Anforderungen an eine IT-Lösung für den ISO27-Sicherheitsprozess

Marlen Hofmann · Andreas Hofmann

CISO27
{marlen.hofmann | hofmann.andreas1}@gmail.com

Zusammenfassung

Steigende Bedeutung von Informationssicherheit und neue gesetzliche Anforderungen motivieren Unternehmen nahezu aller Branchen zur Einführung eines Informationssicherheitsmanagementsystems (ISMS) gemäß den Anforderungen der DIN ISO/IEC 27001 (ISO 27001). Da es der Norm jedoch an Prozessorientierung mangelt, müssen die wiederkehrenden Aktivitäten für den Betrieb des ISMS zunächst definiert und strukturiert werden. In einem ersten Schritt wurde dazu bereits der ISO27-Sicherheitsprozess (ISO27-SP) entwickelt, welcher explizit die Anforderungen und Prioritäten der ISO 27001 abbildet und somit als Pendant zum Sicherheitsprozess nach IT-Grundschutz Vorgehensweise des Bundesamtes für Sicherheit in der Informationstechnik (BSI) angesehen werden kann. Im Rahmen dieses Beitrags wird der ISO27-SP auf Basis einer Literaturanalyse um konkrete einzelne Aktivitäten und methodische Hinweise angereichert und anschließend generische Anforderungen zur deren IT-seitiger Unterstützung abgeleitet. In weiteren Forschungsiterationen sollen diese Anforderungen bei der Konzeption und Entwicklung der IT-Lösung "CISO27-Suite" berücksichtigt werden, welche den ISO27-SP ganzheitlich implementiert und mithilfe derer die Unternehmen zukünftig "by Design" ein normkonformes, natives ISMS aufbauen und betreiben können.

1 Darstellung des Forschungsvorhabens CISO27

Steigende Bedeutung von Informationssicherheit im Allgemeinen 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) [BiVk15]. Da es der Norm jedoch an Prozessorientierung mangelt und sich die (zwischenzeitlich obsoleten [Jend14]) Umsetzungshinweise aus der DIN ISO/IEC 27003 insbesondere auf die projekthafte Einführung des ISMS beziehen, müssen die wiederkehrenden Aktivitäten für den späteren ISMS-Betrieb zunächst definiert und strukturiert werden. Bislang gibt es hierfür keine standardisierten Abläufe, sodass die ISMS-Praktiker sich entweder eigene ISMS-Prozesse entwerfen oder auf bereits bestehende Ansätze, wie z.B. den Sicherheitsprozess nach IT-Grundschutz Vorgehensweise [BSI100-2] des Bundesamt für Sicherheit in der Informationstechnik (BSI) oder die Vorgehensweise "ISIS12" des Netzwerks für Informationssicherheit im Mittelstand zurück greifen müssen. Da die bestehenden Ansätze jedoch i.d.R. anders gelagerte ISMS-Anforderungen aufweisen oder den einzelnen ISMS-Aktivitäten unterschiedliche Bedeutung und Priorität beimessen, kann eine unreflektierte Übernahme der prozessualen und methodischen Vorgaben zu Brüchen, Inkonsistenzen und Irritationen in einem nativen ISMS-Vorgehen führen und dadurch den fortlaufenden ISMS-Betrieb in der Praxis erschweren [HoHo16].

P. Schartner (Hrsg.) · D•A•CH Security 2016 · syssec (2016) 24-35.

Durch das Fehlen eines ISO 27001-konformen Referenzprozesses und des daraus resultierenden mangelnden Standardisierungsgrades der ISMSe in der Praxis, kann es aus Sicht der Autoren auch bislang keine adäquaten und standardisierten IT-Lösungen zur ganzheitlichen Unterstützung eines nativen ISMS geben – wenngleich auch eine Vielzahl von Tool-Anbietern genau damit wirbt. Bei genauerem Analysieren wird jedoch schnell offensichtlich, dass die am Markt verfügbaren Werkzeuge entweder an den Sicherheitsprozess des BSI angelehnt sind oder nur einige wenige, weitläufig bekannte, wiederkehrende ISMS-Aktivitäten (wie z.B. Risiko- und Assetmanagement oder die Verwaltung von Dokumenten) unterstützen [WiPi12, CSC15]. Sowohl die Unsicherheit über die tatsächlich erforderlichen Aktivitäten im ISMS-Betrieb als auch die bestehende Intransparenz über das tatsächliche Leistungsspektrum der ISMS-Tools führt dazu, dass sich die Unternehmen häufig mit selbst erstellten Word-Templates und Excel-Tools zur Unterstützung ihres ISMS behelfen [HoHo16]. Derartige Werkzeuge zur individuellen Datenverarbeitung sind jedoch fehleranfällig, zum Teil unübersichtlich, resp. schwer zu bedienen und bieten nur wenige Möglichkeiten, den einzelnen Mitarbeiter strukturiert bei der Erfüllung seiner Aufgaben und der übergreifenden Kollaboration mit anderen ISMS-Beteiligten zu unterstützen. Darüber hinaus ist der Aufwand zur Konsolidierung und Qualitätssicherung der dezentral erzeugten Daten immens und eine Weiter- und Wiederverwendung der Ergebnisse nahezu unmöglich [Kozl13, SaDi16, HoHo16].

Das Forschungsvorhaben CISO27 adressiert die skizzierten konzeptionellen und praktischen Probleme des ISMS-Betriebs und zielt darauf ab, einen Informationssicherheitsprozess und eine dazu passende, adäquate IT-Lösung zu entwickeln, mithilfe derer die Unternehmen zukünftig "by Design" ein transparentes, natives ISMS aufbauen und betreiben können. In einem ersten Schritt entstand dazu bereits der ISO27-Sicherheitsprozess (ISO27-SP), welcher als Pendant zu dem, im BSI Grundschutzstandard [BSI100-1] vorgestellten Sicherheitsprozess angesehen werden kann. Der neuartige Referenzprozess gibt erstmals einen Überblick über die notwendigen Prozessschritte für einen normkonformen ISMS-Betrieb und zeigt deren Abarbeitungsreihenfolge auf (vgl. [HoHo16]). Im Rahmen dieses Beitrags werden der ISO27-SP auf Basis einer Literaturanalyse um konkrete einzelne Aktivitäten und methodische Hinweise ergänzt und Unterstützungsmöglichkeiten sowie IT-Anforderungen an ein ISMS-Tool zur Unterstützung des Referenzprozess abgeleitet. Der Beitrag ist dazu wie folgt strukturiert: im nächsten Abschnitt findet sich eine überblicksartige Darstellung des ISO27-SP in seiner aktuellen Fassung, die anschließend um konkrete Aktivitäten und methodische Vorgaben aus der Literaturanalyse erweitert wird. Die Ableitung der IT-seitigen Anforderungen findet sich in Kapitel drei. Der Beitrag endet mit einer kurzen Zusammenfassung und dem Ausblick auf die anstehenden Forschungsschritte.

