Maximilian Eibl, Martin Gaedke. (Hrsg.): INFORMATIK 2017,
Lecture Notes in Informatics (LNI), Gesellschaft für Informatik, Bonn 2017 1617

ISMS-Tools zur Unterstützung eines nativen ISMS gemäß ISO 27001

Marlen Hofmann[1] und Andreas Hofmann[2]

Abstract: Steigende Bedeutung von Informationssicherheit und neue gesetzliche Anforderungen motivieren Unternehmen nahezu aller Branchen zur Einführung eines nativen Informationssicherheitsmanagementsystems (ISMS) gemäß den Anforderungen der DIN ISO/IEC 27001. Zur IT-seitigen Unterstützung des ISMS stehen am Markt zahlreiche Werkzeuge zur Verfügung, deren Leistungsspektrum jedoch häufig intransparent ist und die i.d.R. nur einzelne, weitläufig bekannte ISMS-Aufgaben unterstützen. Im Rahmen des Forschungsvorhabens „CISO27" wurden daher in früheren Forschungsiterationen funktionale Anforderungen an ISMS-Tools und ein Referenzprozess zur Umsetzung eines nativen ISMS-Vorgehens erarbeitet. Im Rahmen dieses Beitrags werden dazu ergänzend eine strukturierte Marktstudie zu verfügbaren ISMS-Tools erstellt und deren Funktionalitäten entlang des Anforderungskataloges bewertet.

Keywords: Management von Informationssicherheit, ISO 27001, ISMS-Tools, ISO27-Sicherheitsprozess, ISMS, Anforderungen an ISMS-Tools, Marktstudie zu ISMS-Tools

1 Darstellung des Forschungsvorhabens CISO27

Steigende Bedeutung von Informationssicherheit und neue gesetzliche und regulatorische Anforderungen motivieren Unternehmen nahezu aller Branchen zur Einführung und zum Betrieb eines nativen Informationssicherheitsmanagementsystems (ISMS) gemäß den Anforderungen der DIN ISO/IEC 27001 (ISO 27001) [BV15]. Aufgrund der Freiheitsgrade der Norm und deren eingeschränkter Prozessorientierung gibt es in der Praxis jedoch bislang keine standardisierten Abläufe im ISMS-Betrieb und auch die verfügbaren ISMS-Tools unterstützen i.d.R. nur einige wenige, weitläufig bekannte ISMS-Aktivitäten [HH16a].

Das Forschungsvorhaben CISO27 adressiert diese Problemstellung und hat zum Ziel, einen Informationssicherheitsprozess und eine adäquate IT-Lösung zu konzipieren, mithilfe derer die Unternehmen "by Design" ein transparentes natives ISMS betreiben können. In einem ersten Schritt entstand dazu bereits der ISO27-Sicherheitsprozess (ISO27-SP), welcher einen Überblick über die notwendigen Prozessschritte und Aufgaben für einen normkonformen nativen ISMS-Betrieb gibt [HH16a].

In einem zweiten Schritt wurde auf Basis des ISO27-SP ein Anforderungskatalog erarbei-

[1] CISO27, Am Wachberg 2A 04425 Taucha, info@ciso27.org
[2] CISO27, Am Wachberg 2A 04425 Taucha, info@ciso27.org

doi:10.18420/in2017_162

tet, der übergreifende und prozessspezifische Anforderungen an ISMS-Tools zur Unterstützung des Referenzprozesses beinhaltet (Vgl. [HH16b]). Dieser Anforderungskatalog wird im Rahmen des vorliegenden Beitrags dazu genutzt, das Unterstützungspotential bestehender ISMS-Tools systematisch zu überprüfen und zu bewerten. Der Beitrag ist dazu wie folgt gegliedert: In Kapitel 2 findet sich eine Darstellung der angewendeten Forschungsmethode zur Erstellung der Marktstudie. Kapitel 3 gibt einen Überblick über die identifizierten ISMS-Tools. Die Darstellung der Analyseergebnisse findet sich in Kapitel 4. Die Gesamtbewertung sowie eine kurze Präsentation der erstplatzierten ISMS-Tools erfolgt in Kapitel 5. Der Beitrag endet mit einer Zusammenfassung und einem kurzen Fazit.

2 Forschungsmethode zur Erstellung der Marktstudie

Am Markt steht eine Vielzahl an ISMS-Tools zur Unterstützung des ISO27-SP zur Verfügung (Vgl. z.B. [WP12], [CS15]), die im Rahmen einer Marktstudie hinsichtlich ihres Unterstützungspotentials bewertet werden sollen. Um dabei transparente und nachvollziehbare Ergebnisse zu erzielen, wird die Marktstudie entlang der wissenschaftlichen Methodik zur Erstellung von strukturierten Literaturanalysen durchgeführt (Vgl. [Br09]). Dazu verdeutlicht die Übersicht in Tabelle 1 die wesentlichen Rahmenbedingungen (siehe markierte Zellen): Die Marktstudie fokussiert auf die Identifikation von ISMS-Tools zur Unterstützung des ISO27-SP. Zentrales Ziel ist es, das Leistungsspektrum der identifizierten Werkzeuge hinsichtlich der Eignung zur Unterstützung des ISO27-SP zu untersuchen und damit zentrale Probleme, resp. „Leistungslücken“ in den ISMS-Tools aufzuzeigen. Die Ergebnisse werden konzeptionell entlang des ISO27-SP sowie den dazu abgeleiteten Anforderungen aufbereitet und wertungsfrei dargestellt. Zielgruppe des Beitrages sind ISMS-Praktiker und -Forschungsgruppen. Der Marktstudie liegt die Datenbasis des World Wide Web zugrunde und der Zugriff erfolgte im Juli 2016 über die Suchmaschine google.de. In Bezug auf die Ergebnisse der Suchmaschine handelt es sich um eine umfassende Tool-Suche, die, ausgehend vom Erhebungszeitpunkt, ohne zeitliche Einschränkungen durchgeführt wurde. Die Tool-Analyse erfolgte hingegen selektiv, da nicht alle identifizierten ISMS-Tools überprüft werden konnten.

