Branchenspezifischer Sicherheitsstandard für gesetzliche Kranken- und Pflegeversicherer

B3S-GKV/PV

Bearbeitungsstatus:	**final**
Version:	**1.4**
Stand:	**20.01.2025**
Verfasserin/Verfasser:	**BAK Gesetzliche Krankenversicherungen im UP KRITIS**
Vertraulichkeitsstufe:	**öffentlich**

Impressum

Herausgeber: Branchenarbeitskreis Gesetzliche Krankenversicherungen im UP KRITIS

Kontakt über: Branchenarbeitskreis Gesetzliche Krankenversicherungen im UP KRITIS

Inhaltsverzeichnis

Abbildungsverzeichnis

Tabellenverzeichnis

Vorbemerkung

Die Verordnung zur Bestimmung Kritischer Infrastrukturen nach dem BSI-Gesetz (BSI-Kritisverordnung - BSI-KritisV) definiert im Sektor Finanz- und Versicherungswesen nach Anhang 6 Ziffer 1.27 das Verwaltungs- und Zahlungssystem der gesetzlichen Kranken- und Pflegeversicherung (GKV/PV) ab 500.000 Versicherte als Kritische Infrastruktur und nach § 7 Abs. 1 Ziffer 5 die Versicherungsdienstleistung als kritische Dienstleistung im Sinne des BSI-Gesetzes (BSIG).

Nach BSIG können Betreiber einer Kritischen Infrastruktur und ihre Branchenverbände so genannte branchenspezifische Sicherheitsstandards (B3S) vorschlagen. Das Bundesamt für Sicherheit in der Informationstechnik (BSI) stellt dann auf Antrag fest, ob diese B3S geeignet sind, die Anforderungen nach BSIG zu gewährleisten.

Dieses Dokument stellt einen branchenspezifischen Sicherheitsstandard für die gesetzlichen Kranken- und Pflegeversicherer dar – im Folgenden B3S-GKV/PV genannt.

Dieser Standard ist Grundlage für die Etablierung und Aufrechterhaltung des Stands der Technik für den Betrieb einer Kritischen Infrastruktur bzw. kritischen Dienstleistung (kDL) in der gesetzlichen Kranken- und Pflegeversicherung. Er dient zur Identifikation notwendiger Sicherheits- und Managementmaßnahmen, um einen Ausfall oder eine Beeinträchtigung von kritischen Dienstleistungen zu vermeiden. Es gilt zu verhindern, dass es zu erheblichen Versorgungsengpässen der Bevölkerung oder zu Gefährdungen der öffentlichen Sicherheit kommen könnte.

Die Norm ISO 27001[1] mit Vorgaben zum Aufbau eines ISMS wird berücksichtigt und für die Umsetzung von (Sicherheits-)Anforderungen[2] nach Stand der Technik wird der Annex A der Norm herangezogen, um der Gefährdungslage der GKV/PV risikoorientiert zu begegnen. Es gilt zu beachten, dass die ausschließlich ISO 27001 konforme Umsetzung eines ISMS im Sinne des BSIG nicht ausreichend ist. Der hier vorliegende B3S berücksichtigt entsprechend auch die über die ISO 27001 hinausgehenden Anforderungen.

Ziel ist der Schutz der informationstechnischen Systeme, Komponenten und Prozesse durch Risikoreduzierung und Risikobeherrschung. Dies wird durch ein auf die betroffenen Prozesse ausgerichtetes Risikomanagementsystem erreicht.

Obwohl in der GKV/PV ein weitgehend einheitliches Leistungsspektrum durch den Gesetzgeber vorgegeben wird, ist die Ausprägung der technischen Umsetzung der Leistungserbringung durch den Dienstleistungscharakter individuell gestaltet. Im Gegensatz zu beispielsweise einem Kraftwerksbetrieb ist die notwendige IT-Landschaft eine offene Architektur, an die im Rahmen eines KRITIS-Betriebs mit diesem Standard bestimmte Anforderungen zu stellen sind. Aufgrund dieser Situation ist im vorliegenden Dokument das hohe Abstraktionsniveau mit der Zielsetzung gewählt, allen Anwendern dieses B3S die Möglichkeit einer kassenspezifischen Umsetzung zu geben.

[1] In diesem B3S wird die verkürzte Schreibweise für referenzierte ISO Standards (siehe Kapitel 6.1) verwendet statt des vollständigen Titels (z. B. „ISO 27001“).

[2] Eine Anforderung ist eine Aussage über die notwendige Beschaffenheit oder Fähigkeit, die ein System oder Systemteile erfüllen oder besitzen muss, um einer Norm oder einer Spezifikation zu entsprechen.

Anwendung des B3S-GKV/PV

Dieser B3S stellt einen Standard für gesetzliche Kranken- und Pflegekassen dar. Es liegt in der Entscheidung des jeweiligen Betreibers, ob er den vorliegenden B3S-GKV/PV als Sicherheitsstandard anwendet.

Alle nachfolgenden Inhalte sind bei einer Anwendung des B3S-GKV/PV grundsätzlich verbindlich zu berücksichtigen. Jedem Betreiber wird dabei der erforderliche individuelle Spielraum bei der praktischen Umsetzung des Standards eingeräumt, um die Anforderungen innerhalb seiner jeweils spezifischen Aufbauorganisation, Ablauforganisation sowie der individuellen technischen Ausrichtung und Infrastruktur umzusetzen. Dies bedeutet, dass Abweichungen von der in diesem Standard beschriebenen Vorgehensweise und Anforderungen kassenindividuell zulässig sind, diese müssen dann aber nachvollziehbar dokumentiert und begründet werden.