2 Erweiterung des ISO27-Sicherheitsprozess

Der generisch gehaltene ISO27-SP (vgl. [HoHo16]) folgt in seiner Grundstruktur einem typischen PDCA Zyklus. Der Prozess wird durch insgesamt 10 Prozessschritte konkretisiert, die zur Aufrechterhaltung eines effektiven ISMS wiederkehrend zu durchlaufen sind (ISMS-Betrieb). Innerhalb der Planungsphase des ISO27-SP werden die Grundsteine für jeden neu gestarteten Zyklus gelegt. In diesem Rahmen sind Vorgaben zu Informationssicherheitszielen (IS-Ziele), Anwendungsbereich (ISMS-Scope) und Informationssicherheitspolitik (IS-Politik) sowie ISMS-relevante Verfahren regelmäßig zu überprüfen und ggf. zu aktualisieren. Außerdem ist die wiederkehrende Durchführung der operativen ISMS-Aktivitäten für den anstehenden Prozesszyklus zu planen. In der Do-Phase werden durch die Mitarbeiter der ISMS-

Organisation die Aktivitäten zum Risikomanagement bearbeitet, Informationssicherheitsmaßnahmen (IS-Maßnahmen) initiiert sowie Schulungs- und Sensibilisierungsmaßnahmen durchgeführt. Anschließend sind die Wirksamkeit des ISMS und die Regelkonformität zu den ISMS-Vorgaben zu überprüfen (Check-Phase). Innerhalb der Act-Phase werden Verbesserungs- und Korrekturmaßnahmen festgelegt, sodass der ISO27-SP von neuem gestartet werden kann (vgl. Abbildung 1).

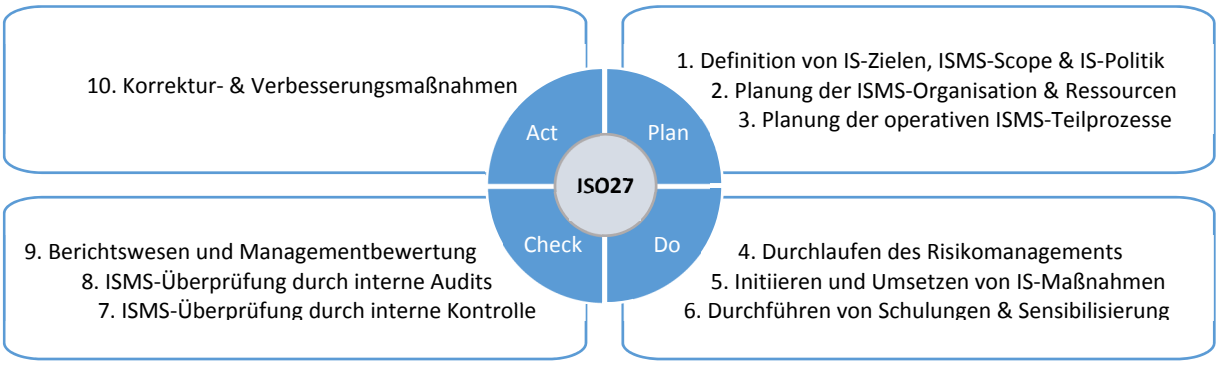

Abb. 1: Überblick über den ISO27-SP (vgl. HoHo16)

Auf Basis einer strukturierten Literaturanalyse [BSN+09] werden im Folgenden die noch sehr allgemein gehaltenen Prozessschritte des ISO27-SP durch einzelne Aktivitäten und methodische Vorgaben konkretisiert. In die Literaturanalyse wurden selektiv die Beiträge von [KeRS13, Hump16, ISO27003, BSI100-2] und [Müll14] einbezogen, mit dem Ziel eine Integration der darin beschriebenen Aktivitäten zum ISMS-Betrieb zu erreichen. Zur Zielgruppe des Beitrags zählen insbesondere ISMS-Praktiker und -Forschungsgruppen, sodass auf die Darstellung von ISMS-relevantem Grundlagenwissen verzichtet wird. Die Darstellung der Ergebnisse der Literaturanalyse erfolgt konzeptionell entlang der Prozessschritte des ISO27-SP und wertungsfrei. Die Zuordnung der identifizierten Aktivitäten zu den einzelnen Prozessschritten des Referenzprozess erfolgt sowohl induktiv auf Basis von eigenen Beobachtungen in der ISMS-Praxis als auch deduktiv durch theoretische Überlegungen zu den Anforderungen der Norm [Beck00].

3 Aktivitäten zum ISO27-Sicherheitsprozess

Prozessschritt P_1

Definition von IS-Zielen, ISMS-Scope und IS-Politik

P_1A_1: Initiierung des ISO27-SP: Das ISMS liegt in der Gesamtverantwortung der obersten Leitung einer Organisation. Ein entsprechender Management-Pate, z.B. der CIO oder CEO [Hump16], sollte daher den ISO27-SP initiieren und regelmäßig, spätestens jedoch alle 2 Jahre [BSI100-2] eine Überprüfung und ggf. eine Aktualisierung der IS-Politik, der IS-Ziele und des ISMS-Scope einfordern [ISO27003, BSI100-2, Hump16].