Characteristic		Categories			
1	Focus	Research outcomes	Research methods	Theories	Applications
2	Goal	Integration	Criticism	Central issues	
3	Organisation	Historical	Conceptual	Methodological	
4	Perspective	Neutral representation		Espousal of position	
5	Audience	Specialised scholars	General scholars	Practitioners/ politicians	General public
6	Coverage	Exhaustive	Exhaustive and selective	Representative	Central/ pivotal

Tab. 1: Dimensionen der strukturierten Marktstudie (Vgl. [Br09])

Die Tool-Suche wurde mit folgenden Suchbegriffen durchgeführt: "ISMS Werkzeug" OR "ISMS Tool" OR "ISMS Software" OR "ISMS Lösung" OR "27001 Werkzeug“ OR "27001 Tool" OR "27001 Lösung" OR "27001 Software". Dieses Vorgehen führte zu einer Vielzahl von Google-Ergebnissen die zunächst reduziert werden mussten. Dazu wurden die Websites nach Titel und Inhalt gescannt und initial deren Relevanz für die Marktstudie bewertet. Zur vertieften Untersuchung wurden Websites ausgewählt, die Werkzeuge zur Unterstützung des ISMS nach ISO 27001 oder BSI Grundschutz bereitstellen. Exkludiert wurden Websites, in denen die Suchbegriffe lediglich zu Werbe- oder Informationszwecken genutzt wurden. Die als relevant eingestuften Websites wurden anschließend in Hinblick auf die Verfügbarkeit von Dokumentationen und/oder Testversionen überprüft. In diesem Zuge wurden weitere Exklusionen vorgenommen: Es wurden Excel-Tools und Word-basierte Dokumentations-Kits ausgeschlossen sowie Werkzeuge exkludiert, die lediglich zu Vermarktungszwecken mit ISMS-relevanten Begriffen beschrieben wurden. Werkzeuge, über die unzureichend Informationen zugänglich oder die nicht in deutscher oder englischer Sprache verfügbar waren, wurden ebenfalls von der Marktstudie ausgeschlossen.

Die Tool-Analyse erfolgte durch ein 2-stufiges Evaluationsverfahren: Zunächst wurden öffentlich zugängliche Informationen (z.B. Produktpräsentationen) genutzt, um eine initiale Bewertung der Tools vorzunehmen. Auf einem herstellerseitigen Freiwilligkeitsprinzip basierend wurden die Werkzeuge anschließend mithilfe von geführten Produktdemonstrationen und/oder mithilfe von Testversionen vertieft analysiert. Jedes Werkzeug wurde dazu an Standard-Anforderungen gemessen und durch eine Experteneinschätzung auf einer dreistufigen Punkteskala bewertet. Bei Erfüllung der Anforderung erhielt das Werkzeug zwei Punkte, bei einer teilweisen Abbildung wurde ein Punkt vergeben. Bei Nichterfüllung oder in Ermangelung von Informationen durch die fehlende Möglichkeit zur vertieften Evaluierung wurden null Punkte vergeben.

3 Überblick über die ISMS-Tools

Durch das zuvor beschriebene Vorgehen wurden 36 ISMS-Tools identifiziert, von denen im Sinne einer priorisierten Abarbeitung zunächst nur europäische Werkzeuge analysiert wurden[3]. Diese lassen sich weitergehend systematisieren: Werkzeuge mit einem breiten fachlichen Ansatz, die dem Bereich der Governance-Risk-Compliance Tools zuzuordnen sind (GRC-Tools), Werkzeuge, die auf die Unterstützung des ISMS nach ISO 27001 nativ abzielen (ISO-Tools), Werkzeuge, die auf die Unterstützung des ISMS nach BSI Grundschutz abzielen (GS-Tools), Werkzeuge, die ihren Ursprung in der IT-Dokumentation haben (Doku-Tools) und Werkzeuge, die originär das Enterprise Risk Managment unterstüt-

[3] Folgende Nicht-Europäische Werkzeuge wurden ausgeschlossen: Comply27, Conformance Works 20000, CYBERWATCH, ISMS software (Paladion), ISO Manager, Modulo Risk Manager und TAMIM ISMS

zen (RM-Tools). Die Einordnung der Werkzeuge kann nachfolgender Tabelle 2 entnommen werden. Markierte Zellen visualisieren Tools, die nur auf Basis von öffentlichen zugänglichen Informationen evaluiert wurden.