Aufbau und Ablauf der Anwendung dieses Standards:

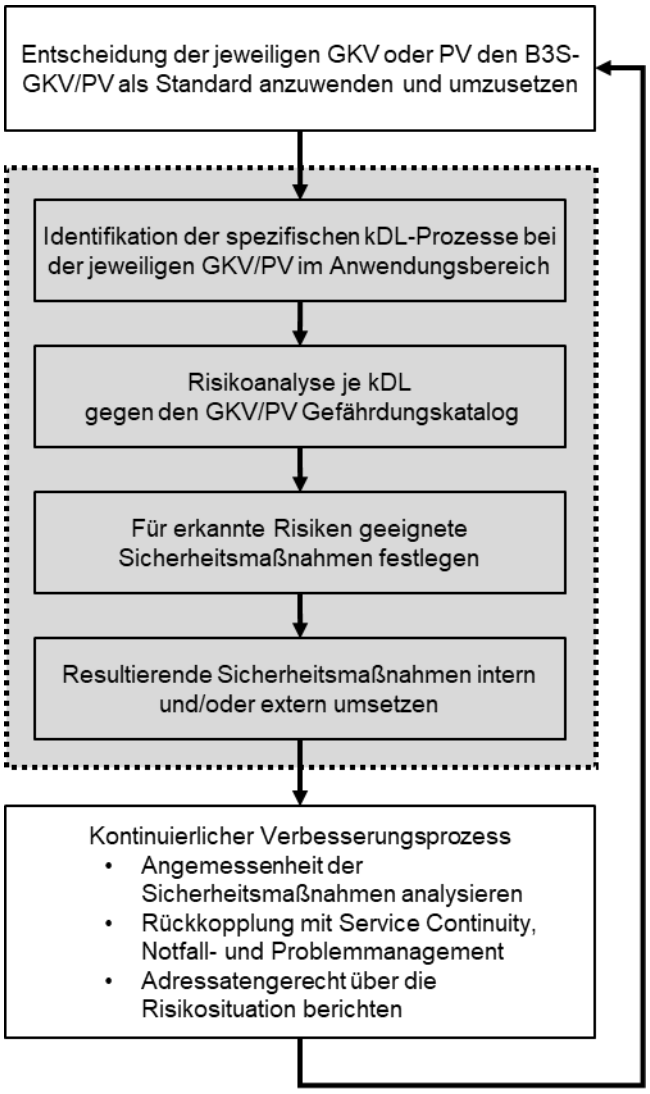

Abbildung 1: Aufbau und Ablaufschema des B3S

Teil 1

1 Anwendungsbereich, kritische Dienstleistungen, Schutzziele

1.1 Anwendungsbereich in der GKV/PV

Mit dem Begriff „Anwendungsbereich“ wird hier der Informationsverbund mit seinen IT-Systemen, Komponenten und Prozessen bezeichnet, der von diesem B3S adressiert wird. Dieser Anwendungsbereich kann sich vom Geltungsbereich des Nachweises bzw. Geltungsbereich des ISMS unterscheiden.

Der vorliegende B3S-GKV/PV unterstützt bei der Umsetzung der vom BSIG zum Schutz der Kritischen Infrastrukturen geforderten Sicherheitsmaßnahmen gemäß „Stand der Technik“. Im Fokus steht das „Verwaltungs- und Zahlungssystem der gesetzlichen Kranken- und Pflegeversicherung“ in Form eines integrierten Anwendungssystems (im Folgenden sowie in mitgeltenden Normen und Regelwerken auch (IT-)Anwendung oder (IT-)System genannt). Dies ist unabhängig davon, ob die Anlagen von der Kranken- oder der Pflegekasse selber betrieben werden oder in Teilen oder vollständig von einem Dienstleister.

Im Folgenden ist der Anwendungsbereich hinsichtlich des Informationssicherheits-Managementsystems (ISMS) und der kritischen Dienstleistungen (kDL) festgelegt.

1.1.1 ISMS

Der Versicherer muss mindestens für den hier definierten Anwendungsbereich ein Informationssicherheits-Managementsystem (ISMS) etablieren und betreiben. Im Folgenden wird der ISMS-Anwendungsbereich bezüglich der Schnittstellen in der gesamten Verarbeitungskette kritischer Dienstleistungen festgelegt.

