu dokumentieren.

Dabei gelten auch für Managementsysteme für Informationssicherheit die grundlegenden Definitionen nach DIN EN ISO 9000 [47, S. 3-5]. Der Begriff des Managements umfasst alle aufeinander abgestimmten Tätigkeiten zum Leiten und Lenken von Organisationen. Von zentraler Bedeutung ist auch die Fähigkeit eines Managementsystems sich kontinuierlich zu verbessern oder auf Änderungen der Rahmenbedingungen zu reagieren.

Das beschriebene Konzept eines Informationssicherheitsmanagementsystems ist grundsätzlich unabhängig von konkreten Standards und der Implementierung dieser Standards. Einige zentrale Standards werden im folgenden Kapitel 3 vorgestellt.

Governance, Risk Management und Compliance

Der Begriff Governance, Risk Management und Compliance (GRC) fasst drei wichtige Handlungsebenen der Unternehmensführung zusammen. Obwohl Governance, Risk Management und Compliance die Hauptebenen von GRC sind, lässt sich ein ganzheitliches GRC nicht strikt auf eine Kombination dieser drei Teilaspekte beschränken. In der Praxis werden im IT-Bereich beispielsweise auch das Herstellermanagement (Vendormanagement) und das Servicemanagement als Teil von GRC betrachtet. Obwohl es keine einheitliche wissenschaftliche Definition von GRC gibt, fasst [53] drei zentrale Beobachtungen zusammen:

- GRC ist ein integriertes und ganzheitliches Managementkonzept.

- Technologie ist ein Schlüsselaspekt von GRC, aber ein integriertes GRC Konzept geht über ein rein technisches System hinaus.
- Ein integriertes GRC soll die Effizienz von Prozessen verbessern.

GRC-Softwaresysteme

Grundsätzlich erfordern die mit den GRC-Handlungsebenen verbundenen Prozesse keine Softwareunterstützung. In der Praxis stellt sich die Realisierung einer integrierten GRC-Strategie und die Umsetzung der dazu notwendigen Prozesse als sehr komplex und aufwendig dar. Daher besteht auch in diesem Bereich das Potenzial, GRC-Prozesse mit Hilfe von Softwaresystemen zu unterstützen. Neben vielen Produkten, die Teilaspekte von GRC, wie z.B. das Risikomanagement durch IT-Systeme, unterstützen wollen, gibt es den Bereich der integrierten GRC-Softwaresysteme, die alle drei Handlungsebenen von GRC in einem Produkt vereinen und um weitere relevante Funktionen erweitern. Im Gegensatz zum Bereich der ISMS-Softwaresysteme ist eine Unterscheidung zwischen papierbasierten GRC-Systemen und GRC-Softwaresystemen nicht notwendig. Im Folgenden bezieht sich die Nutzung des Begriffs GRC-System stets auf Softwaresysteme. Im letzten Quartal 2011 haben sowohl Forrester [41] als auch Gartner [50] Studien zu GRC-Systemen veröffentlicht und kommen überwiegend zu den gleichen Beobachtungen.

Bei den verfügbaren Softwareprodukten in diesem Bereich sind grundsätzlich mehrere Besonderheiten festzustellen. Auf der einen Seite ist der Markt der GRC-Softwaresysteme sehr dynamisch und entwickelt sich schnell weiter. Auf der anderen Seite ist keine klare, herstellerübergreifende Entwicklungstendenz erkennbar. Manche Anbieter versuchen GRC-Systeme als Standardsoftware mit eingeschränkter Anpassungsfähigkeit anzubieten. Andere Hersteller verkaufen vor allem auch ein umfangreiches Beratungsangebot und bieten mit ihrem GRC-System eine Plattform für die Zusammenstellung einer individuellen Lösung.

Die angebotenen Systeme unterscheiden sich auch in Hinblick auf die Ausrichtung der GRC-Bestrebungen auf einzelne Unternehmensbereiche. Historisch gewachsen sind zwei unterschiedliche Ansätze zu finden. Manche GRC-Systeme richten sich speziell auf GRC im IT-Bereich des Unternehmens aus. Diese Systeme werden oft als IT-GRC-Systeme bezeichnet. Andere GRC-Systeme fokussieren sich auf die GRC-Bestrebungen des Unternehmens ohne besondere Berücksichtigung des IT-Bereichs. Diese Systeme werden in Veröffentlichungen und durch die Anbieter unterschiedlich bezeichnet. Gebräuchliche Begriffe sind hier die Bezeichnungen Enterprise GRC-System (eGRC) oder verallgemeinert GRC-Informationssystem (GRC IS).

Neben dem zentralen Treiber im eGRC-Bereich, der Finanzverwaltung eines Unternehmens, sind hier aber auch andere Bereiche denkbar, wie z.B. der Bereich Umweltschutz, Arbeitssicherheit oder Themen nahe an der zentralen unternehmerischen Tätigkeit, wie der Produktion oder des Handels. Obwohl es hier vor

allem im Bereich des Risikomanagements und der Compliance zahlreiche branchenspezifische Produkte gibt, sind neben dem Legal GRC [54] im juristischen Bereich keine weiteren als GRC-Softwaresysteme beworbenen Systeme mit spezieller Ausrichtung auf einzelne Teilgebiete analog des IT-Bereichs bekannt. Im Markt haben eGRC-Systeme einige Jahre Vorsprung vor den IT-GRC-Systemen [25]. Der Bereich der Legal GRC-Systeme steht erst am Anfang der Entwicklung.

GRC und ISMS

Die Anknüpfungspunkte zwischen GRC und ISMS sind vielfältig. Auf der einen Seite ist das im Rahmen eines ISMS geforderte Risikomanagement von Sicherheitsrisiken ein Teil des IT-Risikomanagements. Auf der anderen Seite sind die im Rahmen eines ISMS formulierten Richtlinien auch als Regeln im Sinne der Governance anzusehen. Für viele Unternehmen sind Maßnahmen im Bereich der IT-Sicherheit, z.B. durch die Einführung eines ISMS, gesetzlich vorgeschrieben. Hier könnte das ISMS als Maßnahme aus dem GRC Themenbereich Compliance verstanden werden.

In den auf dem Markt verfügbaren IT-GRC-Systemen sind zumeist alle wesentlichen Funktionen, vor allem im Bereich des Asset-, Konfigurations- und Schwachstellenmanagements, für den Betrieb eines ISMS enthalten oder lassen sich über den Zukauf von Modulen nachrüsten. Eine Abwicklung des ISMS im Rahmen eines vorhandenen GRC-Systems kann demnach zahlreiche Synergieeffekte bieten. Neben dem geringeren Aufwand für die Integration sind in solchen Fällen sowohl die Lösung im Unternehmen bereits bekannt als auch schon Zugänge sowie Schnittstellen oder Prozesse für die Datenlieferung vorhanden.

Komplizierter ist die Situation, wenn kein IT-GRC-System vorhanden ist. Eine Einrichtung eines GRC-Systems im Rahmen der Einführung eines ISMS ist zwar grundsätzlich möglich, allerdings in der Praxis schwierig umzusetzen. Unterschiedliche Zuständigkeiten und Finanzierungsmöglichkeiten können hier die Einführung der ISMS-Funktionalitäten behindern. Dieses Problem wird verstärkt, wenn nicht nur ein IT-GRC-System, sondern ein eGRC-System im Rahmen der ISMS-Einführung eingesetzt werden soll, da hier auch noch weitere Beteiligte außerhalb der IT-Abteilung einbezogen werden müssen. Grundsätzlich sind hier im Sinne von integriertem GRC jedoch unternehmensweit genutzte Systeme wünschenswert, um mittelfristig sowohl Einsparungen bei der Datenerfassung als auch Qualitätsverbesserungen bei der Datenverfügbarkeit zu realisieren.

2.2 Untersuchungsgegenstand

Die vorliegende Studie enhält einen Marktüberblick über die in Deutschland aktiven Anbieter von Management-Werkzeugen für die Informationssicherheit und es wird ein Vorgehensmodell für Auswahl und Einführung eines Softwaresystems für die Unterstützung von Aufbau und Betrieb eines Managementsystems für

Informationssicherheit (ISMS) vorgeschlagen. Des Weiteren werden Handlungsempfehlungen für ISMS-Interessenten und Betreiber aufgezeigt.

Die Studie wurde im Zeitraum von Dezember 2011 bis Mai 2012 durchgeführt. Ziel der Studie war es die Effektivität und Effizienz der am Markt verfügbaren Softwaresysteme zur Unterstützung des Managements der Informationssicherheit zu beurteilen, einen umfassenden Überblick über den ISMS-Markt zu verschaffen sowie Organisationen bei der Auswahl und Einführung von ISMS mit einem Vorgehensmodell zu unterstützen. Dabei wurden auch Softwaresysteme berücksichtigt, deren Funktionsumfang über das Management von Informationssicherheit hinausgeht.

Die Studie basiert auf eigenen Recherchen, auf der von ISMS-Anbieter für diese Untersuchung bereitgestellten Informationen, weiterführenden Interviews mit verantwortlichen Entscheidungsträgern sowie auf einem Test ausgewählter Systeme anhand eines an die Realität angelehnten Beispiels. Die Studie wurde im Rahmen eines Projekts mit Datev eG, dem führenden IT-Dienstleister für Steuerberater, Wirtschaftsprüfer und Rechtsanwälte, durchgeführt.

Die Studie ist wie folgt strukturiert: In einem ersten Schritt werden relevante Normen und gesetzliche Rahmenbedingungen, die als Einflussfaktor auf Managementsysteme für Informationssicherheit wirken, dargestellt. Darauf aufbauend werden solche Managementsysteme in den Kontext gängiger Standards und verwandter Managementprozesse eingebettet, in vier Klassen eingeteilt und ein Marktüberblick der in Deutschland verfügbaren Systeme gegeben. Im nächsten Schritt wird ein Vorgehensmodell zur effektiven Auswahl und Einführung eines solchen Softwaresystems dargestellt. Die Handlungsempfehlungen für den Betreiber eines Informationssicherheitsmanagementsystems runden diese Studie ab.

3 Relevante Normen und Standards

3.1 ISO/IEC 27001 und verbundene Normen

Die wichtigsten Normen für Managementsysteme für Informationssicherheit sind die in der Normenfamilie 27000 zusammengefassten Normen der International Standards Organization [30]. Unter einer einheitlichen Nummerierung, beginnend mit 27, werden die für ISMS relevante Normen zusammengefasst und neue Normen erarbeitet. Von deutscher Seite wird an diesen Normen durch das Deutsche Institut für Normung e.V. (DIN) mit seiner Arbeitsgruppe Normenausschuss Informationstechnik und Anwendungen (NIA) [16] mitgearbeitet. Ein Teil dieser Normen wurde bereits als deutsche DIN Normen übernommen. Die ISO 27000 Normenfamilie geht ursprünglich auf die beiden britischen Normen BS 7799-1 und BS 7799-2, die wesentlich von Prof. Edward Humphreys [11, 31] geprägt wurden, zurück.