P_1A_2: Kick-Off im Management-Forum: Das ISMS erfordert die Mitwirkung von Führungskräften und deren Mitarbeitern. Zu Beginn eines jeden neuen ISO27-SP Zyklus empfiehlt es sich daher, ein ISMS-Management-Forum einzuberufen [ISO27003, KeRS13] und über Aktualisierungsbedarf an IS-Politik, IS-Zielen und ISMS-Scope sowie über anstehende operative ISMS-Aktivitäten und den dafür vorgesehenen Zeitplan zu informieren.

P_1A_3: Kick-Off in der ISMS-Expertenrunde: Im Nachgang zum Management-Forum sollten innerhalb einer ISMS-Expertenrunde (z.B. bestehend aus Fachverantwortlichen und Vertretern der Querschnittsbereiche) die ggf. neuen Vorgaben zum ISMS kommuniziert, fachliche als auch organisatorische Anforderungen diskutiert und Arbeitsaufträge an die jeweiligen Verantwortlichen übertragen werden [BSI100-2].

P_1A_4: Ermittlung der internen ISMS-Rahmenbedingungen: Um die Aktualität und Angemessenheit von IS-Politik, IS-Zielen und ISMS-Scope beurteilen und Änderungsbedarf feststellen zu können, sollten zunächst Aufbau- und Ablauforganisation des Unternehmens hinsichtlich ISMS-relevanter Veränderungen überprüft [ISO27003, KeRS13] und die Kritikalität der (ggf. neuen) Abteilungen und Prozesse mithilfe der Schutzbedarfsanalyse [BSI100-2] bestimmt werden.

P_1A_5: Ermittlung der externen ISMS-Rahmen-bedingungen: Neben den internen ISMS-Rahmenbedingungen sind weiterhin die externen Veränderungen im Unternehmensumfeld zu beleuchten [ISO27003, KeRS13, BSI100-2, Hump16, Müll14]. So lassen sich z.B. mit einer strukturierten Umfeldanalyse die wesentlichen (neuen) Kunden und Dienstleister, relevante Gesetze und die entsprechenden ISMS-relevanten Anforderungen identifizieren.

P_1A_6: Überprüfung und Aktualisierung der IS-Ziele und des ISMS-Scope: Die Analyse zu Veränderungen an internen und externen ISMS-relevanten Rahmenbedingungen kann Änderungsbedarf an IS-Zielen und ISMS-Scope aufzeigen. In jedem Falle sollten die (ggf. neuen) geschäftskritischen Abteilungen und Prozesse [BSI100-2], sowie alle Querschnittsbereiche des Unternehmens [KeRS13] und alle unterstützenden Informationswerte in den ISMS-Scope aufgenommen werden [ISO27003, Hump16]. Abgeleitet aus den Schutzbedarfsanforderungen (vgl. P1A4) lassen sich außerdem (ggf. veränderte) Vorgaben für die IS-Ziele festlegen [BSI100-2, Müll14] und der Weg zu deren Erreichung planen [ISO27003].

P_1A_7: Abstimmung von IS-Zielen und ISMS-Scope: Sollten sich die aktualisierten IS-Ziele und der ISMS-Scope zu früheren Vorgaben erheblich unterscheiden, empfiehlt es sich, die Veränderungen im ISMS-Management-Forum und der ISMS-Expertenrunde zu diskutieren und deren Eignung und Angemessenheit bestätigen zu lassen [ISO27003, BSI100-2].

P_1A_8: Aktualisierung und Inkraftsetzung der IS-Politik: Obgleich die IS-Politik einen sehr hohen Abstraktionsgrad aufweist und daher eher selten aktualisiert werden muss [KeRS13], sollten wesentliche Veränderungen an IS-Zielen und ISMS-Scope im Dokument schriftlich fixiert werden [ISO27003, Hump16, Müll14]. Die aktualisierte IS-Politik ist anschließend durch die oberste Leitung (erneut) freizugeben und verbindlich in Kraft zu setzen. Dieser Beschlussvorgang sollte mithilfe einer Entscheidungsvorlage [KeRS13] initiiert werden, welche nachweislich durch den Management-Paten (Vgl. P1A1) zu befürworten ist [ISO27003, BSI100-2, Hump16, Müll14].

P_1A_9: Kommunikation der IS-Politik: Nach Freigabe durch die oberste Leitung ist die aktualisierte IS-Politik den Mitarbeitern und interessierten Parteien bekannt zu machen [ISO27003, BSI100-2, Hump16].

Prozessschritt P_2

Planung der ISMS-Organisation & Ressourcen

P_2A_1: Überprüfung und Aktualisierung der ISMS-Rollen: Die Rollen innerhalb der ISMS-Organisation variieren z.B. aufgrund der Größe des Unternehmen, des Tätigkeitsfeldes sowie der Aufbau- und Ablauforganisation. Da sich diese Rahmenbedingungen verändern kön-

nen, sollten die ISMS-Rollen, die Rolleninhaber sowie die Rollenbeschreibungen regelmäßig hinsichtlich ihrer Vollständigkeit und Aktualität überprüft und ggf. aktualisiert werden [ISO27003, KeRS13, BSI100-2]. In diesem Zuge empfiehlt es sich auch, die rollenspezifischen Qualifikationsanforderungen und Qualifikationspläne zu überprüfen und ggf. zu überarbeiten [KeRS13, Hump16, Müll14].

P_2A_2: Überprüfung der Ressourcenausstattung: Um eine adäquate Ressourcenausstattung der ISMS-Organisation sicherzustellen [ISO27003], sollte mithilfe einer jährlichen Ressourcenplanung der Personalbedarf für den anstehenden ISO27-SP Zyklus überprüft werden [KeRS13]. Dabei ist nach organisatorischen und technischen Personalressourcen zu unterscheiden [BSI100-2].

P_2A_3: Freigabe der ISMS-Organisation: Die aktualisierte ISMS-Organisation und ggf. erforderliche, zusätzliche Ressourcen für den bevorstehenden ISO27-SP Zyklus sollten z.B. im Rahmen einer Entscheidungsvorlage dargestellt [KeRS13] und durch die oberste Leitung bestätigt und freigegeben werden [Hump16].