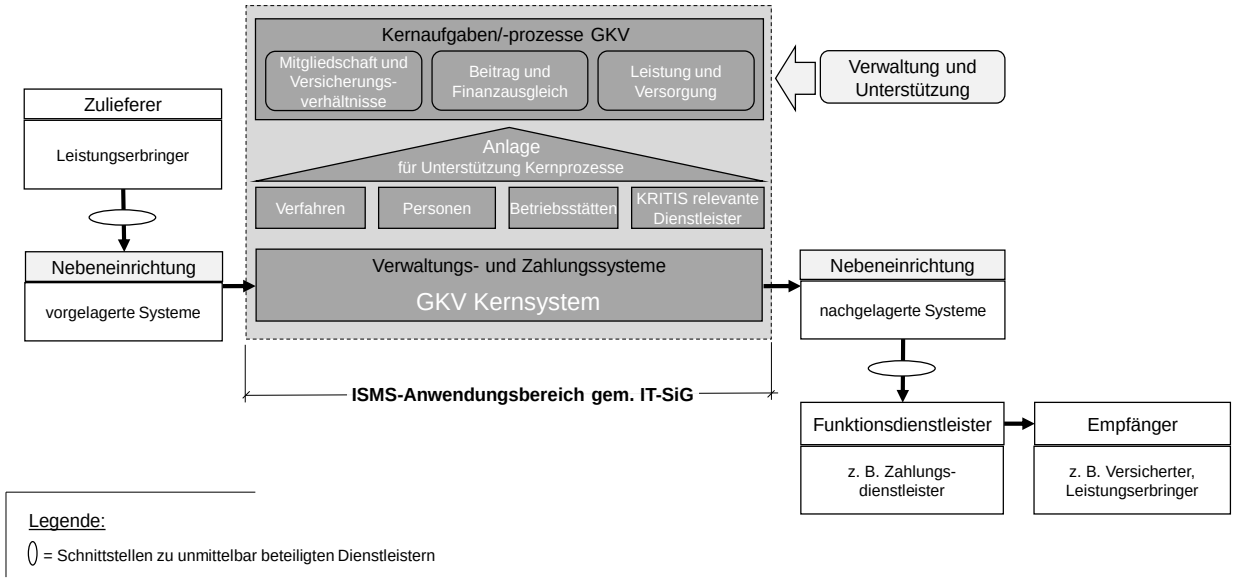

Abbildung 2: ISMS-Anwendungsbereich gem. BSIG bzw. der BSI-KritisV

Jeder Anwender des B3S-GKV/PV muss den oben dargestellten Anwendungsbereich (siehe Abbildung 2: ISMS-Anwendungsbereich gem. BSIG bzw. der BSI-KritisV) in Bezug auf seine individuelle Infrastruktur und auf die darauf betriebenen kritischen Dienstleistungen konkretisieren. Eine Replikation dieses ISMS-

Anwendungsbereichs aus dem B3S ist allein nicht ausreichend und der Geltungsbereich muss auf dieser Basis betreiberspezifisch individuell definiert werden.

Sofern für die ordnungsmäßige Erfüllung der Verwaltungs- und Unterstützungsaufgaben / -prozesse bestimmte Anlagen sowie Nebeneinrichtungen zwingend erforderlich sind, sind diese Bestandteil des ISMS-Anwendungsbereiches. Insbesondere sind wichtige Schnittstellen, wie z. B. Kommunikationskanäle zu diesen Anlagen bzw. Nebeneinrichtungen zu berücksichtigen.

Vom Anwendungsbereich ausgenommen sind Verwaltungs- und Unterstützungsaufgaben / -prozesse und deren Anlagen sowie Nebeneinrichtungen, welche nicht den kDL zuzurechnen sind, wie z. B. Marketingprozesse und deren Anwendungen.

1.1.2 Kritische Dienstleistungen der GKV/PV

Die kDL der GKV/PV wird gemäß BSI-KritisV im Sektor Finanz- und Versicherungswesen erbracht.

Die gesundheitliche Versorgung, insbesondere die Notfallversorgung der gesetzlich Kranken- und Pflegeversicherten erfolgt durch die Leistungserbringer (insbesondere Krankenhäuser, Apotheken, Arztpraxen, Notfallambulanzen) grundsätzlich ohne die unmittelbare Mitwirkung der Kranken- und Pflegeversicherer.

Die öffentliche Sicherheit und die Versorgung der Bevölkerung können seitens der GKV/PV aber dort beeinträchtigt sein, wo die Leistung der GKV/PV unmittelbar auf den Versicherten wirkt oder eine verbindliche Feststellung des Versichertenverhältnisses von Bedeutung ist.

Im § 284 SGB V und § 94 SGB XI werden Zwecke definiert für welche Kranken- und Pflegekassen bestimmte Sozialdaten verarbeiten dürfen. Die folgende Struktur für die Kernaufgaben bzw. die Kernprozesse der Verwaltungs- und Zahlungssysteme wurde hieraus abgeleitet:

Verwaltungs- und Zahlungssysteme beinhalten:	

grundlegende Prozesse der gesetzlichen Kranken- oder der sozialen Pflegeversicherer	• für Mitgliedschaft und Versicherungsverhältnisse, d.h.
	  ○ Feststellung des Versicherungsverhältnisses und der Mitgliedschaft.
	  ○ Ausgabe und Betrieb der elektronischen Gesundheitskarte eGK[3] (Ausstellung des Berechtigungsscheines als Ersatzverfahren).
	• für Finanzen (Beitrag und Finanzausgleich), d.h.
	  ○ Feststellung der Beitragspflicht und der Beiträge, deren Tragung und Zahlung.
	  ○ Durchführung von Erstattungs- und Ersatzansprüchen.
	  ○ Durchführung des Risikostrukturausgleichs.
	• für Leistung und Versorgung
	  ○ Prüfung der Leistungspflicht und der Erbringung von Leistungen an Versicherte.

[3] Gemäß § 8d Abs. 2 Ziffer 3 BSIG sind die Gesellschaft für Telematik, die Betreiber von Diensten der Telematik Infrastruktur und weitere Betreiber von Diensten, soweit sie die bestehende Telematik Infrastruktur für nach § 327 Abs. 2 bis 5 SGB V bestätigte Anwendungen nutzen, nicht vom Anwendungsbereich des BSIG erfasst.