Zentraler Standard dieser Normenfamilie ist der ISO/IEC 27001 Standard [17] [2, S. 17-20] [44, S. 28-31] [33, 34, 35]. Er ist 2005 aus dem zweiten Teil des britischen Standards BS 7799-2 hervorgegangen. Der Standard definiert Anforderungen an ein Informationssicherheitsmanagementsystem und stellt einen prozessorientierten Ansatz vor. Dabei ist das Dokument sehr generisch gehalten und kann in allen Organisationen unabhängig von Größe oder Typ der Organisation angewendet werden. Während der Inhalt auf der technischen Ebene nicht detailliert wird, sind die Anforderungen an die Prozesse ausführlich definiert. Damit bildet ISO/IEC 27001 die Basis der Normenfamilie und definiert Rahmenbedingungen und ein Szenario, die alle anderen Normen der Familie mit weiterem Inhalt und Konkretisierungen füllen. Wie bereits BS 7799-2 bildet er zusätzlich die Basis für Zertifizierungen nach den Kriterien der ISO/IEC 27000 Normenfamilie.

Der auf dem Plan-Do-Check-Act (PDCA) Modell nach Deming [15] basierte prozessorientierte Ansatz implementiert einen kontinuierlichen Verbesserungsprozess [28] und führt damit zu einer lernenden Organisation. Das gleiche Modell wird auch in weiteren ISO und IEC Standards, wie z.B. dem ISO 9001[1] und dem ISO 14001[2] Standard, sowie in ISO/IEC 20000-1[3] genutzt. Der ISO/IEC 27001 Standard ist speziell optimiert worden, um Verträglichkeit mit den genannten Standards und damit die Möglichkeit zur konsistenten und gleichzeitigen Umsetzung und ggf. Integration zu ermöglichen.

[1] Der Standard ISO 9001 ist ein Standard für Qualitätsmanagementsysteme [47, S. 7-18].
[2] Der ISO 14001 ist Standard für Umweltmanagement [47, S. 18-122].
[3] Der ISO/IEC 20000-1 Standard beschäftigt sich mit dem IT Service Management [43].

3.2 BSI Grundschutz

Der Standard 100-2 (früher Grundschutzhandbuch) [8] [29, S. 2-17] des Bundesamtes für Sicherheit in der Informationstechnik (BSI) ist ein weiterer Standard, der sich mit der Gewährleistung von Informationssicherheit beschäftigt. Er richtet sich primär an Sicherheitsverantwortliche, -beauftragte, -experten und -berater. Zusammen mit den IT-Grundschutzkatalogen des BSI bietet der Standard 100-2 eine Vorgehensweise für das Erreichen eines normalen Schutzniveaus. Dabei werden neben potenzieller Schadenshöhe und Eintrittswahrscheinlichkeiten auch die Kosten der Umsetzung von Maßnahmen berücksichtigt. Bei der Verwendung der IT-Grundschutzkataloge kann eine aufwändige Sicherheitsanalyse, die Expertenwissen erfordert, entfallen und mit pauschalisierten Gefährdungen gearbeitet werden. Eines der wichtigsten Ziele des IT-Grundschutzes ist es, den Aufwand im Informationssicherheitsprozess zu reduzieren, indem bekannte Vorgehensweisen zur Verbesserung der Informationssicherheit gesammelt und zur Wiederverwendung angeboten werden.

Dazu wird der Schutzbedarf der Werte basierend auf den einzelnen Schutzzielen Verfügbarkeit, Vertraulichkeit und Integrität bestimmt und in drei Klassen „niedrig bis mittel", „hoch" und „sehr hoch" eingeteilt. Die in den Grundschutzkatalogen vorgegebenen Maßnahmen sind nur für niedrigen bis mittleren Schutzbedarf ausreichend. Bei hohem oder sehr hohem Schutzbedarf sind weitere Maßnahmen erforderlich. Dabei wird angenommen, dass der vorgegebene Maßnahmenpool ausreichend ist. Diese Feststellung kann nur eingeschränkt dem komplexen Problem eines sinnvollen Risikomanagements [36, S. 101-102] gerecht werden. Außerdem entspricht diese Vorgehensweise den Anforderungen an einen kontinuierlichen Verbesserungsprozess und dem PDCA-Zyklus nicht vollständig, da die Bausteine als „abgeschlossen" betrachtet werden und nur durch das BSI weiter verbessert werden.

Zusätzlich werden im BSI Standard 100-1 [7] Anforderungen an ISMS festgelegt. Der Standard ist dabei vollständig kompatibel mit dem ISO/IEC 27001 Standard und enthält auch Aspekte aus ISO/IEC 27002. Er verbindet die ISO/IEC 27000 Normenfamilie und das Vorgehen nach BSI Grundschutz. In diesem Sinne kann der BSI Standard 100-2 auch als Konkretisierung und Ergänzung des BSI Standards 100-1, analog zum Zusammenspiel der Standards ISO/IEC 27001 und ISO/IEC 27002, angesehen werden. Mit der Richtlinie 100-3 [9] bietet das BSI auch einen Standard für die Risikoanalyse an, der immer dann genutzt werden kann, wenn der grundlegende Schutz, den die Vorgehensweise nach BSI 100-2 für niedrigen und mittleren Schutzbedarf bietet, nicht ausreicht und hoher oder sehr hoher Schutzbedarf vorliegt. Ausgehend von vorhandenen Gefährdungen sollen zusätzliche Gefährdungen und Maßnahmen entwickelt werden. ISO/IEC 27005 geht aber weiter und etabliert ein Risikomanagementsystem für Informationssicherheit [36, S. 44-46]. Ein Teil davon sind insbesondere die Prozessbestandteile Risikokommunikation sowie kontinuierliche Risikoüberwachung und die punktuelle -überprüfung, die im BSI Standard nicht ausführlich vorkommen.

Der BSI Grundschutz beschreibt somit durch die BSI Standards 100-1, 100-2, 100-3 und die IT-Grundschutz-Kataloge eine Vorgehensweise zum Aufbau und zur Aufrechterhaltung eines Managementsystems für Informationssicherheit (ISMS). Das damit aufgebaute ISMS erfüllt die Anforderungen von ISO/IEC 27001 und ISO/IEC 27002. Eine detaillierte Übersicht über die Abbildung der einzelnen Kapitel der ISO/IEC Standards auf Teile des BSI Grundschutzes wurde in [6] veröffentlicht. Das Modul zum Thema Datenschutz aus der Grundschutzvorgehensweise [42] berücksichtigt deutsche Rechtsnormen und kann daher nicht in einer internationalen Norm wie ISO/IEC 27001 bzw. ISO/IEC 27002 abgebildet werden. In der technischen Richtlinie 100-4 [10] beschäftigt sich das BSI mit dem Thema Notfallmanagement vor dem Hintergrund von IT-Grundschutz.

Auch eine Zertifizierung gemäß IT-Grundschutz durch das BSI ist möglich. Die ursprüngliche eigenständige Zertifizierung nach IT-Grundschutz durch das so genannte Grundschutzzertifikat in drei Stufen [29, S. 10-17] wurde durch eine anerkannte ISO 27001-Zertifizierung auf der Basis von IT-Grundschutz vollständig abgelöst. Die Integration von ISO 27001 in die BSI Standards macht diese Zertifizierung auf der Basis von IT-Grundschutz besonders für international tätige Institutionen interessant, da außerhalb des deutschsprachigen Raums eine Zertifizierung nach ISO/IEC 27001 mehr Gewicht hat als eine Zertifizierung nach einem regionalen Standard. Ob ein BSI Zertifikat nach ISO/IEC 27001 von internationalen Geschäftspartnern anerkannt wird, ist nicht zuverlässig gewährleistet. Im Zweifelsfall kann also eine doppelte Zertifizierung notwendig sein.

Da auch BSI Standards die Auswahl eines geeigneten Risikomanagementsystems dem Anwender überlassen, steht es dem Anwender der Grundschutzmethodik frei, sich für oder gegen den BSI Standard 100-3 zu entscheiden. Auch ist es möglich, die Risikoanalyse auf der Basis von IT-Grundschutz als zusätzliche Technik des Risiko-Assessments nach ISO/IEC 27005 zu nutzen oder beide Standards parallel anzuwenden. Die umfangreichen BSI Gefährdungskataloge können gerade im Bereich der Risikoidentifizierung wertvoll sein.

3.3 Weitere Normen und Standards

Neben den bereits vorgestellten Normen und Standards gibt es noch zahlreiche weitere Standards im Umfeld von ISMS, die im Folgenden kurz vorgestellt werden sollen. Dabei lassen sich zwei Gruppen unterscheiden. Zunächst gibt es weitere Standards zum Management von IT-Systemen [26], die sich auch mit Sicherheit und dem Management von Sicherheit beschäftigen. Auf der anderen Seite gibt es noch weitere regionale Standards analog zum Grundschutz, die überwiegend an den ISO/IEC 27001 Standard angepasst sind.

COBIT

Mit den Control Objectives for Information and related Technology (COBIT) [32] wird eine Methode zur Kontrolle von Risiken, die sich durch den Einsatz von Informationstechnologie zur Unterstützung geschäftsrelevanter Abläufe ergeben, definiert. Das Framework wird weiterentwickelt vom IT Governance Institute (ITGI) der Information Systems Audit and Control Association (ISACA). Bei der Entwicklung von COBIT orientierten sich die Autoren an vorhandenen Standards zum Thema Sicherheitsmanagement, wie z.B. ISO/IEC 27002.

Zentrale Basis bei COBIT [2, S. 34-35] [44, S. 65-67] [24, S. 11-14] ist die Verantwortung des Managements eines Unternehmens für die Erreichung der Geschäftsziele, die Kontrolle der verwendeten Ressourcen hinsichtlich Effektivität und Effizienz, die Einhaltung rechtlicher Rahmenbedingungen und die Behandlung der mit der Geschäftstätigkeit und dem Ressourceneinsatz verbundenen Risiken. Daraus und aus gesetzlichen Vorschriften (z.B. zur Haftung) ergibt sich für das Management der Wunsch und die Pflicht zur Kontrolle. Dies gilt auch für den Einsatz von IT-Systemen als Ressource zur Realisierung von Geschäftsprozessen. Das COBIT Framework stellt ein Rahmenwerk dar, das alle Aspekte des Einsatzes von IT-Systemen von der Planung über den Betrieb bis zur Entsorgung berücksichtigt und damit eine ganzheitliche Sicht auf die IT einnimmt. Damit ist COBIT thematisch im Bereich der IT-Governance anzusiedeln.