GRC-Tools	ISO-Tools	GS-Tools	Doku-Tools	RM-Tools
Acuity STREAM *Acuity Risk Management*	ISAT-X *isec*	opus i *kronsoft*	i-doit *synetics*	Pilar *CCN*
ADAPTO *ADAPTO Solutions*	Risk27001 *Peter Pakosch*	SAVe® *INFODAS*	INDITOR® BSI *CONTECHNET*	RM Studio *Stiki*
CRISAM® Explorer *calpana business consulting*	ISMart *BIZnet*	sicherer IT-Betrieb *SIZ*		
DHC VISION ISMS *DHC Business Solutions*	ISMSbox *Ceyoniq Technology*	sidoc®-Sicherheits-management *2net® Carsten Lang*		
DocSetMinder® *GRC Partner*	ISO 27001 Toolkit *provensec*	verinice. *SerNet*		
ibi systems iris *ibi systems*	Proteus®GRCyber™ *Proteus-Cyber*			
GRC Toolbox PRO *Swiss Infosec*	TRICK Service *itrust consulting*			
Hiscout ISM & ISMS4ENERGY *HiScout*	vsRISK *Vigilant Software*			
QSEC *Wüpper Mgt. Consulting*				
R2C_ISMS *Schleupen*				
risk2value *avedos GRC*				
S&L Compliance Suite *S&L Firmengruppe*				

Tab. 2: Überblick über ISMS-Tools

4 Ergebnisse der Marktstudie

Im Folgenden werden die Ergebnisse der Marktstudie sowie die zugrundeliegenden Standard-Anforderungen (A) an ISMS-Tools vorgestellt. Die Anforderungen wurden von den einzelnen Prozessschritten und Aufgaben des ISO27-SP abgeleitet und unter Zuhilfen-

ahme von Standardliteratur im ISMS-Kontext konkretisiert (Vgl. [HH16b]) Die Darstellung der Marktstudienergebnisse erfolgt entlang der Plan-, Do-, Check- und Act-Phase des ISO27-SP. Ergänzend finden sich in den Unterkapiteln fünf und sechs prozessübergreifende sowie allgemeine Anforderungen und die jeweiligen Analyseergebnisse zu den betrachteten ISMS-Tools.

4.1 Anforderungen in der Plan-Phase

Innerhalb der Planungsphase des ISO27-SP werden zunächst Rahmenbedingungen und strategische Aspekte des ISMS definiert (z.B. ISMS-Scope und ISMS-Ziele). ISMS-Tools sollten dazu eine **A1: Stammdatenverwaltung** bereitstellen, innerhalb derer insb. Aufbau- und Ablauforganisation sowie ISMS-Assets gepflegt werden können. Keine Punkte in dieser Kategorie erhielten ausschließlich Werkzeuge, die nicht weitergehend analysiert werden konnten. Alle anderen Werkzeuge verfügen über die geforderte Funktionalität, unterscheiden sich jedoch deutlich in der Ausgestaltung. So unterstützen z.B. einige Vertreter der GS-und Doku-Tools lediglich die Verwaltung von klassischen IT-Assets und stellen keine Möglichkeiten zur Verwaltung von Prozessen und Personal-Assets zur Verfügung.

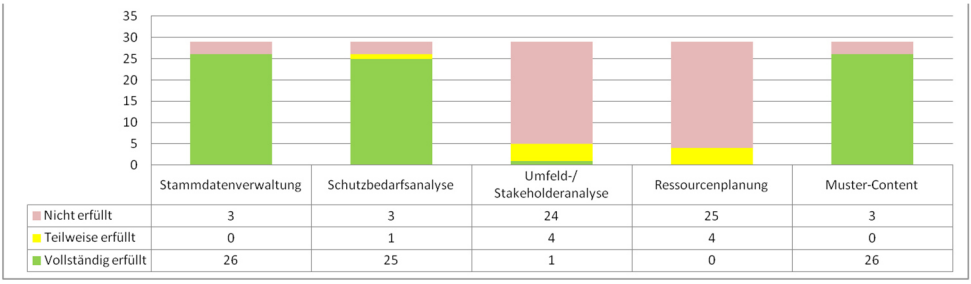
Ebenfalls Teil der Planungsphase des ISO27-SP ist die Bewertung der Schutzbedarfe einzelner ISMS-Assets. Nahezu alle untersuchten Tools unterstützen die **A2: Schutzbedarfsanalyse**, in dem sie bereits innerhalb der Stammdatenverwaltung Datenfelder zur den Schutzzielen bereitstellen. Lediglich i-doit stellt dieses Feature bislang in einem anderen Modul dar, welches zusätzlich zum ISO 27001 Modul erworben werden muss. Die verbleibenden Werkzeuge, die mit null Punkten in dieser Kategorie bewertet wurden, konnten mangels Informationen nicht weitergehend analysiert werden.

Bei der Definition des ISMS-Scope sind die internen und externen Rahmenbedingungen der Organisation zu berücksichtigen. Die dafür erforderliche **A3: Umfeld- und Stakeholder-Analyse** unterstützen jedoch nur ausgewählte ISMS-Tools. Lediglich CRISAM® Explorer, ibi systems iris, ISO 27001 Toolkit und opus i bieten Datenfelder oder Notizbereiche an, um die Ergebnisse dieser Analyse zu verwalten. DocSetMinder® erhielt in dieser Kategorie die volle Punktzahl, da die Erfassung und Interpretation von externen und internen Anforderungen explizit gefordert und unterstützt wird.