Verwaltungs- und Zahlungssysteme beinhalten:	
	○ Abrechnung mit den Leistungserbringern und anderen Leistungsträgern, einschließlich der Prüfung der Rechtmäßigkeit und Plausibilität der Abrechnung und Überwachung der Wirtschaftlichkeit der Leistungserbringung.
übergreifende Unterstützungsprozesse der gesetzlichen Kranken- oder der sozialen Pflegeversicherer	• für Verwaltungsaufgaben und Unternehmensprozesse ○ Notwendige, übergreifende Unterstützungsprozesse zur Erfüllung der Aufgaben der gesetzlichen Kranken- oder der sozialen Pflegeversicherung

Tabelle 1: Kernaufgaben gemäß Sozialgesetzbuch V (SGB)

Als kritische Dienstleistungen (kDL) des Verwaltungs- und Zahlungssystems der gesetzlichen Kranken- und Pflegeversicherung sind daraus folgende Prozesse im Finanzbereich sowie mit unmittelbarer Wirkung auf den Versicherten anzusehen:

Prozess	**Beschreibung**
Zahlungsverkehr mit Gesundheitsfonds und Fremdversicherungsträgern	Zahlungsverkehr mit dem Gesundheitsfonds und den Fremdversicherungsträgern, damit die Einnahmen aller Sozialversicherungsbeiträge verfügbar werden
Zahlungsverkehr mit den Banken (Transaktionssystem)	Fähigkeit, den Geschäftsbanken Zahlungs- und Lastschriftaufträge im rechtsgültigen Format zu übermitteln und Bankkontostände abzurufen (Finanzdisposition/ Liquiditätsmanagement)
Personen- bzw. Kontokorrentbuchhaltung	Fähigkeit, die Forderungen und Verpflichtungen bzw. Aufwände und Erträge im Rahmen von Kreditoren- und Debitoren- oder Zahlungsverkehrskonten, ordnungsmäßig und nachvollziehbar abzubilden sowie die Zahlungsströme korrekt und zeitgerecht abwickeln zu können
Pflegegeldleistung	In der Pflegeversicherung können Pflegebedürftige anstelle der häuslichen Pflegehilfe ein Pflegegeld und Angehörige ein Pflegeunterstützungsgeld beantragen
Krankengeld	Entgeltersatzleistung der GKV; wird insbesondere dann gezahlt, wenn ein Versicherter infolge einer länger als sechs Wochen andauernden Krankheit (Entgeltfortzahlung im Krankheitsfall) arbeitsunfähig ist oder auf Kosten der Krankenkasse stationär behandelt wird
Krankengeld Kind	Kann von einem Elternteil beansprucht werden, das zur Beaufsichtigung, Betreuung oder Pflege des erkrankten versicherten Kindes der Arbeit fernbleiben muss
Mutterschaftsgeld	In der GKV eigenständig versicherte weibliche Mitglieder erhalten vor und nach einer Entbindung ein Mutterschaftsgeld im Rahmen der gesetzlichen Fristen
Übergangsgeld	Entgeltersatzleistung der Sozialversicherungsträger; erhalten Sozialversicherte u. a. während der Teilnahme an Maßnahmen zur medizinischen Rehabilitation und im Rahmen einer Anschlussheilbehandlung nach Auslauf des sechswöchigen Entgeltfortzahlungsanspruches gegenüber dem Arbeitgeber

Prozess	Beschreibung
Verletztengeld	Als Verletztengeld werden 80 % des Bruttoentgelts bei Wegeunfall, Arbeitsunfall und Berufskrankheit als Vorleistung der Krankenversicherung für den Unfallversicherungsträger ausgezahlt
Ausstellung der elektronischen Gesundheitskarte eGK	Nach Herstellung eines Versicherungsverhältnisses bzw. für regelmäßigen oder anlassbezogenen Ersatz stellt die Krankenkasse – i.d.R. mit Hilfe eines Dienstleisters – eine neue eGK für den Versicherten aus
Aktualisierung und Verwaltung der eGK via Versichertenstammdatendienst	Bei Änderung der Daten nach § 291a Abs. 2 SGB V muss zeitnah eine Aktualisierung auf der eGK erfolgen; dies geschieht durch den kassenseitig zur Verfügung gestellten „Dienst“ nach § 291b Abs. 1 SGB V
Einsatz von Ersatz- und Berechtigungsscheinen	Die Kassen können sogenannte Ersatz- und Berechtigungsbescheinigungen ausstellen, die vom Versicherten zur Inanspruchnahme von Leistungen – auch anstelle der eGK – verwendet werden können

Tabelle 2: Prozesse der kDL

Die Beeinträchtigung weiterer Dienstleistungen und Leistungsentscheidungen der Kranken- und der Pflegeversicherer gefährdet im Sinne des BSIG die öffentliche Sicherheit oder die Versorgung der Bevölkerung nicht. Die medizinisch notwendige Versorgung, insbesondere die Notfallversorgung der Versicherten wird von den Leistungserbringern auch ohne die zeitnahe Mitwirkung der Kranken- und Pflegeversicherer erbracht (vgl. Kritische Infrastrukturen der Branchen medizinische Versorgung, Arzneimittel und Impfstoffe sowie Labore im Sektor Gesundheit).

Basis für den kontinuierlichen Betrieb der Geschäftsprozesse bilden die dafür notwendigen Ressourcen, wie IT- und Kommunikationssysteme, Personal, Arbeitsplätze und Geschäftsräume.