Prozessschritt P_3

Planung der operativen ISMS-Teilprozesse

P_3A_1: Überprüfung und Aktualisierung der Vorgaben zum Dokumentenmanagement: Die formalen und prozessualen Vorgaben zum Dokumentenmanagement (z.B. Dokumentenkennzeichnung und -lenkung) werden i.d.R. innerhalb des Qualitätsmanagementsystems beschrieben und aktualisiert [KeRS13]. Sollte dies nicht der Fall sein, müssen die Vorgaben und die inhaltlichen Dokumentationsanforderungen (z.B. zur ISMS-Pflichtdokumentation, -Protokollierung, -Aufzeichnung, etc.) im Rahmen des ISO27-SP regelmäßig überprüft und durch einen Änderungsprozess [BSI100-2] aktualisiert werden [ISO27003, KeRS13].

P_3A_2: Überprüfung, Aktualisierung und Planung des Risikomanagements: Ein zentrales Element des ISMS ist das Management von Informationssicherheitsrisiken (IS-Risiken). Innerhalb der Planungsphase des ISO27-SP sollten die zugrundeliegende Risikomanagement-Methode sowie relevante Informationssicherheitsrisikokriterien gemeinsam mit dem zentralen Risikomanagement des Unternehmens hinsichtlich ihrer Tauglichkeit und erforderlicher Anpassungen überprüft und ggf. aktualisiert werden. Außerdem sind die Ansprechpartner sowie Termine für das bevorstehende Risk Assessment abzustimmen und dieses inhaltlich vorzubereiten [ISO27003, KeRS13, BSI100-2, Hump16].

P_3A_3: Überprüfung und Planung von Schulungs- & Sensibilisierungsmaßnahmen: Mitarbeiterschulung und Sensibilisierung sind weitere zentrale Bestandteile des ISO27-SP. Die Vorgaben dazu werden i.d.R. in einem Schulungs- und Sensibilisierungsprogramm festgehalten, welches regelmäßig überarbeitet werden sollte. Die Planung der operativen Schulungsmaßnahmen sollte jährlich [KeRS13] erfolgen und auch die ISMS-Schulungsunterlagen sollten regelmäßig überprüft und ggf. überarbeitet werden [ISO27003, Hump16].

P_3A_4: Überprüfung und Planung von Überwachungsmaßnahmen: Die Überwachung, resp. Leistungsbewertung [Hump16] des ISMS erfolgt durch (1) operative interne Kontrollen und Monitoring-Prozesse, (2) interne Audits und (3) Berichtswesen und Managementbewertung. Um diese Aktivitäten innerhalb der Check-Phase durchführen zu können, sollten bereits zum Planungszeitpunkt des ISO27-SP die geltenden Vorgaben und Verfahren sowie organisatorische und technische Rahmenbedingungen überprüft und ggf. aktualisiert werden [ISO27003, KeRS13, BSI100-2, Hump16]. Da die internen Audits zum jährlichen Manage-

ment-Review vorgelagert durchgeführt werden, sollten außerdem bereits frühzeitig die erforderlichen Termine mit den jeweiligen Beteiligten koordiniert werden [ISO27003, KeRS13, Hump16].

Prozessschritt P_4

Durchlaufen des Risikomanagements

P_4A_1: Risiko-identifikation: Das Risk Assessment der IS-Risiken beginnt i.d.R. mit der Überprüfung, resp. Identifizierung von bereits bekannten sowie neuen IS-Risikoszenarien und der Ermittlung von bereits umgesetzten IS-Maßnahmen [ISO27003, Hump16].

P_4A_2: Risikoanalyse: Nach der Risikoidentifizierung folgt die Analyse der Risiken, d.h. die Abschätzung von Wahrscheinlichkeit und potentiellen Schaden sowie die Ermittlung des Risikolevels als Kombination beider Größen [ISO27003, KeRS13, Hump16].

P_4A_3: Risikobewertung: Anschließend sind die Risiken (erstmalig oder erneut) zu bewerten, indem sie mit den Informationssicherheitsrisikokriterien abgeglichen werden. Die Bewertung liefert Informationen, ob und welche IS-Risiken im Rahmen der Risikobehandlung weiter bearbeitet werden müssen und welche IS-Risiken ggf. vertieft analysiert werden sollten, um über eine Priorisierung und alternative Risikobehandlungsoptionen zu entschieden [ISO27003, KeRS13, Hump16].

P_4A_4: Auswahl Optionen zur Risiko-behandlung und IS-Maßnahmen: Auf Basis der Risikobewertung sind die Optionen zur Risikobehandlung auszuwählen (z.B. Risikoakzeptanz, -vermeidung, -reduzierung, etc.) und konkrete IS-Maßnahmen zur Steuerung der Risiken zu erarbeiten. Die ausgewählten IS-Maßnahmen sind außerdem mit den Controls aus Annex A der ISO 27001 abzugleichen, um sicherzustellen, dass keine wichtigen IS-Maßnahmen vergessen wurden [ISO27003, Hump16].

P_4A_5: Erstellung des Risikobehandlungsplans: Im Risikobehandlungsplan sind anschließend alle zur Implementierung ausgewählten IS-Maßnahmen mit Prioritäten, Umsetzungsfristen, Handlungsempfehlungen, etc. zu dokumentieren [ISO27003]. Sollten Risikobehandlungsoptionen und IS-Maßnahmen nicht zweifelsfrei bestimmt werden können, muss das Management über einen Entscheidungsprozess eingebunden werden [KeRS13, Hump16].

P_4A_6: Erstellung der Anwendbarkeits-erklärung: In Vorbereitung auf den Freigabeprozess des Risikobehandlungsplans ist die Anwendbarkeitserklärung zu erstellen. Sie gibt Auskunft darüber, welche und warum einzelne Controls aus Annex A der ISO 27001 ggf. nicht umgesetzt werden können oder sollen [ISO27003, Hump16].

P_4A_7: Freigabe von Risikobehandlungsplan und Anwendbarkeitserklärung: Der Teilprozess zum Risikomanagement endet mit der Freigabe von Risikobehandlungsplan und Anwendbarkeitserklärung durch die oberste Leitung der Organisation. In diesem Rahmen sind auch die Restrisiken nachweislich zu bestätigen und damit die Risikoakzeptanz zu bekunden [ISO27003, Hump16].