Zur Unterstützung bei der Planung und Ausgestaltung der ISMS-Organisation und der Ermittlung der erforderlichen ISMS-Ressourcen sollten die ISMS-Tools Funktionalitäten für **A4: Ressourcenplanung** bereitstellen. Diese Funktionalität wird jedoch von keinem der untersuchten Werkzeuge unterstützt. Lediglich vier der untersuchten ISMS-Tools, darunter CRISAM® Explorer, ibi systems iris , HiScout ISM & ISMS4Energy und ISO 27001 Toolkit, stellen rudimentäre Datenfelder oder Notizbereiche zur Verfügung, innerhalb derer Ressourcen, ggf. erforderliche Skills und/oder die Ressourcenausstattung qualitativ erläutert werden können.

Im Zuge der Planung und Vorbereitung der operativen Aufgaben in Do-, Check- und Act-

Phase des ISO27-SP werden Richtlinien, Prozessbeschreibungen, Templates und weitere Vorlagen erstellt. ISMS-Tools können diese Aufgaben durch Bereitstellung von **A5: Muster-Content** deutlich vereinfachen. Alle untersuchten Werkzeuge halten in diesem Zusammenhang beispielsweise generische Bedrohungs- und Maßnahmenkataloge bereit und stellen vereinzelt auch exemplarische Arbeitsanweisungen und Richtlinien zur Verfügung. Lediglich Werkzeuge, die nicht weitergehend untersucht werden konnten, erhielten in dieser Kategorie null Punkte.



	Stammdatenverwaltung	Schutzbedarfsanalyse	Umfeld-/ Stakeholderanalyse	Ressourcenplanung	Muster-Content
Nicht erfüllt	3	3	24	25	3
Teilweise erfüllt	0	1	4	4	0
Vollständig erfüllt	26	25	1	0	26

Abb. 1: Anforderungen der Plan-Phase

4.2 Anforderungen in der Do-Phase

Innerhalb der Do-Phase des ISO27-SP sind die Informationssicherheitsrisiken zu identifizieren und zu analysieren. Alle betrachteten Tools unterstützen diese Aufgabe durch systemseitige Möglichkeiten zur **A6: Risikobeurteilung**. Einige Vertreter der GS- und Doku-Tools liefern hierfür jedoch nur eingeschränkte Funktionalitäten, da die Risikobewertung im jeweiligen Kontext von untergeordneter Bedeutung ist.

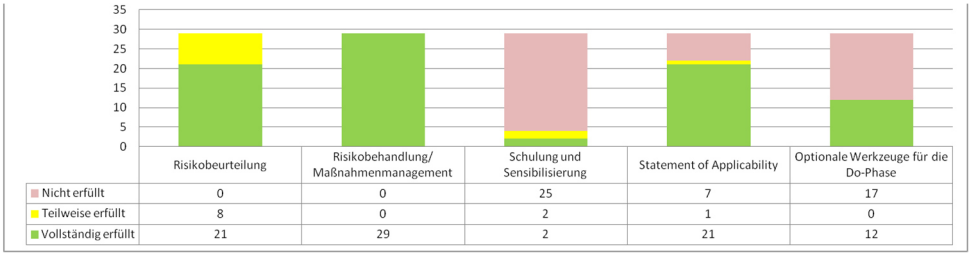
Im Anschluss zur Risikobeurteilung sind Maßnahmen für die Risikobehandlung zu definieren und zu initiieren, die in einem Maßnahmenplan überwacht werden müssen. Die erforderlichen Funktionalitäten für das **A7: Maßnahmenmanagement** stellen alle analysierten ISMS-Tools zur Verfügung.

Maßnahmen zur **A8: Schulung und Sensibilisierung** sind ebenfalls der Do-Phase des ISO27-SP zuzuordnen. Diese Aufgaben werden jedoch nur von Hiscout ISM & ISMS4ENERGY und Proteus®GRCyber™ unterstützt. Ibi systems iris und GRC Toolbox PRO bieten durch ihre hohe Flexibilität jedoch grundsätzlich die Möglichkeit, eigene Wissensbereiche mit Schulungs- und Sensibilisierungsinhalten anzulegen. Diese müssen jedoch eigenständig konzipiert und implementiert werden.

Den geforderten Abgleich der initiierten Maßnahmen zum Anhang A der ISO 27001 in Form einer **A9: Anwendbarkeitserklärung** unterstützen nicht alle Werkzeuge. Aufgrund ihrer Grundschutznatur fehlt dieses Feature beispielsweise INDITOR® BSI, SAVe® und sidoc®-Sicherheitsmanagement und auch i-doit ermöglicht die Erstellung der Anwend-

barkeitserklärung nur über Umwege. Die weiteren Werkzeuge ohne Punkte in diesem Bereich konnten mangels Informationen nicht vertieft analysiert werden.

Da die einzelnen Sicherheitsmaßnahmen sehr unterschiedlich ausgeprägt sein können, wurden keine weiteren Standard-Anforderungen zur Unterstützung der Do-Phase definiert. Dennoch stellen einige der untersuchten ISMS-Tools weitere optionale Funktionalitäten bereit, die zur Unterstützung dieser Phase geeignet sind. So finden sich beispielsweise Module und Funktionalitäten zur Unterstützung des IT-Notfall- und Exception Managements, Möglichkeiten zur Unterstützung des Software- & Lizenzmanagements sowie zur Gestaltung von FAQ-Bereichen und Gewinnspielen bis hin zu Werkzeugen, die die Verwaltung von Betriebs- und Organisationshandbüchern unterstützen.