Für die Prozesse der kDL in GKV/PV werden die Verfügbarkeitsanforderungen unter dem Aspekt der KRITIS-Relevanz in der nachfolgenden Tabelle definiert und begründet. Der Betreiber der kDL hat im Rahmen seiner Notfallvorsorge (vgl. Kap. 4.4) konkrete Wiederanlaufzeiten zu ermitteln. Hierbei ist zu beachten, dass nicht nur die Wiederanlaufzeiten im Rahmen der IT-Prozesse zu berücksichtigen sind, sondern auch die Fragestellung, wie der Prozess als Ganzes aufrechterhalten bzw. wiederhergestellt werden kann.

Die folgend genannten Verfügbarkeitsanforderungen stellen Mindestanforderungen dar.

Prozesse	Verfügbarkeitsanforderung	Begründung
Zahlungsverkehr mit Gesundheitsfonds und Fremdversicherungsträgern	**sehr hoch**	Zahlungsverkehr mit dem Gesundheitsfonds und den Fremdversicherungsträgern, damit die Einnahmen aller Sozialversicherungsbeiträge verfügbar werden
Zahlungsverkehr mit den Banken (Transaktionssystem)	**sehr hoch**	Die Fähigkeit Banktransaktionen durchzuführen, ist Grundlage und notwendige Voraussetzung für alle Geldleistungen, die empfangen und gezahlt werden.
Personen- bzw. Kontokorrentbuchhaltung	**hoch**	Um Forderungen und Verpflichtungen zu bedienen, müssen diese bekannt und dokumentiert sein (Voraussetzung zur Erkennung der Zahlungspflichten und -ansprüche).
Pflegegeldleistung	**hoch**	Pflegegeld, Pflegeunterstützungsgeld und Pflegesachleistung werden entweder einzeln und dann vollständig monetär oder vollständig als Sachleistung erbracht. Es ist auch die kombinierte Inanspruchnahme von Pflegegeld und Pflegesachleistung möglich.

Prozesse	Verfügbarkeits-anforderung	Begründung
Krankengeld	**hoch**	Als Entgeltersatzleistung nach Lohnfortzahlung ist eine zeitnahe Verfügbarkeit des Krankengeldes beim Krankengeldempfänger von Bedeutung.
Krankengeld Kind	**hoch**	Als Entgeltersatzleistung bei Erkrankung eines Kindes relevant
Mutterschaftsgeld	**normal**	Es handelt sich um einen relativ niedrigen Betrag und die Zahlung erfolgt nicht fortdauernd, sondern i.d.R. nur zwei Mal
Übergangsgeld	**hoch**	Analog Krankengeld
Verletztengeld	**hoch**	Analog Krankengeld
Ausstellung der elektronischen Gesundheitskarte eGK	**hoch**	Technisch bedingt gibt es bereits eine Mindestzeitdauer aufgrund der Kartenproduktion. Auch bei verfügbarem Prozess kann die eGK (Bearbeitungs- und Postlaufzeit) nicht schneller zur Verfügung gestellt werden
Aktualisierung und Verwaltung der eGK via Versicherten-stammdatendienst	**sehr hoch**	Der Dienst betrifft sämtliche Versicherungsverhältnisse, da die Inanspruchnahme von Gesundheitsleistungen durch gesetzlich Versicherte fast ausschließlich auf Basis einer gültigen eGK erfolgt
Einsatz von Ersatz- und Berechtigungsscheinen	**normal**	Ist ein Ersatz- /Backup-Verfahren für die eGK (siehe Tabelle 2: Prozesse der kDL)

Tabelle 3: Prozesse der kDL und Verfügbarkeitsanforderungen

1.2 Anwendungsbereich extern erbrachter Leistungen

Der B3S-GKV/PV berücksichtigt, wie das notwendige informationstechnische Sicherheitsniveau auch dort sichergestellt werden kann, wo für die Aufrechterhaltung der kDL relevante Prozesse im Auftrag des Betreibers durch Dritte betrieben werden.

Der notwendige Schutz der informationstechnischen Systeme, Komponenten, Prozesse und Daten ist bereits frühzeitig bei Planung und Erstellung entsprechender Systeme, bei der Beschaffung entsprechender Komponenten und insbesondere bei der Beauftragung von (IT-)Dienstleistern zu berücksichtigen. Dies bedeutet, dass Dienstleister, die unterstützende Services für den definierten Anwendungsbereich des Betreibers erbringen, entsprechend den Vorgaben der ISO 27001, Annex A 5.19 - 5.22, zu steuern sind.

Der Einsatz von Dienstleistern oder Arbeitsgemeinschaften (ARGE) entbindet den Betreiber nicht von der Pflicht, seine Informationssicherheitsbelange auch in den ausgelagerten Betriebs- und Serviceprozessen inklusive eingesetzter Anlagen bzw. Nebeneinrichtungen vertraglich einzufordern und die Einhaltung regelmäßig zu überprüfen.

1.3 Gesetzlicher und regulatorischer Rahmen

Der B3S-GKV/PV orientiert sich an den Anforderungen, die unter anderem in den nachfolgenden Gesetzen und Regelwerken zur Umsetzung des Stands der Technik definiert sind:

- Gesetz über das Bundesamt für Sicherheit in der Informationstechnik (BSI-Gesetz – BSIG)
- Sozialgesetzbücher (SGB)
- Vorgaben des Bundesamts für Soziale Sicherung (BAS)
- ISO 27001
- ISO 22301
- BDSG / EU-DSGVO

Es handelt sich um eine nicht abschließende Aufzählung relevanter Gesetzes- und Regelwerke. Die Betreiber der Anlagen müssen dafür Sorge tragen, dass die jeweils geltenden Fassungen der Gesetze und Regelwerke unter Berücksichtigung der länderspezifischen Anforderungen – soweit zutreffend - identifiziert und angewendet werden.