Prozessschritt P_5

Initiieren und Umsetzen von IS-Maßnahmen

P_5A_1: Umsetzen der IS-Maßnahmen: Gemäß Risikobehandlungsplan sind die technischen und organisatorischen IS-Maßnahmen zu konkretisieren und im Rahmen von Projekten oder Linientätigkeit zu implementieren. Die Bearbeitung der IS-Maßnahmen erfolgt damit außerhalb des ISO27-SP und wird i.d.R. nicht länger durch den Chief Information Security

Officer, resp. ein ISMS-Kernteam (ISMS-Zentralfunktion) gesteuert. Da die Maßnahmenumsetzung jedoch eine entscheidende Voraussetzung für ein wirksames ISMS ist, sollten Umsetzungsstand und Termintreue kontinuierlich und mithilfe eines zentralen Maßnahmenmanagements nachgehalten werden [ISO27003, KeRS13, Hump16].

Prozessschritt P_6

Durchführen von Schulungen & Sensibilisierung

P_6A_1: Durchführung von Schulungen und Trainings: Gemäß verabschiedetem Schulungsplan sind die Schulungen und praktischen Trainings (z.B. ISMS-Informationsveranstaltungen, Video-, Web- oder Computer Based Trainings, etc.) durchzuführen und zu dokumentieren [KeRS13, BSI100-2, Hump16, Müll14]).

P_6A_2: Mitarbeiter-Sensibilisierung: Weiterhin sind die geplanten (ggf. auch anlassbezogene) Sensibilisierungsmaßnahmen (z.B. Flyer, Poster, Wettbewerbe, Arbeitsplatzbegehungen, etc.) umzusetzen und zu dokumentieren [KeRS13, BSI100-2, Hump16, Müll14]).

Prozessschritt P_7

ISMS-Überprüfung durch interne Kontrollen:

P_7A_1: Überwachung der Informations-Sicherheitsleistung: Zur Überwachung der Informationssicherheit im engeren Sinne sind die geplanten internen Kontrollen und operativen Monitoring-Prozesse durchzuführen. Sie dienen der Frühwarnung und -erkennung [Müll14] sowie der Identifizierung, Analyse und Bewertung von aufgetretenen Schadensereignissen [KeRS13, BSI100-2, Hump16]. Anders wie die bisher beschriebenen Aktivitäten, sind die internen Kontrollen und Monitoring-Prozesse permanent (und nicht nur während der Check-Phase) auszuführen, resp. aufrecht zu erhalten.

P_7A_2: Überwachung der Leistungsfähigkeit des ISMS: Rechtzeitig vor dem internen Audit ist der Reifegrad, resp. die Wirksamkeit des ISMS zu überprüfen und zu dokumentieren [KeRS13, BSI100-2, Hump16]. In diesem Rahmen ist zu kontrollieren, ob und inwieweit die ISMS-Vorgaben eingehalten, die IS-Maßnahmen wirksam und die Korrektur- und Verbesserungsmaßnahmen aus früheren ISO27-SP Zyklen umgesetzt wurden [Hump16, Müll14, KeRS13, BSI100-2].

Prozessschritt P_8

ISMS-Überprüfung durch interne Audits

P_8A_1: Durchführen interner Audits und Erstellen des Audit-Berichts: Durch ISMS-unabhängige Mitarbeiter ist das interne Audit durchzuführen. Da die Auditierung i.d.R. einem eigenständigen Audit-Prozess (z.B. Vgl. DIN ISO/IEC 27006) außerhalb des ISO27-SP folgt, soll an dieser Stelle auf eine detailliertere Darstellung der einzelnen Aktivitäten verzichtet werden. Die Ergebnisse des Audits sind in Form eines Audit-Berichts oder -Protokolls festzuhalten [KeRS13].

Prozessschritt P_9

Berichtswesen und Managementbewertung

P_9A_1: Erstellung des Berichtswesens: Alle wichtigen Veränderungen im ISMS sowie ISMS-relevante Informationen aus dem ISO27-SP Zyklus (z.B. identifizierte Schwachstellen und Sicherheitsvorfälle, Ergebnisse des internen Audits, etc.) sind für die Managementbewertung zu konsolidieren und für das Berichtswesen aufzubereiten [ISO27003, KeRS13, BSI100-2, Hump16, Müll14].

P_9A_2: Durchführung Managementbewertung: Anschließend ist die Managementbewertung durchzuführen und zu dokumentieren. In einem gemeinsamen Termin mit der obersten Leitung sollten dazu alle wesentlichen ISMS-Beteiligten über mögliche Verbesserungswünsche und Korrekturmaßnahmen im ISMS beraten und dazu nachweisbare Festlegungen treffen [BSI100-2, Hump16].

Prozessschritt P_{10}

Korrektur- & Verbesserungsmaßnahmen

$P_{10}A_1$: Konzeption von Verbesserungsmaßnahmen: Die in der Managementbewertung und im Verlauf des ISO27-SP ermittelten Verbesserungsmöglichkeiten und -vorschläge dienen in der Act-Phase als Basis für die Konzeption von konkreten Verbesserungsmaßnahmen [ISO27003, KeRS13, BSI100-2, Hump16, Müll14].

$P_{10}A_2$: Konzeption von Korrekturmaßnahmen: Insbesondere die in der Check-Phase ermittelten Schwachstellen sowie aufgetretene Sicherheitsvorfälle und die Ergebnisse aus internem Audit und Managementbewertung sind weiterführend zu analysieren, um Korrekturmaßnahmen für den nächsten ISO27-SP Zyklus zu konzipieren [ISO27003, KeRS13, BSI100-2, Hump16, Müll14].

$P_{10}A_3$: Überführung in die Planungsphase: Sowohl Verbesserungs- als auch Korrekturmaßnahmen sind beispielsweise in Improvement-Plänen, Roadmaps oder Projektplänen zu dokumentieren [Hump16, Müll14] und an interne und externe Stakeholder zu kommunizieren. Sie bilden außerdem den Input für den nächsten ISO27-SP Zyklus [KeRS13], der regelmäßig von neuem zu initiieren ist.