	Risikobeurteilung	Risikobehandlung/ Maßnahmenmanagement	Schulung und Sensibilisierung	Statement of Applicability	Optionale Werkzeuge für die Do-Phase
Nicht erfüllt	0	0	25	7	17
Teilweise erfüllt	8	0	2	1	0
Vollständig erfüllt	21	29	2	21	12

Abb. 2: Anforderungen der Do-Phase

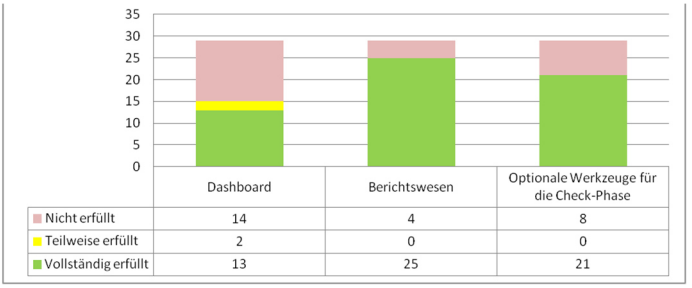
4.3 Anforderungen in der Check-Phase

Während der Check-Phase des ISO27-SP sind die Wirksamkeit des ISMS zu überprüfen und das tatsächliche Sicherheitslevel zu überwachen. Das in diesem Kontext erforderliche **A11: Berichtswesen** unterstützen alle untersuchten Werkzeuge. Die Möglichkeiten zur Konfiguration der Reports sind jedoch unterschiedlich ausgeprägt. Während einige Werkzeuge lediglich mit Standard-Reports aufwarten, liefern andere, insb. im GRC-Umfeld angesiedelte Werkzeuge ausgereifte Report-Generatoren, die Auswertungen über die gesamte Datenbank ermöglichen. Keine Punkte in dieser Kategorie erhielten lediglich die nicht weiterführend analysierten Werkzeuge.

Um dem ISMS-verantwortlichen Management einen möglichst raschen und umfassenden Überblick über das ISMS zu geben, sollten die ISMS-Tools außerdem **A10: Dashboards** bereitstellen. Über diese Funktionalität verfügen allerdings nur etwa die Hälfte der untersuchten Werkzeuge. Die Möglichkeiten zur Dashboard-Ausgestaltung reichen von statisch vorgegebenen bis hin zu frei konfigurierbaren Ansichten und Inhalten.

Aufgrund der Heterogenität und Vielfalt von operativen Check-Maßnahmen, wurden keine weiten Standard-Anforderungen zur Unterstützung dieser Phase definiert. Dennoch stellt die Mehrheit der ISMS-Tools weitere Funktionalitäten zur Unterstützung der Kontrollaufgaben zur Verfügung. So finden sich beispielsweise Funktionalitäten für das

Security Incident Management, die Durchführung von Self Assessments, Gap- und Reifegradanalysen sowie Audits, die Verwaltung von internen Kontrollen und Kennzahlen, die Unterstützung des Compliance Managements bis hin zu Möglichkeiten des Echtzeit-Monitorings einzelner IT-Komponenten.



	Dashboard	Berichtswesen	Optionale Werkzeuge für die Check-Phase
Nicht erfüllt	14	4	8
Teilweise erfüllt	2	0	0
Vollständig erfüllt	13	25	21

Abb. 3: Anforderungen der Check-Phase

4.4 Anforderungen in der Act-Phase

Innerhalb der Act-Phase werden die Verbesserungs- und Korrekturmaßnahmen zum ISMS festgelegt. Häufig erfolgt dies in der Praxis jedoch nicht auf Basis eines standardisierten Vorgehens, sodass auf die Definition von Standard-Anforderungen an ISMS-Tools in diesem Kontext verzichtet wurde. Die Marktstudie verdeutlichte ebenfalls, dass nur wenige systematische Ansätze zur Unterstützung dieser Phase existieren. So stellen beispielsweise DHC VISION ISMS, DocSetMinder®, verinice. und opus i Datenfelder zur Erfassung von qualitativ zu beschreibenden Verbesserungs- und Korrekturmaßnahmen bereit. GRC Toolbox PRO und HiScout ISM & ISMS4Energy erlauben durch ihre hohe Flexibilität außerdem die Erstellung von zusätzlichen Wissensbereichen (z.B. Wikis) und das Werkzeug ISMart wirbt mit einem integrieten Recommender- und Feedback-System zur Unterstützung der Act-Phase. Diese Funktionalität wurde jedoch lediglich der öffentlich zugänglichen Dokumentation entnommen und nicht evaluiert.

4.5 Übergreifende ISMS-fachliche Anforderungen

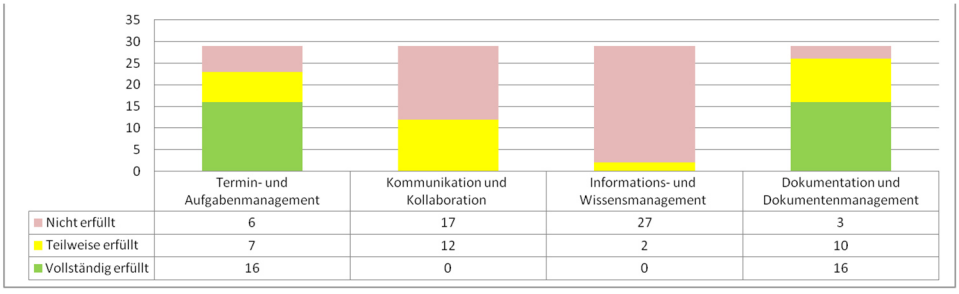
Über alle Phasen des ISO27-SP hinweg entstehen Querschnitts-Tätigkeiten, die durch ganzheitlich orientierte ISMS-Tools unterstützt werden sollten. Das übergreifende **A12: Termin- und Aufgabenmanagement** wird von etwa der Hälfte der Werkzeuge durch entsprechende Datenfelder und konfigurierbare Sichten auf die zugrundeliegende Datenbank unterstützt. Einigen Werkzeugen mangelt es jedoch an diesen übergeordneten Termin- und Aufgabensichten. Stattdessen geben sie lediglich durch Aufrufen der Einzelmaßnahmen konkretere Informationen zu Terminen, Verantwortlichen uund Inhalten preis.