COBIT bietet Ansätze zur Messung und Steuerung auf Basis eines Reifegradmodells [37, S.78,179-186]. Die einzelnen Prozesse werden mit sechs Stufen von „nicht existent“ bis „optimiert“ beurteilt. Für den Themenbereich ISMS relevant ist vor allem der Prozess „Ensure System Security“ [23, S.25-43], der der Domäne „Deliver and Support“ zugeordnet wird. In insgesamt elf „Control Objectives“ finden sich auch Inhalte des Anhangs A der ISO/IEC 27001 Norm wieder. Informationssicherheit ist im Rahmen von COBIT auch eine Querschnittsaufgabe. Deshalb wird Informationssicherheit zusätzlich in mehreren Prozessen unterschiedlicher Domänen behandelt. Eine Abbildung der Überschneidungen zwischen COBIT und der ISO/IEC 27001 Norm findet sich in [20, S.150-187]. Bei der gemeinsamen Nutzung ergeben sich demnach Synergieeffekte. So kann z.B. eine erfolgreiche Zertifizierung im Rahmen des ISMS als Nachweis für den Reifegrad der Bemühungen der Organisation im Rahmen von COBIT dienen. Ein Vorteil ist dabei der deutlich größere Detaillierungsgrad der Anforderungen nach ISO/IEC 27001 [20, S.187]. Im Gegenzug können auch die Steuerungs- und Messmethoden des COBIT Frameworks im Rahmen des ISMS genutzt werden.

ITIL

Das Akronym ITIL leitete sich ursprünglich aus dem Begriff IT Infrastructure Library [58, 2] [44, S. 61-65] ab und hat sich bis zur aktuellen Version 3 darüber hinaus weiter entwickelt. Es ist ein Best Practice Referenzmodell für das

IT-Servicemanagement (ITSM). ITIL sieht auch Sicherheitsaspekte als unverzichtbare Bestandteile eines ordnungsgemäßen IT-Betriebs an. Der Standard hilft durch zahlreiche Empfehlungen für die Gestaltung von Unternehmensprozessen, sodass die Planung, Erbringung und Optimierung von IT-Dienstleistungen mit Blick auf die unternehmerischen Ziele unterstützt wird. Übergreifendes Ziel ist die Optimierung bzw. Verbesserung sowohl der Qualität von IT-Services als auch der Kosteneffizienz. Als weltweit akzeptierter Defacto-Standard für IT-Servicemanagement konzentriert sich der Standard in der aktuell gültigen Version 3 auf fünf zentrale Themen:

- Servicestrategie,
- Serviceentwurf,
- Serviceüberführung,
- Servicebetrieb und
- kontinuierliche Serviceverbesserung.

Mit der Veröffentlichung von Version 3 wurde weiterhin der strategische Planungsprozess zur Verzahnung des IT-Servicemanagements mit der Unternehmensstrategie optimiert und dadurch die Kompatibilität zum IT-Servicemanagement-Standard ISO/IEC 20000 [18] hergestellt. Das IT-Sicherheitsmanagement wird in ITIL als eigene Disziplin außerhalb des IT-Servicemanagements betrachtet. Die ISO 20000 Norm enthält nur allgemeine Vorgaben für die Einrichtung eines IT-Sicherheitsmanagements. Inhaltlich ergeben sich jedoch vielfältige Überschneidungen mit dem ISO/IEC 27001 Standard. Eine Abbildung überschneidender Anforderungen nach ISO 20000 und ISO/IEC 27001 wird in [20, S.150-187] dargestellt.

Regionale Standards

Neben dem Grundschutz des BSI in Deutschland gibt es auch noch weitere lokale Standards für das Management von Informationssicherheit. Generell ist zu beobachten, dass auch die internationalen Standards der ISO/IEC 27001 und ISO/IEC 27002, wie im Kapitel 3.1 beschrieben, aus solchen regionalen Standards hervorgegangen sind. Dazu gehört auch das Österreichische Informationssicherheitshandbuch [60], das in der Version 2010 auch an die internationalen Normen angepasst wurde. Auch in Australien existiert mit dem Information Security Manual (ISM) (früher ACSI 33) [14] ein lokaler Standard, der ebenfalls mit den international verfügbaren ISO/IEC Normen abgestimmt wurde. Als Ursprungsland der ISO/IEC Standards 27001 und 27002 gibt es in Großbritannien keine eigenständige lokale Abbildung, aus der Normenfamilie BS 7799 [3] ist jedoch der Standard BSI 7799-3 „Guidelines for information security risk management“ in einer 2006 veröffentlichten Version erhalten geblieben.

Das US-amerikanische National Institute of Standards and Technology (NIST) [46, 51] veröffentlicht im Rahmen von so genannten NIST Special Publications zahlreiche Standards für IT-Sicherheit und richtet sich damit im Besonderen an Behörden der Vereinigten Staaten. In der Veröffentlichungsreihe NIST SP 800 sind zahlreiche relevante Standards, wie z.B. NIST Special Publication 800-53 Recommended Security Controls for Federal Information Systems and Organizations [13] verfügbar. Außerdem wird auch auf ISO/IEC Standards verwiesen und es werden einzelne Aspekte aus den ISO/IEC Standards übernommen.

Diese Auflistung zeigt, dass es auf ISO/IEC 27001 basierend oder damit abgestimmt zahlreiche weitere internationale Standards gibt, und dass der Trend zur Abstimmung mit den internationalen Standards nicht nur auf Deutschland beschränkt ist. Ergänzend zu den aufgeführten Standards gibt es in vielen Ländern auch weitere Standards für Einzelaspekte, wie z.B. dem Risikomanagement analog zu BSI 100-3.

4 Marktüberblick Deutschland

Das beschriebene und in der Norm ISO/IEC 27001 definierte Konzept eines ISMS ist zunächst nicht automatisch mit speziellen Softwaresystemen verbunden. Sowohl die Einführung als auch der Betrieb eines ISMS und sogar die Zertifizierung nach ISO/IEC 27001 kann prinzipiell papierbasiert erfolgen. In der Praxis wird die Erzeugung notwendiger Dokumente in jedem Fall unterstützt durch Software erfolgen. Viele Unternehmen setzen dazu aber keine Spezialsoftware, sondern Standardsoftware wie Microsoft Office ein.

In einem ersten Schritt lässt sich die Effizienz der Prozesse für die Einrichtung und vor allem für den Betrieb eines ISMS durch weitere Softwaresysteme ohne speziellen Fokus auf ISMS verbessern. Ein in vielen Organisationen vorhandenes Dokumentenmanagementsystem kann z.B. die Verwaltung der im Rahmen des ISMS entstehenden Dokumente vereinfachen.

Auch für die zahlreichen Einzelmaßnahmen, die notwendig sind, um Konformität mit dem ISO/IEC Standard 27001 zu erreichen, ist in vielen Organisationen Softwareunterstützung vorhanden bzw. auf dem freien Markt verfügbar. Als Beispiel können hier spezielle Softwaresysteme, wie z.B. für das Risikomanagement oder integrierte Systeme für das Servicemanagement, dienen, die einzelne Teilaspekte eines ISMS abdecken.

Als weiterer Schritt kann auch die Nutzung von Spezialsoftware für die Einführung und den Betrieb eines ISMS sinnvoll sein. Solche Softwaresysteme ergänzen bzw. übernehmen Teile der bereits beschriebenen Funktionen und integrieren zusätzlich das Konzept eines ISMS und die relevanten Normen. Damit bieten diese Softwaresysteme umfangreichen zusätzlichen Nutzen:

- Durch eine Tool-gestützte Überwachung werden Abweichungen von den Vorgabe der genutzten Standards schneller sichtbar und deren Behebung durch das Softwaresystem aktiv überwacht.
- Die in den Softwaresystemen abgebildete Best Practive reduziert das Risiko das Abweichungen auftreten zusätzlich.
- Eine Aufbereitung der Inhalte der relevanten Normen und Standards in einer graphischen Benutzeroberfläche verringert die auf der Benutzerseite notwendige Erfahrung mit diesen Normen und erleichtert den Einstieg in die Einrichtung und den Betrieb eines ISMS.
- Inhaltliche Überschneidungen mit anderen Standards, wie z.B. COBIT oder ITIL werden durch die Anbieter abgebildet. Dadurch wird der Aufwand für

die Datenerhebung reduziert und gleichzeitig steigt die Verfügbarkeit und Qualität der vorhandenen Daten.

Die angebotenen Systeme können auch in Hinblick auf die Integrationstiefe in die unternehmensinterne System- und Prozesslandschaft betrachtet werden. Abbildung 1 gibt eine Übersicht über mögliche Ansätze und den jeweils zu erwartenden Aufwand und Nutzen.

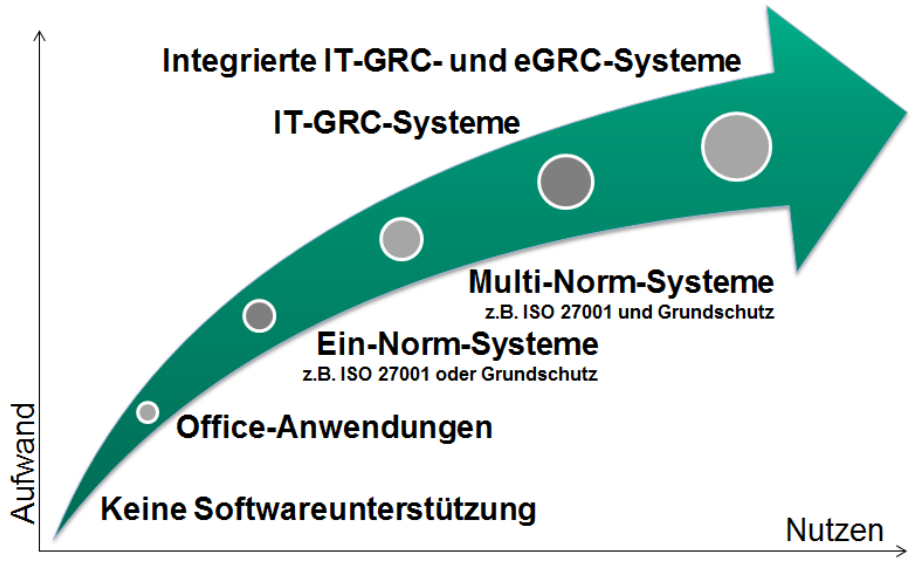


Abbildung 1:
Integrationstiefe von Softwaresystemen zur Unterstützung beim Betrieb eines ISMS

Unter Berücksichtigung der Beobachtung, dass alle für den Betrieb eines ISMS notwendigen Funktionen auch in gängigen IT-GRC-Systemen enthalten sind und der besonderen Situation des Betriebs eines ISMS auf Basis des BSI Grundschutzes, lassen sich die auf dem Markt verfügbaren und für den deutschsprachigen Raum relevanten Systeme aus Nutzersicht grob in die folgenden vier Klassen zusammenfassen:

1. ISMS Softwaresysteme nach ISO/IEC 27001,
2. Grundschutztools,
3. IT-GRC-Systeme und
4. integrierte IT-GRC- und eGRC-Systeme.