4 IT-seitige Unterstützung des ISO27-SP

Abgeleitet aus den voranstehenden Aktivitäten des ISO27-SP werden im Folgenden aufgabenübergreifende und ISMS-fachliche IT-Anforderungen und -Unterstützungsmöglichkeiten aufgezeigt. Die Anforderungen sind nicht priorisiert und vernachlässigen sowohl rein technische Aspekte als auch Vorgaben zur Benutzerfreundlichkeit, da sich diese nicht explizit aus den prozessualen Vorgaben ableiten lassen und separat betrachtet werden sollten.

4.1 Aufgabenübergreifende IT-Anforderungen

Die voranstehende Darstellung des ISO27-SP offenbart eine Vielzahl von strategischen, administrativen und operativen Aktivitäten, die im Rahmen des ISMS-Betriebs zu bearbeiten sind. Um den ISO27-SP steuern zu können, muss die ISMS-Zentralfunktion den Überblick über die verschiedenen Aktivitäten behalten und deren termingerechte Fertigstellung überwachen. *Ein ISMS-Tool sollte demnach das Termin- und Aufgabenmanagement unterstützen* **(R1)**.

In den Betrieb des ISMS sind, je nach Unternehmensgröße und Definition des ISMS-Scope, eine Vielzahl von Führungskräften und Mitarbeitern eingebunden, die jeweils rollenspezifische Aktivitäten im ISO27-SP wahrnehmen, unterschiedliche Informationen bereitstellen oder Zugriff auf diese benötigen. *Entsprechend sollte eine IT-Lösung zur Unterstützung des ISO27-SP netzwerk- und mehrbenutzerfähig sein und über eine Nutzerverwaltung mit Rechtemanagement verfügen* **(R2)**.

Die einzelnen Aktivitäten des ISO27-SP werden i.d.R. durch dezentrale ISMS-Rolleninhaber und Mitarbeiter bearbeitet, die durch die ISMS-Zentralfunktion koordiniert werden. In Abhän-

gigkeit von der Anzahl der Prozessbeteiligten kann diese Aktivität zu einer komplexen Herausforderung anwachsen, die ohne methodische und technische Unterstützung nicht zu bewältigen ist. *Ein ISMS-Tool sollte daher die Allokation und Koordination von Ressourcen unterstützen und eine Workflow-gestützte Ausführung der Aktivitäten erlauben* **(R3)**.

Insbesondere die operativen Aktivitäten des ISO27-SP können häufig nur gemeinschaftlich von verschiedenen Ansprechpartnern und Experten bearbeitet werden. So ist beispielsweise bei der Analyse von IS-Risiken der Fachbereich dafür zuständig, die potentiellen Schäden von Sicherheitsvorfällen abzuschätzen, während IT-Mitarbeiter deren Eintrittswahrscheinlichkeit bewerten. *Entsprechend sollte IT-seitig die Kommunikation und Kollaboration zwischen den jeweiligen Bearbeitern der ISMS-Aktivitäten unterstützt werden* **(R4)**.

Alle ISMS-relevanten Vorgaben sowie wesentliche Aktivitäten, Ereignisse und Entscheidungen im ISO27-SP sind angemessen zu dokumentieren, damit sie später überprüft und deren Ordnungsmäßigkeit ggf. durch eine Zertifizierung bestätigt werden kann. *Wichtige Entscheidungspunkte und fachliche Aktivitäten sollten daher innerhalb der IT-Lösung protokolliert und Methoden und Funktionalitäten zur Dokumentation und zum Dokumentenmanagement bereitgestellt werden* **(R5)**.

Die Wirksamkeit des ISMS ist insbesondere auch vom ISMS-Verständnis und -Wissensstand der Belegschaft abhängig. Wissenserwerb sowie Wissens- und Informationsverteilung bilden daher eine wesentliche Voraussetzung, um in den wiederkehrenden Zyklen des ISO27-SP eine fortlaufende Verbesserung zu erreichen. *IT-seitig sollten daher Methoden und Funktionalitäten bereit gestellt werden, um das Informations- und Wissensmanagement innerhalb der ISMS-Organisation zu unterstützen* **(R6)**.

Ein ISMS weißt Schnittstellen und fließende Grenzen zu anderen Managementsystemen (z.B. Qualitäts- und Risikomanagement) und operativen Prozessen (z.B. Security Information and Event Management, Security Incident-Management) auf. Die gewachsenen Strukturen werden i.d.R. IT-seitig bereits durch verschiedenste Werkzeuge (z.B. E-Learning- und Belehrungstools, Monitoring-Werkzeuge, usw.) unterstützt. *Ein ISMS-Tool sollte daher die Anbindung zusätzlicher IT-Systeme über entsprechende Schnittstellen erlauben, resp. die Einbindung von zusätzlichen Informationen ermöglichen* **(R7)**.

Zu den wesentlichen Vorzügen des nativen ISMS zählen die Freiheitsgrade, die den Unternehmen bei der Ausgestaltung der ISMS-Aktivitäten zustehen (z.B. Wahlfreiheit bei Analysemethoden, risikoorientierte Auswahl von IS-Maßnahmen, etc.). Um diese Vorteile nicht zu beeinträchtigen, sollte die Flexibilität auch IT-seitig erhalten bleiben. *Ein ISMS-Tool sollte daher modular aufgebaut sein, alternative Analysemethoden zur Auswahl bereitstellen und sich an die Bedürfnisse des Unternehmens anpassen lassen* **(R8)**.

4.2 ISMS-fachliche IT-Anforderungen

Innerhalb der Planungsphase des ISO27-SP sind durch die ISMS-Zentralfunktion administrative Aufgaben, z.B. die Überprüfung der Aktualität von Aufbau- und Ablauforganisation und ISMS-Rollen wahrzunehmen (Vgl. z.B. P_1A_4, P_2A_1). *Ein ISMS-Tool sollte daher eine ISMS-Stammdatenverwaltung bereitstellen* **(R9)**.