Da die einzelnen Aufgaben des ISO27-SP i.d.R. nicht durch eine einzelne Person bearbei-

tet werden, sind Möglichkeiten zur **A13: Kommunikation und Kollaboration** von besonderer Bedeutung für die Funktionsfähigkeit des ISMS. Dennoch unterstützen weniger als die Hälfte der untersuchten ISMS-Tools diesen Aufgabenbereich. Häufig handelt es sich um Expertensysteme, deren Oberfläche und Usability bereits deutlich machen, dass lediglich eine zentral gesteuerte Datenerfassung und -verwaltung durch ISMS-Verantwortliche vorgesehen ist. Einige Werkzeuge bieten jedoch vereinzelte Unterstützungsmöglichkeiten im Bereich der kollaborativen Text- und Richtlinienerstellung an (z.B. CRISAM® Explorer, DHC VISION ISMS, DocSetMinder®, GRC Toolbox PRO). Andere ISMS-Tools stellen verschiedene Kommunikationswerkzeuge wie z.B. Chatfuntion (SAVe®), Kommentarfunktionen (risk2value) oder ein Nachrichtenmodul (z.B. ibi systems iris) zur Verfügung.

Selten bis gar nicht vertreten sind ISMS-Tools, die Unterstützungsmöglichkeiten für das ISMS-bezogene **A14: Informations- und Wissensmanagement** anbieten. Obwohl beide Disziplinen für den Aufbau und die kontinuierliche Verbesserung des ISMS von besonderer Bedeutung sind, stehen innerhalb der ISMS-Tools keine Funktionalitäten hierfür bereit. Allenfalls GRC Toolbox PRO und HiScout ISM & ISMS4Energy erlauben durch ihre hohe Flexibilität die Erstellung zusätzlicher Informations- & Wissensbereiche, die jedoch individuell designed und implementiert werden müssen.

Die **A15: Dokumentation und das Dokumentenmanagement** im ISMS-Kontext werden von der Mehrheit der untersuchten Werkzeuge unterstützt. Durch integrierte Dokumentenmanagementsysteme oder Funktionalitäten zur Verlinkung von Dokumentationen auf Fileshares kann i.d.R. ein guter Überblick über das ISMS generiert werden. Keine Punkte in dieser Kategorie erhielten lediglich Werkzeuge, die nicht weitergehend analysiert werden.



	Termin- und Aufgabenmanagement	Kommunikation und Kollaboration	Informations- und Wissensmanagement	Dokumentation und Dokumentenmanagement
Nicht erfüllt	6	17	27	3
Teilweise erfüllt	7	12	2	10
Vollständig erfüllt	16	0	0	16

Abb. 4: Übergeordnete ISMS-fachliche Anforderungen

4.6 Allgemeine Anforderungen

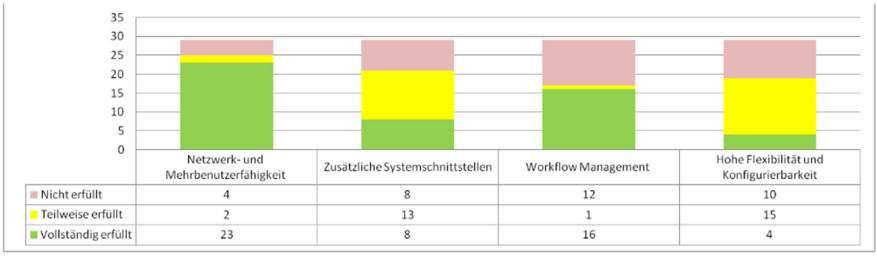
Da die einzelnen Aufgaben des ISO27-SP i.d.R. durch eine dezentrale ISMS-Organisation bearbeitet werden, zählen **A16: Netzwerk- und Mehrbenutzerfähigkeit** zu den allgemeinen Anforderungen an ISMS-Tools, die ebenfalls durch die Mehrheit der Werkzeuge

erfüllt werden. Lediglich PILAR und sidoc®-Sicherheitsmanagement waren zum Zeitpunkt der Überprüfung nicht netzwerkfähig.

Um weitere ISMS-relevante Systeme anbinden zu können, sollten die ISMS-Werkzeuge außerdem über **A17: Schnittstellen** verfügen. Über die klassischen Import-/Export sowie LDAP- und AD-Schnittstellen hinaus, verfügen jedoch nur ausgewählte Werkzeuge über weitere Schnittstellen. So erlauben beispielsweise i-doit und verinice. die Anbindung von Monitoringwerkzeugen und auch QSEC wirbt damit, individuell konfigurierbare Schnittstellen zu besitzen. Über generische Schnittstellen, z.B. zur Anbindung von Sharepoint oder CMDB verfügen CRISAM® Explorer, ibi systems iris, risk2value, HiScout ISM & ISMS4Energy und INDITOR® BSI.