Der vorliegende B3S-GKV/PV erlangt Geltung in der jeweiligen Kranken- und Pflegeversicherung, indem die oberste Leitung seine Anwendung verbindlich vorschreibt und die Umsetzung und Aufrechterhaltung mit angemessenen Ressourcen unterstützt.

1.4 Schutzziele

Im Vordergrund steht die Aufrechterhaltung der Versorgung der Versicherten und der öffentlichen Sicherheit im Hinblick auf die in Kapitel 1.1.2 genannten kDL-Prozesse.

Alle Betreiber Kritischer Infrastrukturen in der GKV/PV sind verpflichtet, angemessene organisatorische und technische Vorkehrungen zur Vermeidung von Störungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit ihrer informationstechnischen Systeme, Komponenten oder Prozesse zu treffen, die für die Funktionsfähigkeit der von ihnen betriebenen Kritischen Infrastrukturen maßgeblich sind.

Organisatorische und technische Vorkehrungen (Sicherheitsmaßnahmen) sind angemessen, wenn der dafür erforderliche Aufwand nicht außer Verhältnis zu den Folgen eines Ausfalls oder einer Beeinträchtigung der betroffenen Kritischen Infrastruktur steht.

Zum Schutz der öffentlichen Sicherheit, der Versorgungssicherheit der Bevölkerung sowie der Versichertendaten gem. Sozialgesetzbüchern und EU-DSGVO werden die Schutzziele wie folgt definiert:

Schutzziel	Definition
Verfügbarkeit (inkl. Belastbarkeit)	Dienste und Informationen stehen belastbar und gesetzeskonform oder wie vertraglich vereinbart zur Verfügung. Informationen sind vor Verlust geschützt.
Vertraulichkeit	Informationen dürfen nur befugten und autorisierten Nutzern zugänglich sein.
Integrität (inkl. Authentizität)	Unversehrtheit und Vollständigkeit sowie Korrektheit von Informationen sind sichergestellt. Informationen können jederzeit ihrem legitimen Ursprung zugeordnet werden. Die Authentizität ist ein wichtiger Bestandteil des Schutzes von Informationen insbesondere im Kontext von Kommunikationsbeziehungen.

Tabelle 4: Definition der Schutzziele

Nachfolgende Anforderungen verdeutlichen die Motivation der Schutzziele für die kDL:

- Der Zugriff auf die relevanten Daten soll jederzeit in geschäftlich erforderlichem Umfang von den dazu Befugten möglich sein, um kritische Dienstleistungen wie Zahlungsleistungen an die Versicherten sicherzustellen.
- Die Informationen sollen auch in Krisenlagen angemessen vor unbefugter Preisgabe geschützt sein, um das Vertrauen der Versicherten in das staatliche System der GKV/PV aufrecht zu erhalten.
- Die unautorisierte Modifikation der informationstechnischen Systeme, Komponenten oder Prozesse für kritische Dienstleistungen soll verhindert werden, somit die korrekte Funktion der Systeme und die Unversehrtheit der Daten gewahrt bleibt, um jederzeit korrekte Zahlungen an die Versicherten durchführen zu können.
- Die Überprüfbarkeit und Vertrauenswürdigkeit der Daten und ihrer Herkunft (Authentizität) soll gewährleistet sein, um sicherstellen zu können, dass Leistungen korrekt und nur bei den legitimierten Empfängern ankommen.

Für alle Prozesse der kDL muss der Schutzbedarf in Hinblick auf die oben definierten Schutzziele im Rahmen von Schutzbedarfsanalysen durch den Betreiber ermittelt werden.

Weitere branchenspezifische Schutzziele, wie sie beispielsweise zu betrachten sind, wenn der breiten Öffentlichkeit über das Internet entsprechende Funktionalitäten zugänglich gemacht werden, existieren, haben auf die kDL jedoch keinen direkten Einfluss, da die Kernsysteme hiervon nicht direkt betroffen werden. Es kommen ebenfalls branchenweit keine speziellen Technologien (z. B. eingebettete Systeme, „Internet of Things“ (IoT) Geräte, industrielle Systeme bzw. Maschinen) zum Einsatz, die spezielle branchen- bzw. technik-spezifische Schutzziele erfordern.

Im Rahmen der Gewährleistung der Schutzziele müssen ferner die nachfolgenden möglichen Zustände beim Betrieb der kDL betrachtet werden:

Normallage:

Die Kernprozesse der GKV/PV sind in Bezug auf die Verwaltungs- und Zahlungssysteme funktionsfähig und gewährleisten den zielgerichteten und ordnungsgemäßen geschäftlichen Betrieb. Alle dem Geschäftszweck entsprechenden Aufgaben und Funktionen werden regelkonform ausgeführt und die erwarteten Arbeitsergebnisse können vollständig, richtig, zeitgerecht, geordnet und dokumentiert vorgenommen werden. Eventuelle Störungen der Anwendungen können über standardisierte Abläufe zeitnah behoben werden und führen nicht zu einer spürbaren Beeinträchtigung der kDL.

Notfalllage:

Ein Notfall stellt eine Störung größeren Ausmaßes dar. Für die kDL sind angemessene Vorkehrungen zu treffen um die Wahrscheinlichkeit des Eintritts von Notfalllagen auf ein angemessenes Maß zu reduzieren. Für die Bewältigung einer Notfalllage müssen Ablaufpläne und Verfahrensanweisungen existieren, um die Normallage wiederherzustellen.