Dabei ist zu beachten, dass eine eindeutige Zuordnung nicht möglich ist und daher einzelne Systeme auch in mehren Klassen enthalten sein können. Innerhalb der einzelnen Klassen sind grundsätzlich Systeme mit unterschiedlicher Integrationstiefe vorzufinden. Allerdings ist festzustellen, dass vor allem die GRC-Systeme, um einen hohen Automatisierungsgrad zu erreichen, stark in die unternehmensinterne System- und Prozesslandschaft eingebunden werden müssen.

Für die in den nächsten Kapitel folgenden Marktüberblicke wurden Veröffentlichungen in Fachzeitschriften, Informationen der Standardisierungsorganisationen sowie verfügbare Marktübersichten von Beratungsunternehmen Anfang 2012 ausgewertet, aggregiert und unter Berücksichtigung eigener Auswertungen von den Herstellerinformationen konsolidiert [19, 5, 50, 41, 40].

4.1 ISMS Softwaresysteme nach ISO/IEC 27001

Auf dem Markt sind zahlreiche Softwaresysteme für den deutschsprachigen Raum verfügbar, die bei der Einführung und dem Betrieb eines ISMS auf Basis der Norm ISO/IEC 27001 unterstützen. Einen Überblick über wesentliche Marktteilnehmer bietet Tabelle 1. Diese Softwaresysteme werden durch zahlreiche kleinere Anwendungen und Office-Vorlagen ergänzt, die Teilaspekte eines ISMS nach ISO/IEC 27001 abdecken. Die angebotenen Produkte und auch die Anbieter unterscheiden sich stark. So bietet die Secopan UG als sehr kleines Unternehmen mit ihrem Produkt *ChaRMe* eine vollständig quelloffene Lösung und finanziert dieses Angebot vor allem durch ergänzend angebotene Dienstleistungen [55]. Andere Anbieter, wie z.B. die SerNet GmbH, bieten mit ihrem Produkt *Verinice.PRO* [56] eine klassische Standardsoftware an, die prinzipiell von jedem Kunden erworben und genutzt werden kann. Die Swiss Infosec AG stellt ihre *ISMS Toolbox* [57] ausschließlich Kunden Ihres Beratungsangebots oder Mitgliedern eines geschlossenen „ISMS Praxis Forums“ kostenfrei zur Verfügung. Die meisten anderen Anbieter, wie z.B. die WMC GmbH mit ihrem Produkt *QSec* sowie die DHC GmbH mit ihrem Produkt *DHC Vision* sind mit ca. 20 bis 100 Vollzeitbeschäftigten [19] klassische mittelständische Unternehmen und bieten in erster Linie das Produkt und, ggf. in Kooperation mit Partnern, dazu ergänzend beratende Dienstleistungen an. Die *Hiscout GRC Suite* [27] der HiScout GmbH hebt sich von den anderen Angeboten vor allem durch seine hohe Konfigurierbarkeit ab und entspricht damit eher einem generischen Framework für ISMS-Softwaresysteme, das individuell für den Kunden angepasst werden muss.

Der überwiegende Teil der angebotenen ISMS-Softwaresysteme setzt bereits auf eine Weboberfläche als Schnittstelle zum Benutzer, einzelne Produkte wie *Verinice* und die *ISMS Toolbox* sind allerdings nicht webbasiert und unterscheiden sich auch bei den unterstützten Client Betriebssystemen. Dadurch, dass die Software webbasiert ist, können die Anbieter prinzipiell die ISMS-Softwaresysteme auch als Software-as-a-Service (SaaS)-Angebot über das Internet bereitstellen. Da es sich bei den im ISMS-Softwaresystem verwalteten Daten jedoch um unternehmenskritische Daten handeln kann, wird solch eine Softwarebereitstellung zumindest in Deutschland kaum genutzt.

Die Anzahl der aktiv im Einsatz befindlichen Installationen ist bei den meisten Anbietern überschaubar und schwankt von niedrigen zweistelligen bis zum hohen dreistelligen Bereich [19]. Grundsätzlich ist bei der Fortentwicklung der einzelnen Produkte eine hohe Dynamik zu erkennen. Die Weiterentwicklung der Produkte erfolgt dabei, unter anderem oft aufgrund der geringen Kundenzahlen, sehr

Produkt	Hersteller
chaRMe Version 0.7	Secopan UG
CRISAM Explorer	Calpana business consulting GmbH
DHC Vision Information Security Manager 5.0	DHC Dr. Herterich & Consultants GmbH
HiScout GRC Suite 2.0	HiScout GmbH
ISMS Toolbox	Swiss Infosec AG
opus i BSI-Grundschutz	kronsoft e.K.
QSEC 3.0	WMC GmbH
risk2value 4.0	avedos business solutions GmbH
Sicherer IT-Betrieb 9.0	SIZ Informatikzentrum der Sparkassenorganisation GmbH
verinice. 1.5.0	SerNet GmbH
verinice.PRO 1.5.0	SerNet GmbH

Tabelle 1: Marktüberblick gängiger ISMS-Softwaresysteme nach ISO/IEC 27001

nah an den Wünschen und Bedürfnissen der Kunden. Zahlreiche Anbieter, wie z.B. die Hiscout GmbH und die WMC GmbH, entwickeln ihre Produkte vor allem auch in Richtung vollständiger IT-GRC-Systeme und bewerben die Produkte entsprechend, sodass vor allem in Verbindung mit der hohen Flexibilität bei der Anpassung für den einzelnen Kunden eine klare Unterscheidung zwischen ISMS-Softwaresystem und IT-GRC-System schwierig ist.

4.2 Grundschutztools

Die zweite Klasse bilden so genannte Grundschutztools, die bei der Einführung und dem Betrieb eines ISMS auf Basis der Grundschutzmethodik des BSI unterstützen. Eine Übersicht der wichtigsten Softwaresysteme wird in Tabelle 2 dargestellt. Durch die zunehmende Anpassung der Grundschutzmethodik an den Standard ISO/IEC 27001 besteht eine große inhaltliche Verwandtschaft zwischen ISMS-Softwaresystemen nach ISO/IEC 27001 und den Grundschutztools. Es ist daher nicht weiter verwunderlich, dass sich ein erheblicher Teil der Produkte aus Kapitel 4.1 auch in diesem Kapitel wiederfindet. Eine wichtige Referenz ist das *GSTOOL*, das offizielle Grundschutztool des BSI, das jedoch wenig Flexibilität bietet und geradezu historisch anmutet. Mit diesen Schwächen werden Anreize für die Entwicklung alternativer Anwendungen erst geschaffen. Diesen Eindruck bestätigt eine Studie aus 2010 von ibi research [38], in der über 20 Prozent der befragten Nutzer Probleme mit dem Grundschutztool des BSI äußerten. So lassen sich die angebotenen Lösungen in drei Kategorien unterteilen. Neben dem *GSTOOL* des BSI gibt es alternative Grundschutztools und ISMS-Softwaresysteme

nach Kapitel 4.1, die auch die Grundschutzmethodik und die -kataloge beinhalten.

Produkt	Hersteller
DHC Vision Information Security Manager 5.0	DHC Dr. Herterich & Consultants GmbH
DocSetMinder	GRC Partner GmbH
GRC-Suite iRIS	ibi research GmbH
GSTOOL 4.7	BSI
HiScout GRC Suite 2.0	HiScout GmbH
i-doit pro	synetics GmbH
opus i BSI-Grundschutz	kronsoft e.K.
SAVe	INFODAS GmbH
Security Audit	Secure IT Consult
sidoc-Sicherheitsmanagement 9.0	2Net Carsten Lang
verinice. 1.5.0	SerNet GmbH
verinice.PRO 1.5.0	SerNet GmbH

Tabelle 2: Marktüberblick wesentlicher Grundschutztools

Während für die dritte Kategorie die bereits beschriebene hohe Dynamik bei der Weiterentwicklung und eine starke technologische Tendenz zu Webanwendungen zu beobachten ist, sind reine Grundschutztools, wie das *sidoc-Sicherheits management-Tool* [39], deutlich weniger dynamisch in der Fortentwicklung und oft nicht webbasiert. Grundsätzlich ist davon auszugehen, dass reine Grundschutztools ohne ergänzende Funktionen langfristig kaum Entwicklungspotenzial auf dem Markt haben werden, da das BSI mit der Version 5 des Grundschutztools bereits an einer vollständig neu entwickelten und deutlich verbesserten Lösung [22] arbeitet. Langfristig ist, auch aufgrund der inhaltlichen Annäherung des Grundschutzes an die Vorgehensweise nach ISO/IEC 27001, davon auszugehen, dass außerhalb von deutschen Behörden vor allem die sehr detaillierten Kataloge des Grundschutzes bestehen bleiben, die bereits heute in zahlreiche Systeme nach Kapitel 4.1 integriert werden können. Dennoch ist vor allem die breite Nutzerbasis des Grundschutztools des BSI mit ca. 20.000 Lizenzen [22] im Bereich der bisher vorgestellten Systeme einmalig.

4.3 IT-GRC-Systeme

Eine weitere Kategorie von Softwaresystemen, die bei der Einführung und dem Betrieb von ISMS unterstützen können, sind die IT-GRC-Systeme. Ein Überblick über die wichtigsten am Markt verfügbaren Lösungen ist in Tabelle 3 aufgeführt. Im Vergleich zu den bisher behandelten Kategorien fallen vor allem die

Unterschiede bei den Herstellern auf. Bei den wichtigsten Herstellern von IT-GRC-Systemen, wie z.B. *Modulo* [45], handelt es sich zumeist um international aufgestellte Unternehmen mit Niederlassungen auf mehreren Kontinenten und teilweise auch um bekannte Namen aus der IT-Branche, wie Symantec oder Microsoft. Die Produkte basieren überwiegend auf langjähriger Erfahrung der Hersteller in diesem Bereich. Gerade die führenden Anbieter betreuen deutlich mehr Kunden als die Anbieter der bisher besprochenen ISMS-Softwaresysteme. Es gibt jedoch auch kleinere Anbieter, wie die dänische Firma Neupart, die sich mit ihrer IT-GRC-Lösung *SecureAware* [49] vor allem auch an Kunden aus einigen speziellen Sektoren, wie z.B. dem Finanzsektor [48], richten.

Produkt	Hersteller
Brinqa GRC Platform	Brinqa GRC
Compliance and IT Risk Management	Lumension Security, Inc.
ControlCase IT-GRC	ControlCase LLC
Control Compliance Suite 11	Symantec Corporation
Easy2comply	Dynasec Ltd.
HiScout GRC Suite 2.0	HiScout GmbH
IT Compliance Management Series	Microsoft Deutschland GmbH
Modulo Risk Manager	Modulo
QSEC 3.0	WMC GmbH
RiskVision OpenGRC	Agiliance, Inc.
Rsam	Relational Security Corporation
SecureAware	Neupart GmbH
TruComply 4.0	ANXeBusiness Corp.