Technologie für das **A18: Workflow Management** ist in ca. der Hälfte der untersuchten ISMS-Tools enthalten. In der Regel unterstützen diese Werkzeuge die Zuweisung von einzelnen Aktivitäten zu Nutzern und bieten Workflow-Support für deren Benachrichtigung und ggf. Freigabeaktivitäten an. Hervorzuheben ist der neuartige Ansatz von QSEC zu Kollaborationsworkflows (Wizard-Technologie), die die verschiedenen dezentralen und ISMS-relevanten Analysen prozessual abbilden und workflowseitig unterstützen.

Die methodischen Freiräume, die zu den wesentlichen Vorteilen der Norm zählen, erlauben es den Unternehmen, eigene Ansätze und Verfahren zu entwickeln und unternehmensspezifische Begrifflichkeiten im ISMS-Kontext zu benutzen. Die entsprechende systemseitige **A19: Flexibilität und Konfigurierbarkeit** bieten jedoch nur wenige ISMS-Tools an. Häufig sind logische Abläufe vordefiniert und lassen sich allenfalls in einzelnen Attributen customizen. Lediglich einige Vertreter aus dem Bereich der GRC-Tools sind modular und flexibel genug aufgebaut, um die logisch-inhaltliche Anpassung einzelner Funktionalitäten zu unterstützen (darunter ibi systems iris, GRC Toolbox PRO, HiScout ISM & ISMS4Energy und risk2value).



	Netzwerk- und Mehrbenutzerfähigkeit	Zusätzliche Systemschnittstellen	Workflow Management	Hohe Flexibilität und Konfigurierbarkeit
Nicht erfüllt	4	8	12	10
Teilweise erfüllt	2	13	1	15
Vollständig erfüllt	23	8	16	4

Abb. 5: Allgemeine Anforderungen

5 Gesamtübersicht und Darstellung der Top4

Die untersuchten ISMS-Tools wurden entlang von 19 Standard-Anforderungen hinsichtlich ihres Unterstützungspotentials für den ISO27-SP analysiert. Durch Kumulation der

erzielten Punkte ergibt sich die Gesamtübersicht in Abbildung 6. Auf der X-Achse wurden die erzielten Punkte im Bereich der Standard-Anforderungen kumuliert. Auf der Y-Achse wurden Zusatzpunkte für Werkzeuge mit ergänzenden Funktionalitäten und Modulen zur Unterstützung der Do-, Check- und Act-Phase des ISO27-SP kumuliert. Für 1 bis 2 zusätzliche Funktionalitäten erhielten die ISMS-Tools jeweils einen Extrapunkt und bei mehr als zwei zusätzlichen Features wurden zwei Extrapunkte vergeben. Die nachstehende Darstellung verdeutlicht damit sowohl die Platzierungen der einzelnen Werkzeuge in Bezug auf die definierten Standard-Anforderungen als auch die Potentialträger mit weiteren Nutzungsmöglichkeiten.

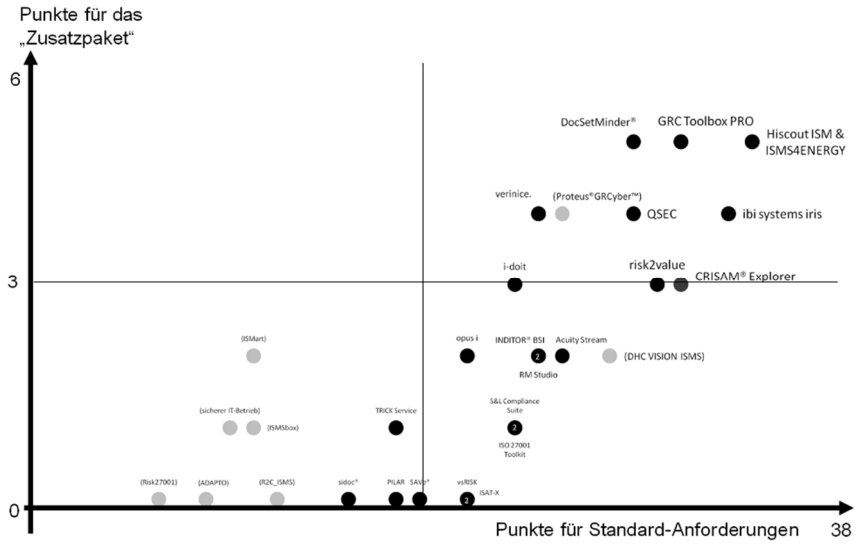


Abb. 6: Gesamtsicht nach Punkten

Zu den vier erstplatzierten Werkzeugen in Bezug auf die untersuchten Standard-Anforderungen zählen CRISAM® Explorer, ibi systems iris, GRC Toolbox PRO und HiScout ISM & ISMS4Energy. Die ISMS-Tools erhielten zwischen 30 bis 33 von 38 möglichen Punkten und sind damit in hohem Maße geeignet, den ISO27-SP zu unterstützen. Keines der betrachteten Werkzeuge erfüllt jedoch alle der für den ISO27-SP relevanten Standard-Anforderungen (Vgl. Tabelle 3). Mithilfe der nachfolgenden Spinnendiagramme werden zusammenfassend die einzelnen Stärken und „Leistungslücken“ der Top4 Werkzeuge verdeutlicht.