Krisenlage:

Krisen können dann entstehen, wenn Notfalllagen eskalieren oder Ereignisse außerhalb des Betreibers die kDL bedrohen (z. B. Epidemien, dauerhafter Ausfall vitaler Infrastrukturen). Ein typisches Merkmal einer Krise ist die vorübergehende Natur des Ereignisses.

Vorkehrungen für Notfall- und Krisenlagen sind im Rahmen des BCM nach Kapitel 4.4 zu organisieren.

2 Gefährdungslage

2.1 All-Gefahrenansatz

Der B3S fordert die Behandlung aller relevanten Bedrohungen und Schwachstellen (All-Gefahrenansatz) für die maßgeblichen Anwendungen, Komponenten oder Prozesse, insbesondere aus den im Anhang genannten Bedrohungs- und Schwachstellenkategorien (gemäß „Orientierungshilfe zu Inhalten und Anforderungen an branchenspezifische Sicherheitsstandards (B3S) gemäß § 8a Absatz 2 BSIG“, Version 1.3 vom 23.02.2024, im Folgenden „Orientierungshilfe“ genannt, siehe dort Kapitel 5.1, 5.2 und 5.3).

Erst wenn eine Bedrohung auf eine Schwachstelle wirken kann, entsteht eine Gefährdung. Sicherheitsmaßnahmen können sowohl für Schwachstellen als auch gegen Bedrohungen ergriffen werden, um die damit verbundenen Risiken zu reduzieren.

Bei einer umfassenden Betrachtung des Gefahrenspektrums (alle relevanten Gefahren und Bedrohungen) für die maßgeblichen Anwendungen, Komponenten und Prozesse spricht man von einem sogenannten „All-Gefahren-Ansatz“ (siehe KRITIS-Strategie des BMI[4]).

Die zu betrachtenden Gefährdungen umfassen nach Vorgabe des BMI die Bereiche

- Naturereignisse,
- technisches und menschliches Versagen sowie
- Terrorismus, Kriminalität.

Dieser B3S folgt dem All-Gefahrenansatz. Bedrohungen und Schwachstellen werden im GKV/PV Gefährdungskatalog (siehe Kapitel 6.3) konsolidiert betrachtet und sind branchenspezifisch erweitert worden.

2.2 Berücksichtigung der allgemeinen Gefährdungslage

Da sich Gefährdungslagen – z. B. durch technischen Fortschritt – ändern können, müssen sie kontinuierlich überwacht und Änderungen am Gefährdungskatalog individuell berücksichtigt werden. Der Gefährdungskatalog ist daher entsprechend fortzuschreiben[5]. Dabei müssen vom Betreiber mindestens berücksichtigt werden:

- allgemeine Bedrohungen wie
  - neu hinzugekommene Typen von Angreifern und Angriffen,
  - intensivere Aktivität oder verbesserte Expertise/ Ressourcen von Angreifern,
  - Neuausrichtung/ Zielrichtung von Angriffen und Angreifern,
- neue, bekannt gewordene Schwachstellen,
- Änderungen der Gefährdungslage durch Veränderungen an der Systemarchitektur.

Änderungen an der allgemeinen Gefährdungslage (Bedrohungen und Schwachstellen) sind zu berücksichtigen und mit Sicherheitsmaßnahmen zu belegen.

2.3 Berücksichtigung der branchenspezifischen Gefährdungslage

Die branchenspezifische Gefährdungslage (siehe Kapitel 6.3) muss regelmäßig, z. B. über den BAK Gesetzliche Krankenversicherungen im UP KRITIS, spezielle Gremien innerhalb der Kassenverbände oder den GKV-Spitzenverband, auf Änderungen hin beobachtet und bewertet werden. Änderungen an der branchenspezifischen Gefährdungslage (Bedrohungen und Schwachstellen) sind zu berücksichtigen und ggf. mit Sicherheitsmaßnahmen zu unterlegen. Erfahrungen der Anwender bei der Umsetzung des B3S-GKV/PV sollen im BAK Gesetzliche Krankenversicherungen für die Weiterentwicklung eingebracht werden.

---

[4] Quelle: Nationale KRITIS-Strategie, BMI 2009; https://www.bmi.bund.de/SharedDocs/downloads/DE/publikationen/themen/bevoelkerungsschutz/kritis

[5] siehe dazu Hilfestellungen gem. BSI-Standard 200-3, Kapitel 9.3

Grundsätzlich sind die Verwaltungs- und Zahlungssysteme der GKV/PV in betreiberspezifischen Infrastrukturen realisiert, so dass keine einheitliche Gefährdungslage abgeleitet werden kann.

Dennoch entstehen branchentypische Gefährdungen durch die folgenden Umstände:

Für den Fall, dass (technische) Schnittstellen zu Betreibern im Gesundheitssektor existieren, die Opfer krimineller Aktivitäten oder Angriffe (z. B. durch Einsatz von „Ransomware“) geworden sind, gilt es ein Übergreifen der dortigen Auswirkungen in den Bereich der GKV/PV möglichst zeitnah zu verhindern (u. a. durch Firewalls, IDS/IPS). Daher sind insbesondere im Bereich des Datenaustausches (z. B. EESSI, Telematik-Infrastruktur) besondere Anforderungen an den Schutz vor Schadsoftware zu stellen.

Eine besondere branchenspezifische Gefährdungslage ergibt sich durch die hohe Konzentration von sensiblen Sozial- bzw. Gesundheitsdaten in den Anlagen der Betreiber.