Tabelle 3: Marktüberblick wesentlicher IT-GRC-Systeme

Technologisch wird bei IT-GRC-Systemen fast ausschließlich auf webbasierte Anwendungen gesetzt. Da der Bereich der ISMS-Funktionen für IT-GRC-Systeme nur einen Teilbereich darstellt, unterscheiden sich die einzelnen IT-GRC-Systeme vor allem auch in Aspekten, die die ISMS-Funktionalitäten nicht betreffen. Große Unterschiede gibt es auch bei der Abbildung verschiedener Standards und der Konnektivität zu weiteren im Unternehmen vorhandenen Systemen. Für deutsche Unternehmen relevante Standards und Vorschriften, wie z.B. das Bundesdatenschutzgesetz (BDSG), sind aufgrund der Internationalität der Kundenkreise meist integriert.

Da es sich bei IT-GRC-Systemen um hoch komplexe Systeme handelt, deren Einführung im Unternehmen auch mit großen Aufwänden verbunden ist, richten sich die Hersteller mit ihren Produkten in erster Linie an große Unternehmen mit entsprechend komplexen Systemlandschaften, die ohne die Unterstützung durch Softwaresysteme nicht mehr effizient zu steuern und zu kontrollieren sind.

4.4 Integrierte IT-GRC- und eGRC-Systeme

Die Unterscheidung von IT-GRC-Systemen und integrierten Enterprise- und IT-GRC-Systemen spiegelt sich nicht automatisch funktional in den IT-GRC-Komponenten wider. Prinzipiell ist eine Integration von eGRC- und IT-GRC-Komponenten in einem System nur die konsequente Fortsetzung des integrativen Ansatzes von GRC-Systemen. Dennoch zeigen Marktanalysen von Forrester [41] und Gartner [50], dass die Hersteller der unterschiedlichen Systeme in der Praxis Probleme haben, die sich unterscheidenden Anforderungen von Enterprise- und IT-GRC in einem System abzubilden und trotzdem die Komplexität beherrschbar zu halten. Aus diesem Grund behandeln sowohl Forrester als auch Gartner in ihren Marktüberblicken eGRC-Systeme [40, 12] und IT-GRC-Systeme getrennt voneinander.

Produkt	Hersteller
GRC Platform	BWise BV
IBM OpenPages GRC Platform 6.0	IBM Corporation
IT GRC Software Solution	MetricStream, Inc.
RSA Archer eGRC Platform 5.1.4.	EMC Corporation

Tabelle 4: Marktüberblick der relevanten integrierten IT-GRC- und eGRC-Systeme

Ungeachtet dessen gibt es bereits mehrere Systeme, die von den Herstellern sowohl für den Einsatz als eGRC-System als auch als IT-GRC-System beworben werden. Einen Überblick über die wichtigsten Marktteilnehmer in tabellarischer Form ist in Tabelle 4 aufgeführt. Besonders bemerkenswert ist hierbei, dass die Angebote von EMC/RSA, BWise BV und Metricstream sowohl bei dem Marktüberblick für eGRC-Systeme als auch für IT-GRC-Systeme sehr gute Plätze erreichen. Diese Ergebnisse zeigen, dass viele integrierte eGRC-Systeme und IT-GRC-Systeme bereits einen hohen Entwicklungsstand erreicht haben.

5 Vorgehensmodell für die Einführung eines ISMS-Softwaresystems

Grundsätzlich wird zwischen der Einführung eines ISMS-Softwaresystems und der Einführung eines ISMS als papierbasiertes System unterschieden. Für die Einführung eines ISMS sind bereits zahlreiche Hinweise in den einschlägigen Normen [17, 8] vorhanden. Des Weiteren kann auch auf das generische Modell zur Einführung von Sicherheitsstandards in Unternehmen nach BITKOM und DIN [2, S.15-6] zurückgegriffen werden.

Die Angabe einer typischen Projektdauer für die Einführung eines solchen ISMS-Softwaresystems ist nicht zuletzt wegen der großen Vielfalt der verfügbaren Lösungen schwierig. Eine Einzelplatzlösung ist deutlich schneller einzuführen, als ein unternehmensweites eGRC-System. Bereits bei mittleren Lösungen wie *QSEC* berichten die Hersteller jedoch von Projektlaufzeiten von 24 Monaten [59] und mehr. Nicht betrachtet wird die Einführung eines ISMS-Softwaresystems als Teil einer bereits im Unternehmen vorhandenen GRC-Lösung, da hier nach der Entscheidung zur Nutzung des vorhandenen Systems vor allem systemspezifisch vorgegangen werden muss.

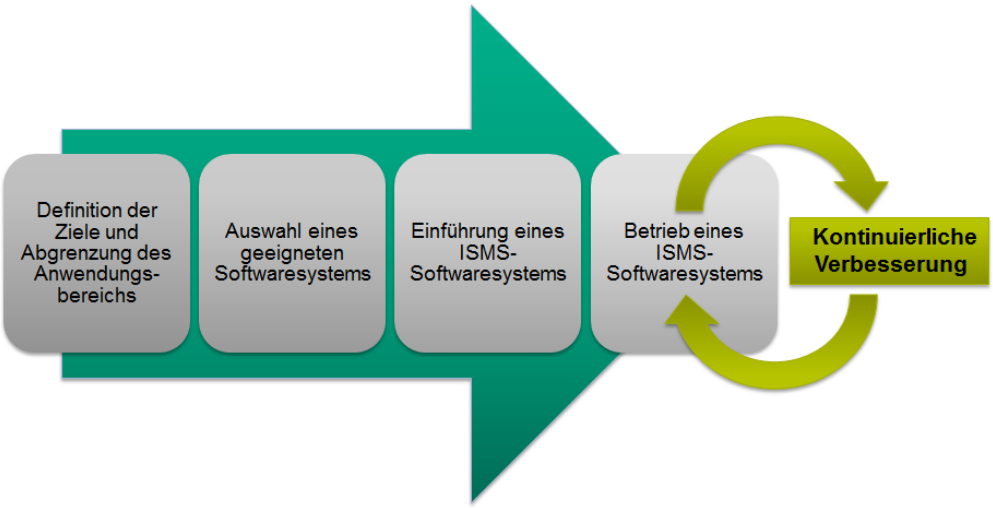


Abbildung 2: Vorgehensmodell für die Einführung eines ISMS-Softwaresystems

Die Einführung des ISMS-Softwaresystems soll in die drei in Abbildung 2 dargestellten Phasen untergliedert werden, an die sich die Phase des Betriebs des Systems anschließt. Es ergibt sich damit grundsätzlich ein Vorgehen analog des von ISO/IEC 27001 und BSI Standard 100-1 genutzten PDCA-Zyklus aus Abbildung 3, sodass eine Einführung mit Hilfe dieses Systems auch mit der erstmaligen Einführung eines ISMS synchronisiert werden kann. Die Abbildung des PDCA-Zyklus

erfolgt dabei vor allem in der letzten Phase, während die ersten drei Phasen nur einmalig durchlaufen werden. In den folgenden Abschnitten werden die einzelnen Phasen beschrieben.

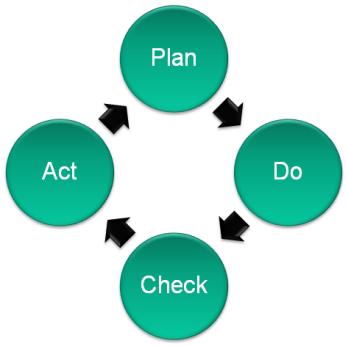


Abbildung 3: PDCA-Zyklus nach Deming

5.1 Definition der Ziele und Abgrenzung des Anwendungsbereichs

Von zentraler Bedeutung für den Erfolg der Einführung des Softwaresystems ist die erste Phase. Die große Vielfalt der am Markt verfügbaren Systeme wurde nicht zuletzt anhand der vier vorgestellten Klassen von Systemen bereits dargestellt. Auch innerhalb dieser Klassen gibt es umfangreiche Unterschiede, sodass dieses Modell prinzipiell von der Einführung einer Einzelplatzlösung für die Bearbeitung der Grundschutzkataloge bis hin zur Einführung eines unternehmensweiten GRC-Systems skalieren muss. In der Praxis erfordert die Einführung einer integrierten Lösung eine ausführlichere Planung, als die Einführung eines Einzelplatzsystems.

Gerade wenn Systeme nach langen und teuren Einführungsprojekten tief in die IT-Infrastruktur einer Organisation integriert sind, ist eine langjährige Nutzung und eine dauerhafte Partnerschaft mit dem Hersteller sinnvoll, um regelmäßige Systemwechsel zu vermeiden. Daher ist es wichtig, die Projektziele und den Anwendungsbereich nicht nur kurzfristig sondern auch mittel- und langfristig zu definieren.

Kurzfristige Perspektive

Bei der Festlegung einer kurzfristigen Perspektive gilt es klar zu definieren, welche Funktionen und welche Prozesse kurzfristig, also während der Laufzeit des Einführungsprojekts, realisiert werden sollen. Wie auch bei der Einführung eines ISMS ist hier die Unterstützung durch das Management erforderlich, um den Geltungsbereich und die ggf. gewünschte Integration in Unternehmensprozesse auch über den Fokus eines ISMS hinaus in Richtung eines IT-GRC- oder eGRC-Systems festzulegen und die benötigten Ressourcen zur Verfügung zu stellen.

Mittel- und langfristige Perspektive

Neben der kurzfristigen Perspektive sollten bei der Einführung eines ISMS-Softwaresystems aber auch weitere Optionen für die Zukunft abgewogen werden. Viele Hersteller unterstützen solche langfristigen Planungen durch flexible Lizenzierungsoptionen, bei denen einzelne Module bedarfsorientiert nachgerüstet werden können. Allerdings lassen sich so nur Funktionen nachrüsten, die im System vorhanden sind. Um die Investition in das Softwaresystem und das Einführungsprojekt langfristig zu sichern, sollten auch Erweiterungsoptionen für die Zukunft bedacht werden. Es bietet sich daher an, noch vor der Auswahl eines Softwaresystems zukünftig denkbare Anforderungen oder ggf. in anderen Abteilungen bereits vorhandene Systeme zu erfassen und zu dokumentieren.

5.2 Auswahl eines geeigneten Softwaresystems

Nach der Definition der Ziele und des Anwendungsbereichs ist es erforderlich, geeignete Softwaresysteme auszuwählen. Dazu wird ein dreistufiges Vorgehen vorgeschlagen. Nach einer Grobauswahl folgt eine Feinauswahl und in einer Pilotierung sollten Systeme noch vor Einführungsbeginn getestet werden.