#	Anforderung	#	Anforderung
A1	Stammdatenverwaltung	A11	Berichtswesen
A2	Schutzbedarfsanalyse	A12	Termin- und Aufgabenmanagement
A3	Umfeld-/ Stakeholderanalyse	A13	Kommunikation und Kollaboration
A4	Ressourcenplanung	A14	Informations- & Wissensmanagement

A5	Muster-Content	A15	Dokumentation & Dokumentenmgt.
A6	Risikobeurteilung	A16	Netzwerk- und Mehrbenutzerfähigkeit
A7	Maßnahmenmanagement	A17	Zusätzliche Systemschnittstellen
A8	Schulung und Sensibilisierung	A18	Workflow Management
A9	Anwendbarkeitserklärung	A19	Flexibilität & Konfigurierbarkeit
A10	Dashboard		

Tab. 1: Übersicht der Anforderungen

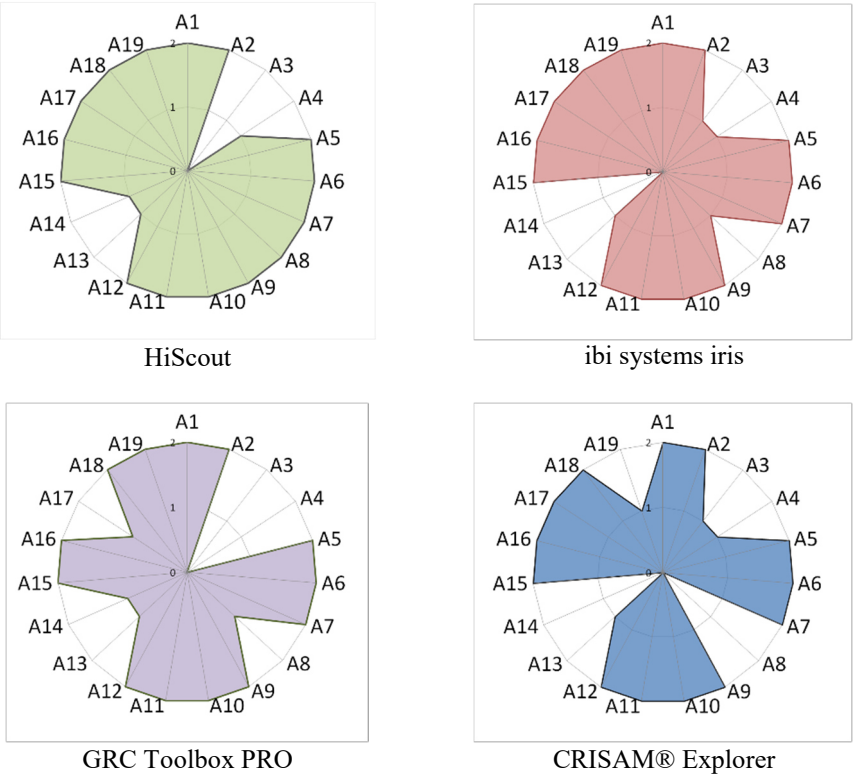


Abb.7: Die Top4 im Überblick

6 Zusammenfassung und Fazit

Die vorliegende Markstudie gibt einen Überblick über 29 verschiedene ISMS-Tools und zeigt deren Eignung zur Unterstützung des ISO27-SP auf. Damit erhalten ISMS-Praktiker und Forschungsgruppen einen umfassenden Überblick über verfügbare ISMS-Tools und einen Einblick in das Leistungsspektrum der Werkzeuge. Zu den Limitationen der Studie zählen insbesondere der Erhebungszeitpunkt der Daten, die

gewählten Suchbegriffe, sowie die vorgenommenen Eingrenzungen bei der Auswahl der zu analysierenden Werkzeuge. Dies führt zu einer eingeschränkten Sicht auf die aktuelle Marktsituation. Dennoch verdeutlicht die Studie, dass nur wenige Werkzeuge verfügbar sind, die den nativen ISMS-Betrieb ganzheitlich unterstützen. Außerdem erhält der Leser eine Indikation zu den Stärken und Schwächen einzelner ISMS-Tools. Dadurch kann die Studie beispielsweise als Grundlage zur Weiterentwicklung der Werkzeuge genutzt werden und zu einem verkürzten Software-Auswahlprozess im Unternehmen beitragen.

Literaturverzeichnis

[BV15] Bitkom; VKU: Praxisleitfaden IT-Sicherheitskatalog, Anforderungen an die IT für den sicheren Betrieb von Energieversorgungsnetzen (2015).

[Br09] Vom Brocke, J. et.al.: Reconstructing the giant: On the importance of rigour in documenting the literature search process. 17th European Conference on Information Systems (2009).

[CS15] CSC: GSTOOL QUO VADIS? Evaluation von Information Security Management System Tools als Grundschutz Tool Alternativen (2015).

[HH16a] Hofmann, M.; Hofmann, A.: Der ISO27-Sicherheitsprozess: Ein Referenzprozess zur Umsetzung der ISO/ IEC 27001. Multikonferenz Wirtschaftsinformatik (2016)

[HH16b] Hofmann, M.; Hofmann, A.: Anforderungen an eine IT-Lösung für den ISO27-Sicherheitsprozess. DACH Security (2016)

[WP12] Windhorst, I.; Pirzer, B.: Managementsysteme für Informationssicherheit: Marktübersicht. Vorgehensmodell. Handlungsempfehlungen. Fraunhofer Research In-stitution AISEC (2012).