Zu den operativen Aktivitäten in der Planungsphase zählen insbesondere die Schutzbedarfsanalyse (P_1A_6), die Umfeldanalyse (P_1A_5) und die Ressourcenplanung (P_2A_2). Diese Analysen sind zwar nicht explizit durch die Norm gefordert, haben sich jedoch als Best Practices bewährt.

IT-seitig sollten daher (optionale) fachliche Module bereitgestellt werden, um Schutzbedarfs- und Umfeldanalyse sowie die Ressourcenplanung zu unterstützen **(R10)**.

Die verbleibenden Aktivitäten innerhalb der Planungsphase sind weitestgehend von organisatorischer Natur, z.B. die Überprüfung, Abstimmung und Aktualisierung von strategischen und operativen Vorgaben (z.B. P_1A_6, P_2A_1, P_3A_2). Eine IT-seitige Unterstützung im engeren Sinne ist dabei nur bedingt möglich. Allerdings können auf elektronischem Weg insbesondere Formulierungsvorschläge (z.B. für IS-Ziele) und beispielhafte Sicherheitsrichtlinien sowie Verfahrensbeschreibungen bereitgestellt werden. *Ein ISMS-Tool sollte demnach ISMS-relevante Unterlagen, Templates und sonstige Materialien als Orientierungshilfe, resp. Muster anbieten* **(R11)**.

Das Risikomanagement (P_4A_1 bis P_4A_7) innerhalb der Do-Phase kann sowohl methodisch als auch technisch unterstützt werden. So lassen sich beispielsweise durch Bereitstellung von datenbankgestützten Fragebögen und strukturierten Eingabeformularen alle relevanten Informationen zur Identifikation, Analyse und Bewertung von IS-Risiken erfassen. Außerdem kann das Risk Assessment durch Bereitstellung von archivierten Daten sowie zusätzlichem Content (z.B. Bedrohungs-, Schwachstellen- und Maßnahmenkataloge) deutlich vereinfacht werden. Darüber hinaus helfen strukturierte Eingabeformulare bei der Erstellung des Risikobehandlungsplans und der Anwendbarkeitserklärung. *Ein ISMS-Tool sollte demnach fachliche Module zur Unterstützung des Risk Assessments, zur Verwaltung des Risikobehandlungsplans und zur Erstellung der Anwendbarkeitserklärung bereitstellen* **(R12)**.

Die Umsetzung der IS-Maßnahmen (P_5A_1) erfolgt außerhalb des ISO27-SP, sodass die Zentralfunktion den Umsetzungsstand der IS-Maßnahmen und die Termintreue nachhalten und überprüfen muss (P_5A_1). *IT-seitig lässt sich diese eher administrative Aktivität der Datenerfassung und -pflege durch die Bereitstellung eines Moduls zum Maßnahmenmanagement unterstützen* **(R13)**.

Neben den normativen Referenzmaßnahmen aus Annex A lassen sich auch die obligatorischen, im ISO27-SP fest verankerten Schulungs- und Sensibilisierungsmaßnahmen (P_6A_1, P_6A_2) sowie interne Kontrollen, Monitoring-Prozesse und interne Audits (P_7A_1, P_7A_2: P_8A_1) den IS-Maßnahmen zuordnen. Die Bandbreite an IT-seitigen Unterstützungsmöglichkeiten reicht von datenbankgestützten Self Assessments und Fragebögen über zusätzliche Verwaltungs- und Analysemodule bis hin zu technischen Monitoring-Werkzeugen (z.B. Port- oder Schwachstellenscanner). *Ein ISMS-Tool sollte entsprechend (optionale) fachliche Module zur Unterstützung der (obligatorischen und normativen) IS-Maßnahmen bereitstellen und, wie in R7 gefordert, die Anbindung von spezialisierten IT-Security-Werkzeugen erlauben* **(R14)**.

Berichtswesen und Managementbewertung (P_9A_1, P_9A_2) sind auf die Informationen angewiesen, die im Laufe des ISO27-SP erzeugt oder gesammelt wurden. Mithilfe von Dashboard-Funktionalitäten, Berichtstemplates und rollenspezifischen Sichten können relevante Informationen direkt aus den (ggf. auch dezentralen) Datenbeständen des ISMS-Tools und seiner Umsysteme extrahiert, transformiert und zielgruppengerecht aufbereitet werden. *IT-seitig sollten daher ETL-Prozesse und (konfigurierbare) Reporting-Funktionalitäten bereitgestellt werden* **(R15)**.

Die Erfassung von Verbesserungsvorschlägen sowie die Konzeption von Korrektur- und Verbesserungsmaßnahmen in der Act-Phase des ISO27-SP kann z.B. durch ein betriebliches Vorschlagswesen oder Ideenmanagement sowie weitere Werkzeuge zur Kommunikation und Kol-

laboration (Vgl. R4) unterstützt werden. *Ein ISMS-Tool sollte entsprechende (optionale) Module zur Unterstützung der Act-Phase bereitstellen und, wie in R7 gefordert, die Anbindung zusätzlicher Werkzeuge erlauben* **(R16)**.

5 Zusammenfassung und Ausblick

Im Rahmen des vorliegenden Beitrags wurde das Forschungsvorhaben CISO27 sowie der, durch eine Literaturanalyse erweiterte, ISO27-SP vorgestellt. Aus den Prozessschritten und einzelnen Aktivitäten des Referenzprozesses wurden IT-seitige Unterstützungsmöglichkeiten und Anforderungen an ein ISMS-Tool zur Unterstützung des Referenzprozesses abgeleitet. Diese Anforderungen sollen in weiteren Forschungsiterationen ihren Eingang bei der Entwicklung der modular aufgebauten IT-Lösung CISO27-Suite finden, welche den ISO27-Sicherheitsprozess ganzheitlich implementiert.