Grobauswahl

Der erste Schritt bei der Auswahl eines Softwaresystems ist die Grobauswahl. Als Basis hierzu können die Marktübersichten aus Kapitel 4 dienen. Es erscheint zweckmäßig, dabei auch auf die Klassifizierung der Systeme zurückzugreifen und grundlegend zu entscheiden, ob ein Grundschutztool, ein ISMS-Softwaresystem, ein IT-GRC-Softwaresystem oder eGRC-Softwaresystem für die Realisierung der definierten Ziele geeignet ist. Durch die Auswahl einer Klasse der ISMS-Softwaresysteme anhand der vorgeschlagenen Klassifikation können bereits in der Grobauswahl-Phase Systeme ausgeschlossen werden, die nicht alle benötigten Standards unterstützen.

Feinauswahl

Nach Abschluss der Grobauswahl ist es zweckmäßig, eine Feinauswahl vorzunehmen, um die Gruppe möglicher Systeme weiter zu reduzieren. Da eine solche Bewertung aufwändig ist, sollte die Anzahl der betrachteten Systeme möglichst gering gehalten werden. Neben der Auswertung von Herstellerinformationen können in dieser Phase auch Produktpräsentationen wichtige Informationsquellen sein.

Pilotierung und Auswahl

Nach Abschluss der Feinauswahl wird eine Pilotierung mit einem oder zwei geeigneten Systemen vorgeschlagen. In dieser Phase ist es nicht notwendig, alle technischen Schnittstellen zu implementieren oder die eigene Organisation vollständig abzubilden, vielmehr erscheint es zweckmäßig, ausgewählte zukünftige Nutzer des Systems mit dem Prototypen arbeiten zu lassen, um exemplarisch Teilaspekte abzubilden und zu testen. Nachdem nur von wenigen Systemen Testversionen frei verfügbar sind, erfordert diese Phase eine intensive Zusammenarbeit mit dem Hersteller und kann so gleichzeitig als Test für die Zusammenarbeit und die Verständigung mit dem Hersteller dienen. Als letzter Schritt vor der nächsten Phase muss eine Entscheidung für ein Produkt und für die Einführung eines solchen Softwaresystems getroffen werden.

5.3 Einführung eines ISMS-Softwaresystems

Für die Einführung eines ISMS-Softwaresystems ist ein organisations- und produktabhängiger Projektplan erforderlich, der im Rahmen dieses generischen Vorgehensmodells nicht genau definiert werden kann. Dieser Projektplan kann z.B. das Einführungsprojekt in verschiedene Phasen unterteilen oder eine Einführungsreihenfolge für einzelne Organisationsteile festlegen.

Von zentraler Bedeutung für den Projekterfolg ist die Unterstützung durch das Management und aller Verantwortlichen der betroffenen Organisationseinheiten. So erscheint es z.B. als nicht durchführbar, dass die Einführung eines unternehmensweiten eGRC-Systems ausschließlich durch die für Informationssicherheit verantwortliche Stelle getrieben wird. Gerade bei der Einführung von GRC-Systemen handelt es sich um sehr langfristige Projekte mit vielen Beteiligten, die konsequent und dauerhaft gesteuert werden müssen. Die Einführung eines solchen, komplexen Systems ohne Unterstützung durch den Hersteller erscheint nicht möglich oder zumindest wirtschaftlich nicht sinnvoll. Je nach Qualifikationsniveau der beteiligten Mitarbeiter kann auch eine über das gewählte Tool hinausgehende Beratungsleistung erforderlich oder sinnvoll sein. Eine schrittweise Einführung erscheint generell möglich, allerdings sollte dabei beachtet werden, dass alle logischen Schnittstellen bereits frühzeitig definiert werden müssen, während die technische Umsetzung automatisierter Schnittstellen auch schrittweise erfolgen kann. Grundsätzlich gilt, dass Effizienzgewinne nicht der einzige Grund für die Einführung eines solchen Systems sein sollten. Auch weitere Aspekte, wie eine steigende Konformität mit Vorschriften oder eine bessere Transparenz der aktuellen Situation müssen berücksichtigt werden und können oft nur schwer als finanzieller Vorteil quantifiziert werden. Vor allem im Bereich der Compliance ist jedoch bereits belegt, dass die Kosten bei fehlender Compliance die Kosten von Maßnahmen zur Gewährleistung von Compliance übersteigen [52]. Zumindest während der Einführungsphase sind Effizienzgewinne nicht sofort, sondern zusätzliche Aufwände, auch durch Änderungen im Arbeitsablauf der betroffenen

Mitarbeiter, zu erwarten. Alle Mitarbeiter, die mit dem System arbeiten, müssen ebenfalls berücksichtigt werden. Gerade bei den komplexen Systemen, wie den eGRC-Systemen, ist die Erstellung von organisationsspezifischen Handbüchern und Schulungsmaterialien notwendig, die die Komplexität und Funktionalitäten des Systems auf das von den Nutzern benötigte Maß reduzieren.

5.4 Betrieb eines ISMS-Softwaresystems

An die Einführung des Softwaresystems schließt sich die Phase des Betriebs der Lösung an. Sofern es sich bei der gewählten Lösung nicht um ein SaaS-Angebot handelt, ist neben dem inhaltlichen Betrieb der Lösung auch eine technische Betreuung notwendig. Unabhängig von dem technischen Betrieb muss die Lösung auch kontinuierlich inhaltlich betreut werden. Zu dieser Betreuung zählt organisationsintern die Betreuung der Nutzer der Lösung und die Durchführung von Schulungen für neu hinzukommende Benutzer. Nach außen gerichtet steht vor allem der regelmäßige Kontakt mit dem Hersteller im Vordergrund. Vor allem bei Lösungen mit nur einer überschaubaren Anzahl aktiver Installationen lassen sich so die weitere Entwicklung der Lösung aktiv beeinflussen und die eigenen Interessen vertreten. Aber auch bei weiter verbreiteten Lösungen ist ein dauerhafter Kontakt zum Hersteller sinnvoll, um neue Entwicklungen frühzeitig zu erkennen und von Erfahrungen des Herstellers mit anderen Kunden zu profitieren. Eine gute Möglichkeit zum Austausch mit anderen Kunden bieten Anwendertage der Hersteller oder im Falle des BSI Grundschutztools die regelmäßig stattfindenden Grundschutztage.

Während größere Erweiterungen des Softwaresystems, wie z.B. die Nutzung zusätzlicher GRC-Funktionen, in der Regel in Form von eigenen Projekten eingeführt werden, sollte auch während des Betriebs des Softwaresystems kontinuierlich an Verbesserungen gearbeitet werden und die Nutzung des Systems kritisch begleitet werden. Ein solches Vorgehen und der damit verbundene kontinuierliche Verbesserungsprozess ähnelt somit dem in Kapitel 8 „Verbesserung des ISMS“ der ISO/IEC 27001 [17] Norm beschriebenen Vorgehens.

6 Handlungsempfehlungen für Betreiber eines Informationssicherheitsmanagementsystems

Eine Studie der British Standards Institution [4] aus dem Jahr 2011 belegt, dass sich die Nutzung des ISMS-Standards ISO/IEC 27001 auf 87 Prozent der befragten Unternehmen positiv ausgewirkt hat und in vielen Fällen zu einer Kostenreduktion geführt hat. Neben der Entscheidung für die Nutzung eines solchen Standards im eigenen Unternehmen und für Unternehmen, die bereits erfolgreich auf Basis von ISO/IEC 27001 oder nach BSI Grundschutz zertifiziert wurden, steht vor allem auch die Frage nach geeigneter Softwareunterstützung im Raum. Wie im Kapitel 4 beschrieben, bietet der Markt ein breites Angebot an sehr unterschiedlichen Lösungen, so dass die Auswahl einer geeigneten Lösung schwer fällt. Gleichzeitig nutzen noch wenige Unternehmen ISMS-Softwaresysteme[1], so dass sich noch keine Branchen- oder Unternehmensgrößensabhängigen Trends zur Nutzung einzelner Lösungen erkennen lassen. Die in diesem Kapitel beschriebenen Handlungsempfehlungen unterstützen bei der Schaffung der notwendigen Rahmenbedingungen für die Auswahl und Einführung einer für die individuellen Anforderungen geeigneten Lösung.

Entscheidung für die Einführung eines ISMS-Softwaresystems

- Strategische Ausrichtung festlegen

Die Entscheidung für die Einführung eines ISMS-Softwaresystems ist eine langfristige strategische Überlegung. Dies gilt umso mehr, wenn über die Einführung einer stark integrierten Lösung entschieden wird. Besonders in diesem Fall sollten auch die langfristigen Anforderungen sowie eine maximal geplante Integrationstiefe festgelegt werden. Ebenfalls sollten bereits frühzeitig alle aktuell und ggf. zukünftig genutzten ISMS-Standards erfasst und festgehalten werden, da diese Rahmenbedingungen die Basis für eine Auswahl eines auch langfristig geeigneten Systems darstellen.

- Unterstützung sichern und Ressourcen bereitstellen

IT-GRC- und eGRC-Systeme erweitern den Fokus des Systems und auch den Nutzerkreis über die mit dem Betrieb eines ISMS beauftragte Abteilung hinaus. Aus

[1] Studien belegen dass der größte Teil der Unternehmen für den kompletten Bereich der Compliance keine speziellen Softwaresysteme nutzt. Diese Beobachtung deckt sich auch mit den von den Herstellern von ISMS-Softwaresystemen gemeldeten niedrigen Zahlen zu aktiven Installationen [38, 19].

diesem Grund müssen schon bei der Projektplanung und der Einführungsentscheidung alle Beteiligten identifiziert und ihre Unterstützung gewonnen werden. In eingeschränkter Form gilt dies auch bei weniger komplexen Multinormensystemen, die neben dem ISMS auch eng verwandte Themen, wie z.B. Business Continuity Management (BCM) und Business Impact Analysen (BIA), behandeln. In jedem Fall ist auch die Unterstützung durch das Management und die Bereitstellung der für das Einführungsprojekt notwendigen Ressourcen notwendig. Im Besonderen bei der Nutzung integrierter Systeme sind Kostenersparnisse durch Effizienzgewinne erst nach der Einführungsphase zu erwarten.

Während der Auswahl eines ISMS-Softwaresystems

- Unabhängige Beratungsangebote nutzen

Für den langfristigen Erfolg und die Erzielung von Effizienzgewinnen, die die Kosten für Betrieb und Einführung eines ISMS-Softwaresystems übersteigen, ist es von zentraler Bedeutung die richtige Lösung für das eigene Unternehmen auszuwählen. Dabei kann auch auf die Erfahrung Dritter zurückgegriffen werden. Zum einen bieten mittlerweile einige IT-Dienstleister Beratungsangebote nicht nur bezüglich der Einführung von ISMS, sondern auch mit Hinblick auf Softwareunterstützung an. Zum anderen kann auch auf das in diesem Whitepaper vorgestellte Vorgehensmodell zurückgegriffen werden, dass um ein am Fraunhofer AISEC entworfenes Bewertungsschema für den Vergleich mehrerer Softwaresysteme, ergänzt werden kann.

- Mehrstufiges Auswahlverfahren durchführen

Unabhängig vom konkreten Vorgehen sollte das Auswahlverfahren stets mehrstufig erfolgen, da sich Systeme aus unterschiedlichen der in Kapitel 4 vorgestellten Klassen nur eingeschränkt vergleichen lassen.

- Sicherheitsanforderungen beachten

Der aktuelle Trend der Bereitstellung von Anwendungen im SaaS-Lizenzmodell ist auch im Bereich der ISMS-Softwaresysteme wahrnehmbar. Vor allem amerikanische Anbieter nutzen SaaS bereits aktiv. Deutsche Unternehmen sollten eine Nutzung solcher Angebote aber sehr sorgfältig abwägen, da die Daten eines ISMS-Softwaresystems einen umfangreichen Überblick über die unternehmenseigene System- und Prozesslandschaft bieten und selbst wenn der Betreiber der Lösung als vertrauenswürdig eingestuft wird, gesteigerte Sicherheitsanforderungen, wie z.B. die Anforderung einer externen Auditierung des Softwaresystems, im Regelfall nicht erfüllt werden.

Während der Einführung eines ISMS-Softwaresystems

- Unterstützung durch den Hersteller nutzen

Viele Hersteller bieten, teilweise auch in Zusammenarbeit mit Partnern, zum Produkt ergänzende Beratungsleistungen für die Einführungsphase an. Da es sich bei allen integrierten Systemen um komplexe Softwaresysteme handelt, bietet es sich an, das in der eigenen Organisation notwendige Know-How durch die Nutzung externer Unterstützung zu begrenzen.

- Modulare Lösungen schrittweise einführen

Die Einführung komplexer Systeme sollte dabei schrittweise erfolgen. Zahlreiche Hersteller unterstützen solch ein Vorgehen auch durch flexible Lizenzmodelle, mit deren Hilfe sich weitere Funktionen bei Bedarf nachrüsten lassen. Ebenfalls müssen nicht sofort alle technisch wünschenswerten Schnittstellen realisiert werden. Sofern vorgesehen, kann auch mit logischen Schnittstellen und manuellen Übertragungsvorgängen gestartet werden.

- Aufgabenspezifische Mitarbeiterschulungen bereitstellen

Im Verlauf der Durchführung dieser Studie hat sich gezeigt, dass die von den Anbietern bereitgestellten Dokumentationen überwiegend nicht für Endnutzer geeignet sind. Hier ist es notwendig für einzelne Nutzergruppen spezifische und auf den tatsächlich benötigten Funktionumfang reduzierte Schulungsmaterialien vorzubereiten.

Während des Betriebs einer ISMS-Lösung

- Kontinuierlichen Verbesserungsprozess umsetzen

In der Betriebsphase gilt es das eingeführte System zu pflegen und weiter zu verbessern. Als Teil des ISMS sollte auch das ISMS-Softwaresystem den in ISO/IEC 27001 vorgegebenen kontinuierlichen Verbesserungsprozess umsetzen.

- Effizienzsteigerungen durch Automatisierung realisieren

Eine Maßnahme im Rahmen der kontinuierlichen Verbesserungsprozesses kann der kontinuierliche Ausbau des Automatisierungsgrades durch die Realisierung weiterer technischer Schnittstellen sein.

- Weiterentwicklung des Softwaresystems begleiten und beeinflussen

Der überwiegende Teil der Anbieter hat einen überschaubaren Kundenstamm, so dass man als einzelner Kunde die Weiterentwicklung des Produkts durch den Hersteller aktiv begleiten und durch die Platzierung eigener Anforderungen beeinflussen kann.

7 Zusammenfassung der Ergebnisse

Im Rahmen der vorliegenden Studie wurden neben einer groben Klassifizierung der angebotenen Produkte in die folgenden vier Klassen:

- ISMS-Softwaresysteme auf Basis von ISO/IEC 27001,
- Grundschutztools,
- IT-GRC-Systeme und
- integrierte GRC-Systeme.

Auch ein Vorgehen für die Auswahl und Einführung eines geeigneten Softwaresystems vorgeschlagen. Trotz vielfältiger Unterschiede zwischen den angebotenen Systemen lassen sich vor allem zwei große Trends erkennen. Der erste Trend ist die technologische Ausrichtung hin zu webbasierten Anwendungen und damit die Eröffnung neuer Nutzungsszenarien wie SaaS. Der zweite Trend ist die zunehmende Integration von GRC-Funktionen in die ISMS-Softwaresysteme. Damit entwickeln sich die Systeme immer mehr in Richtung von IT-GRC-Systemen. Wie weit diese Entwicklung bereits fortgeschritten ist, hängt stark von der Leistungsfähigkeit und Historie des Herstellers ab. Grundsätzlich ist eine Entwicklung hin zu IT-GRC- und damit Multi-Standardsystemen eine logische Konsequenz der gleichzeitigen Nutzung vieler unterschiedlicher Standards in Organisationen. Gerade mit den beiden wichtigen Standards COBIT und ITIL beschäftigen sich sehr viele IT-Abteilungen und sammeln dabei auch Informationen, die sich mit dem ISMS überschneiden. Die Verwaltung gleicher Informationen in voneinander getrennten Systemen ist nicht effizient und die wiederholte manuelle Abfrage gleichartiger Daten bei internen Datenlieferanten kann nicht nur für mangelnde Akzeptanz der Standardisierungsbemühungen sorgen, sondern auch zu Widersprüchen oder Abweichungen in den getrennten Datenbasen führen. Eine Konvergenz der Daten in gemeinsame Systeme ist daher nicht nur eine Maßnahme zur Steigerung der Effizienz, sondern erhöht auch direkt die Verfügbarkeit, Aktualität und Qualität der Daten.

Die beiden in dieser Studie schwerpunktmäßig behandelten Standards ISO/IEC 27001 und BSI Grundschutz sind für Organisationen unterschiedlicher Größe anwendbar. Die am Markt verfügbaren Systeme bieten diese Universalität nur eingeschränkt. Durch das vielfältige Angebot an Lösungen ist aber für fast jedes Szenario eine geeignete Softwarelösung verfügbar. Neben potenziellen Effizienzsteigerungen bieten ISMS-Softwaresysteme auch weitere Vorteile, wie zunehmende Transparenz und steigende Konformität mit den Vorgaben der Standards.

Multi-Normen-Werkzeuge oder GRC-Systeme verbinden darüber hinaus inhaltlich verknüpfte Informationen, die ohne diese Systeme bisher zumeist getrennt und ggf. mehrfach gepflegt werden.

Der Einsatz integrierter GRC-Systeme erfordert allerdings erhebliche Aufwände für Einführung und Anpassung. Kritisch für den Erfolg bei der Nutzung von solchen Softwaresystemen ist die Auswahl einer auch dauerhaft für die eigenen Anforderungen geeigneten Lösung. Das im Rahmen dieser Studie vorgeschlagene Vorgehensmodell für die Einführung eines solchen Softwaresystems berücksichtigt daher neben kurzfristigen Anforderungen auch mittel- und langfristige Entwicklungsperspektiven. Alle Organisationen, die bereits ISMS betreiben oder über die Einführung eines solchen Managementsystems nachdenken, sollten sich daher über die Vorteile von Softwareunterstützung informieren und eine Einführung eines geeigneten Softwaresystems abwägen.

Literaturverzeichnis

[1] *Gesetz zur Kontrolle und Transparenz im Unternehmensbereich (KonTraG)*. April 1998 *Referenziert auf S. 2*

[2] BITKOM ; DIN: *Kompass der IT-Sicherheitsstandards - Leitfaden und Nachschlagewerk, 4. Auflage*. August 2009 *Referenziert auf S. 2, S.10, S.13 und S.23*

[3] British Standards Institution: *BS 7799-3:2006*. http://shop.bsigroup.com/en/ProductDetail/?pid=000000000030125022. – Zuletzt abgerufen am 3. September 2012 *Referenziert auf S. 14*

[4] British Standards Institution: *How does an information securitymanagement system help my business?* http://www.bsigroup.de/upload/Case_Studies/Erasmus-ISO-27001-Research-Sheet.pdf. Version: September 2011 *Referenziert auf S. 28*

[5] Bundesamt für Sicherheit in der Informationstechnik: *Andere Tools zum IT-Grundschutz*. https://www.bsi.bund.de/DE/Themen/weitereThemen/GSTOOL/AndereTools/anderetools_node.html. – Zuletzt abgerufen am 3. September 2012 *Referenziert auf S. 18*

[6] Bundesamt für Sicherheit in der Informationstechnik: *Zuordnungstabelle ISO 27001 sowie ISO 27002 und IT-Grundschutz*. https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Hilfsmittel/Vergleich_ISO27001_GS.pdf?__blob=publicationFile. – Zuletzt abgerufen am 3. September 2012 *Referenziert auf S. 12*

[7] Bundesamt für Sicherheit in der Informationstechnik: BSI-Standard 100-1 Managementsysteme für Informationssicherheit Version 1.5. (2008) *Referenziert auf S. 6 und S.11*

[8] Bundesamt für Sicherheit in der Informationstechnik: BSI-Standard 100-2 IT-Grundschutz-Vorgehensweise Version 2.0. (2008) *Referenziert auf S. 11 und S.23*

[9] Bundesamt für Sicherheit in der Informationstechnik: BSI-Standard 100-3 Risikoanalyse auf Basis von IT-Grundschutz. (2008) *Referenziert auf S. 11*

[10] Bundesamt für Sicherheit in der Informationstechnik: BSI-Standard 100-4 Notfallmanagement Version 1.0. (2008) *Referenziert auf S. 12*

[11] Butler-Stewart, James: *Father of ISMS Standards*. Infosec Publications, 2009 *Referenziert auf S. 10*

[12] Caldwell, French ; Scholtz, Tom ; Hagerty, John: *Magic Quadrant for Enterprise Governance, Risk and Compliance Platforms*. Gartner, Juli 2011 *Referenziert auf S. 22*

[13] Computer Security Division Information Technology Laboratory: *Recommended Security Controls for Federal Information Systems and Organizations*. http://csrc.nist.gov/publications/nistpubs/800-53-Rev3/sp800-53-rev3-final.pdf. Version: August 2009 *Referenziert auf S. 15*

[14] Defence Signal Directorate: *ISM - Information Security Manual*. http://www.dsd.gov.au/infosec/ism/index.htm. – Zuletzt abgerufen am 3. September 2012 *Referenziert auf S. 14*

[15] Deming, W. E.: *Out of the Crisis*. The MIT Press, 1988 *Referenziert auf S. 10*

[16] Deutsches Institut für Normung e.V.: *NA 043 Normenausschuss Informationstechnik und Anwendungen (NIA)*. http://www.nia.din.de. – Zuletzt abgerufen am 3. September 2012 *Referenziert auf S. 10*