Die CISO27-Suite soll die übergreifende Verwaltung sowie die einzelnen Prozessschritte und Aktivitäten des ISO27-SP in allen Phasen des PDCA Zyklus unterstützen und Workflow-Funktionalitäten bereitstellen, um die Zuweisung und Durchführung der ISMS-Aktivitäten zu (semi-) automatisieren. Darüber hinaus sollen die einzelnen Verwaltungs- und Analysemodule durch einen umfangreichen Methodenbaukasten ergänzt werden, der alternative und aufeinander abgestimmte Methoden zur Unterstützung der jeweiligen ISMS-Aktivitäten bereitstellt. Hierdurch lassen sich die, für den Unternehmenskontext passenden fachlichen Bausteine und zugehörigen IT-Module flexibel zusammenstellen. Interaktive Elemente dienen außerdem der Informationsversorgung, führen den Nutzer strukturiert durch den ISO27-SP und unterstützten ihn sowohl methodisch bei der Bearbeitung seiner Aufgaben als auch technisch in Bezug auf die Bedienung der CISO27-Suite (vgl. Abbildung 2).

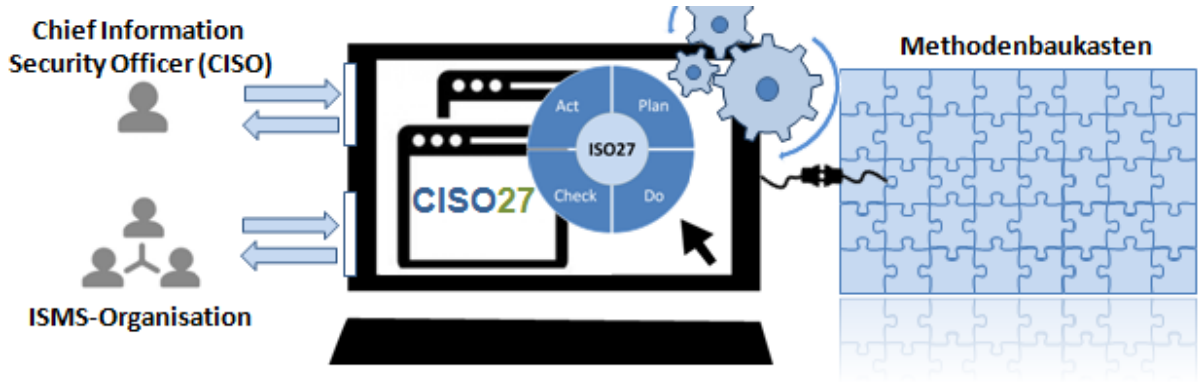

Abb. 2: Überblick zur CISO27-Suite

In den nächsten Forschungsiterationen sollen der Referenzprozess und die abgeleiteten IT-Anforderungen gemeinsam mit Praxispartnern und ISMS-Auditoren evaluiert und kontinuierlich weiterentwickelt werden. Durch die Evaluierung der Zwischenergebnisse und das iterative Forschungsvorgehen (vgl. [HMPA04]) wird sichergestellt, dass keine inhaltlichen, normativen und, zu deren Implementierung erforderlichen, technischen Anforderungen bei der Entwicklung des ISMS-Tools übersehen werden. Im Ergebnis des Forschungsvorhabens können ISO27-SP und CISO27-Suite gemeinsam genutzt werden, um "by Design" ein normkonformes, natives ISMS aufzubauen und zu betreiben.

Literatur

[Beck00] J. Becker: Informationsmodelle für das Electronic Business. In: Weiber R (Hrsg.) Handbuch Electronic Business: Informationstechnologien – Electronic Commerce – Geschäftsprozesse. Gabler (2000).

[Jend14] K. Jendrian: Der Standard ISO/IEC 27001:2013. In: Datenschutz und Datensicherheit – DuD, Volume 38, Issue 8 (2014) 552-557.

[HoHo16] M. Hofmann, A. Hofmann: Der ISO27-Sicherheitsprozess: Ein Referenzprozess zur Umsetzung der ISO/ IEC 27001. Research-in-Progress- und Poster-Beiträge der Multikonferenz Wirtschaftsinformatik (2016).

[BiVk15] Bitkom und VKU: Praxisleitfaden IT-Sicherheitskatalog, Anforderungen an die IT für den sicheren Betrieb von Energieversorgungsnetzen (2015).

[CSC15] CSC: GSTOOL QUO VADIS? Evaluation von Information Security Management System Tools als Grundschutz Tool Alternativen (2015).

[WiPi12] I. Windhorst, B. Pirzer: Managementsysteme für Informationssicherheit: Marktübersicht. Vorgehensmodell. Handlungsempfehlungen. Fraunhofer Research Institution AISEC (2012).

[SaDi16] J. Saat, P. Dirding: "Legalize IT" – Sinnvoller Umgang mit Schatten-IT, www.bankinghub.de (2016).

[Kozl13] E. Kozlova: Governance der individuellen Datenverarbeitung, Wertorientierte und risikobewusste Steuerung der IDV-Anwendungen in Kreditinstituten, Springer (2013).

[HMPA04] A.R. Hevner, S.T. March, J. Park, S. Ram: Design science in Information Systems research, MIS Quarterly, 28, 1 (2004) 75-105.

[KeRS13] H. Kersten, J. Reuter, K.W. Schröder: IT-Sicherheitsmanagement nach ISO 27001 und Grundschutz: Der Weg zur Zertifizierung. 4.Auflage, Springer (2013).

[Klip15] S. Klipper: Information Security Risk Management: Risikomanagement mit ISO/IEC 27001, 27005 und 31010. 2.Auflage, Springer (2015).

[Hump16] E. Humphreys: Implementing the ISO/IEC 27001 ISMS Standard. Second Edition, Artech House (2016).

[ISO27003] ISO/IEC 27003: Information technology – Security techniques – Information security management system implementation guidance (2010).

[BSI100-2] BSI-Standard 100-2: IT-Grundschutzvorgehensweise, Version 2.0 (2008).

[Müll14] K-R. Müller: IT-Sicherheit mit System, Integratives IT-Sicherheits-, Kontinuitäts- und Risikomanagement - Sichere Anwendungen - Standards und Practices. 5. Auflage, Springer (2014)

[BSN+09] J. Vom Brocke, A. Simons, B. Niehaves, K. Riemer, R. Plattfaut, A. Cleven: Reconstructing the giant: On the importance of rigour in documenting the literature search process. In : 17th European Conference on Information Systems (2009) 2206-2217.