[17] DIN ISO/IEC: *Informationstechnik - IT-Sicherheitsverfahren - Informationssicherheits-Managementsysteme - Anforderungen DIN ISO/IEC 27001*. – Entwurf Februar 2007 *Referenziert auf S. 6, S.10, S.23 und S.27*

[18] Disterer, Georg: ISO 20000 for IT. In: *Business & Information Systems Engineering* 1 (2009), S. 463–467 *Referenziert auf S. 14*

[19] Eichler, Jörn ; Bona-Stecki, Mike ; Wieczorek, Thomas: Sicherheitsverwalter. In: *iX* 6 (2011), S. 90–94 *Referenziert auf S. 2, S.18 und S.28*

[20] Falk, Michael: *Ableitung des Control-Frameworks für IT-Compliance*. Gabler, 2012 *Referenziert auf S. 13 und S.14*

[21] Fiege, Stefanie: Risikomanagement und KonTraG. In: Reimer, Marko (Hrsg.) ; Fiege, Stefanie (Hrsg.): *Perspektiven des Strategischen Controllings*. Gabler, 2010, S. 301–312 *Referenziert auf S. 2*

[22] Förtsch, Michael: *GSTOOL 5.0 Die nächste Generation*. https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Veranstaltungen/Grundschutz/3GS_Tag_121011/Die-naechste-Generation.pdf?__blob=publicationFile. Version: Oktober 2011. – Zuletzt abgerufen am 3. September 2012 *Referenziert auf S. 20*

[23] Goltsche, Wolfgang: *COBIT kompakt und verständlich*. Vieweg, 2006 *Referenziert auf S. 13*

[24] Grünendahl, Ralf-T. ; Steinbacher, Andreas F. ; Will, Peter H. L.: COBIT und BSI als Leitschnur der IT-Sicherheit. In: *Das IT-Gesetz: Compliance in der IT-Sicherheit*. Vieweg+Teubner, 2009, S. 11–17 *Referenziert auf S. 13*

[25] Heiser, Jay: *Hype Cycle for Governance, Risk and Compliance Technologies, 2011*. Gartner, Juli 2011 *Referenziert auf S. 8*

[26] Heschl, Jimmy: COBIT in Relation to Other International Standards. In: *Information Systems Control Journal* 4 (2004) *Referenziert auf S. 12*

[27] HiScout GmbH: *HiScout GRC Suite*. `http://www.hiscout.com/index.php?id=3`. – Zuletzt abgerufen am 3. September 2012 *Referenziert auf S. 18*

[28] Howaldt, Jürgen ; Kopp, Ralf ; Winther, Michael: *Kontinuierlicher Verbesserungsprozeß - KVP als Motor lernender Organisation*. Schäffer-Poeschel, 1998 *Referenziert auf S. 10*

[29] Humpert, Frederik: *IT-Grundschutz umsetzen mit GSTOOL*. Hanser, 2005 *Referenziert auf S. 11 und S.12*

[30] Humphreys, Edward: Information Security Management System Standards. In: *Datenschutz und Datensicherheit* 1 (2011) *Referenziert auf S. 10*

[31] Humphreys, Edward u. a. ; Humphreys, Edward (Hrsg.): *SC27 Platinum Book Twenty Years of ISO/IEC JTC 1 / SC27*. Gipping Press Ltd, 2010 *Referenziert auf S. 10*

[32] ISACA: *COBIT Framework for IT Governance and Control*. `http://www.isaca.org/Knowledge-Center/COBIT/Pages/Overview.aspx`. – Zuletzt abgerufen am 3. September 2012 *Referenziert auf S. 13*

[33] Kilian, Detlef: Einführung in Informationssicherheitsmanagementsysteme (I): Begriffsbestimmung und Standards. In: *IT-Sicherheit & Datenschutz* 10 (2006) *Referenziert auf S. 10*

[34] Kilian, Detlef: Einführung in Informationsmanagementsysteme (II): BSI-Standards und Vergleich. In: *IT-Sicherheit & Datenschutz* 1 (2007) *Referenziert auf S. 10*

[35] Kilian, Detlef: Einführung in Informationsmanagementsysteme (III): Praktische Umsetzung von Informationssicherheitsstandards. In: *IT-Sicherheit & Datenschutz* 3 (2007) *Referenziert auf S. 10*

[36] Klipper, Sebastian: *Information Security Risk Management: Risikomanagement mit ISO/IEC 27001, 27005 und 31010*. Vieweg+Teubner, 2011 *Referenziert auf S. 11*

[37] Königs, Hans-Peter: *IT-Risiko-Management mit System: Von den Grundlagen bis zur Realisierung - Ein praxisorientierter Leitfaden*. 3. Auflage. Vieweg+Teubner, 2009 *Referenziert auf S. 13*

[38] Kronschnabl, Stefan ; Weber, Stephan ; Dirnberger, Christian ; Török, Elmar ; Münch, Isabel: *IT-Sicherheitsstandards und IT-Compliance 2010 Befragung zu Status quo, Trends und zukünftigen Anforderungen*. http://epub.uni-regensburg.de/19032/. – Zuletzt abgerufen am 3. September 2012 *Referenziert auf S. 2, S.19 und S.28*

[39] Lang, Carsten: *sidoc-Sicherheitsmanagement*. http://www.sidoc.info/. – Zuletzt abgerufen am 3. September 2012 *Referenziert auf S. 20*

[40] McClean, Chris: *The Forrester Wave: Enterprise Governance, Risk, And Compliance Platforms, Q4 2011*. Forrester, Dezember 2011 *Referenziert auf S. 18 und S.22*

[41] McClean, Chris: *The Forrester Wave: IT Governance, Risk And Compliance Platforms, Q4 2011*. Forrester, Dezember 2011 *Referenziert auf S. 7, S.18 und S.22*

[42] Meints, Martin: Datenschutz nach BSI-Grundschutz? In: *Datenschutz und Datensicherheit* 30 (2006) *Referenziert auf S. 12*

[43] Menken, Ivanka: *ISO/IEC 20000 Certification and Implementation Guide - Standard Introduction, Tips for Successful ISO/IEC 20000 Certification, FAQs, Mapping ... and ISO 20000 Acronyms*. Emereo Pty Ltd, 2010 *Referenziert auf S. 10*

[44] Müller, Klaus-Rainer: *IT-Sicherheit mit System*. 4. Auflage. Vieweg+Teubner, 2011 *Referenziert auf S. 6, S.10 und S.13*

[45] Modulo: *Learn more about Modulo*. http://www.modulo.com/modulo/modulo. – Zuletzt abgerufen am 3. September 2012 *Referenziert auf S. 21*

[46] National Institute of Standards an Technology: *Computer Security Division*. http://csrc.nist.gov/. – Zuletzt abgerufen am 3. September 2012 *Referenziert auf S. 15*

[47] Neumann, Alexander: *Integrative Managementsysteme*. Physica-Verlag HD, 2008 *Referenziert auf S. 6 und S.10*

[48] Neupart Inc.: *IT GRC for Financial Services*. http://www.neupart.com/industries/financial-services.aspx. – Zuletzt abgerufen am 3. September 2012 *Referenziert auf S. 21*

[49] Neupart Inc.: *SecureAware - achieve continuous compliance*. http://www.neupart.com/products.aspx. – Zuletzt abgerufen am 3. September 2012 *Referenziert auf S. 21*

[50] Nicolett, Mark ; Proctor, Paul E.: *MarketScope for IT Governance, Risk and Compliance Management*. Gartner, September 2011 *Referenziert auf S. 7, S.18 und S.22*

[51] Pattinson, Fiona: *Security Assurance: Contrasting FISMA and ISO/IEC 27001*. atsec information security corporation, 2011. http://www.atsec.com/downloads/documents/FISMA_27001.pdf. – Zuletzt abgerufen am 3. September 2012 *Referenziert auf S. 15*

[52] Ponemon Institute: *The True Cost of Compliance Benchmark Study of Multinational Organizations*. http://www.tripwire.com/ponemon-cost-of-compliance/. Version: Januar 2011. – Zuletzt abgerufen am 3. September 2012 *Referenziert auf S. 26*

[53] Racz, Nicolas ; Weippl, Edgar ; Seufert, Andreas: A Frame of Reference for Research of Integrated Governance, Risk and Compliance (GRC). In: De Decker, Bart (Hrsg.) ; Schaumüller-Bichl, Ingrid (Hrsg.): *Communications and Multimedia Security* Bd. 6109. Springer Berlin / Heidelberg, 2010, S. 106–117 *Referenziert auf S. 6*

[54] Roebuck, Kevin: *Legal GRC: High-impact Strategies - What You Need to Know: Definitions, Adoptions, Impact, Benefits, Maturity, Vendors*. Tebbo, 2011 *Referenziert auf S. 8*

[55] Secopan UG: *Dienstleistungen*. http://www.secopan.de/home/dienstleistungen2.html. – Zuletzt abgerufen am 3. September 2012 *Referenziert auf S. 18*

[56] SerNet GmbH: *Willkommen bei verinice.PRO!* http://verinicepro.org/. – Zuletzt abgerufen am 3. September 2012 *Referenziert auf S. 18*

[57] Swiss Infosec AG: *ISMS Tool Box Pro*. http://infosec.ch/ismstoolboxpro/ismstoolboxpro.htm. – Zuletzt abgerufen am 3. September 2012 *Referenziert auf S. 18*

[58] The APM Group Ltd: *The Official ITIL® Website*. http://www.itil-officialsite.com/. – Zuletzt abgerufen am 3. September 2012 *Referenziert auf S. 13*

[59] WMC GmbH: *Huf Gruppe Informationssicherheitsmanagement*. http://www.wmc-direkt.de/branchen/automotive/CaseStudy_Huf_20110525.pdf. – Zuletzt abgerufen am 3. September 2012 *Referenziert auf S. 23*

[60] Zentrum für sichere Informationstechnologie Austria: *Österreichisches Informationssicherheitshandbuch Version 3.1.002*. Bundeskanzleramt Österreich, 2010 *Referenziert auf S. 14*

Kontaktdaten

Fraunhofer Research Institution AISEC
Parkring 4
D 85748 Garching bei München
Tel.: +49 (0)89 322 9986 0
Fax.: +49 (0)89 322 9986 299
http://www.aisec.fraunhofer.de

Planung und Durchführung der Studie
Iryna Windhorst
Tel.: +49 (0)89 322 9986 157
iryna.windhorst@aisec.fraunhofer.de

Benedikt Pirzer
Tel.: +49 (0)89 99954991
benedikt.pirzer@tum.de

Forschungsbereich „Sichere Services und Qualitätstests“
Mario Hoffmann
Tel.: +49 (0)89 322 9986 177
mario.hoffmann@aisec.fraunhofer.de

Presse und Öffentlichkeitsarbeit
Viktor Deleski
Tel.: +49 (0)89 322 9986 169
viktor.deleski@aisec.fraunhofer.de

Stand des Whitepapers: September 2012