Neue Erkenntnisse zur branchenspezifischen Gefährdungslage werden beispielsweise auf Ebene der Verbände der GKV/PV (z. B. im „Arbeitskreis für Informationssicherheit der Krankenkassen, ihrer Organisationen und des GKV-Spitzenverbandes“) oder im BAK Gesetzliche Krankenversicherungen des UP KRITIS zusammengetragen und konsolidiert. Sie können in eine Überarbeitung dieses B3S-GKV/PV einfließen, müssen jedoch durch die Betreiber bereits innerhalb des Risikomanagements berücksichtigt werden.

2.4 Branchenspezifische Relevanz von Bedrohungen und Schwachstellen

Bei den kDL der GKV/PV werden die Leistungen unter Einsatz des Verwaltungs- und Zahlungssystems bzw. des integrierten Anwendungssystems erbracht. Typischerweise werden diese Anlagen im Rahmen von geordnetem und standardisiertem Rechenzentrumsbetrieb bereitgestellt. Dieser basiert auf standardisierter Software und Hardware.

Betreiberspezifische Gefährdungen können durch individuelles Customizing und selbst entwickelte Funktionen entstehen.

3 Risikomanagement

3.1 Geeignete Behandlung aller für die kDL relevanten Risiken

Risiken müssen durch ein Informationssicherheitsrisikomanagement identifiziert, bewertet, dokumentiert und mit Sicherheitsmaßnahmen belegt werden. Grundsätzlich sollte dabei der Gefährdungskatalog GKV/PV (siehe Kapitel 6.3) verwendet werden. Alternativ kann auch eine andere Methodik (z. B. auf Basis der Elementargefährdungen aus dem BSI IT-Grundschutz-Kompendium) verwendet werden, sofern sie dokumentiert und mit dem obigen Verfahren vergleichbar ist sowie dem Stand der Technik entspricht. Die Methodik muss geeignet sein, die Risiken angemessen zu reduzieren, um die Kontinuität der kDL sicherzustellen.

Beim Betreiber muss ein dedizierter Risikomanagementprozess etabliert werden. Die nachfolgend beschriebene Vorgehensweise kann hier zur Ausgestaltung wesentlicher Aspekte herangezogen werden.

3.2 Beschränkung der Behandlungsalternativen für Risiken

Aufgrund der Vorgaben des BSIG sind für die Betreiber der kDL grundsätzlich die Optionen „Risiken mindern“ und ggf. „Risiken vermeiden“ anzuwenden. Nur in begründeten Ausnahmefällen darf die Option „Risiko tragen“ und somit die eigenständige und dauerhafte Risikoakzeptanz durch den Betreiber in Betracht gezogen werden. Ähnliches gilt für die Versicherung gegen bestimmte Risiken, da hierdurch zwar der betriebswirtschaftliche Schaden des Betreibers verringert bzw. abgedeckt wird, die Auswirkungen in Bezug auf Versorgungsengpässe für die Bevölkerung aber unverändert bestehen bleiben.

Eine Risikoakzeptanz ist z. B. nur aufgrund regulatorischer Vorgaben oder expliziter Beschränkung der Anforderungen an die Qualität oder Quantität der kDL möglich. Dennoch sind alle angemessenen Sicherheitsmaßnahmen anzuwenden, welche die akzeptierten Risiken weiter mindern können. Eine eigenständige dauerhafte Risikoakzeptanz ist in der Regel keine zulässige Option im Sinne des BSIG.

Maßstab für die Beurteilung der Angemessenheit von Sicherheitsmaßnahmen ist die Frage, ob der dafür erforderliche Aufwand nicht außer Verhältnis zu den Folgen eines Ausfalls oder einer Beeinträchtigung der betroffenen kritischen Infrastruktur steht (siehe § 8a Absatz 1 BSIG). Die betriebswirtschaftliche Kosten-Nutzenbetrachtung (vgl. § 4 Abs. 4 SGB V) ist daher sekundär.

Dabei sind das Ausmaß der Risikoexposition, die Größe der Einrichtung, die Umsetzungskosten und die Eintrittswahrscheinlichkeit und Schwere von Sicherheitsvorfällen sowie ihre gesellschaftlichen und wirtschaftlichen Auswirkungen zu berücksichtigen. Sollen oder können Sicherheitsmaßnahmen nicht umgesetzt werden, so ist diese Tatsache begründet zu dokumentieren und durch die oberste Leitung freizugeben.

Bei einer Aufgabenübertragung an externe (IT-)Dienstleister durch z. B. Outsourcing verbleibt die volle Verantwortung für das Risikomanagement beim Betreiber.

3.3 Berücksichtigung von Abhängigkeiten bei der Risikoanalyse

Betreiber müssen im Zuge des Risikomanagement-Prozesses analysieren, inwieweit ihre Anlagen zur Unterstützung der jeweiligen kDL-Abhängigkeiten zu Dritten haben, die unmittelbar oder mittelbar an der Erbringung der kDL beteiligt sind.

Die Verantwortung für die Risikobehandlung verbleibt beim Betreiber, auch wenn Teile oder der gesamte Betrieb extern ausgeführt werden (Outsourcing). In diesem Fall sind zusätzlich Risiken, die mit dem Outsourcing verbunden sind, zu identifizieren, zu analysieren / bewerten und entsprechend zu berücksichtigen.

Es müssen u. a. die nachfolgenden Ebenen mit potentiellen Abhängigkeiten betrachtet, bewertet und wo erforderlich mit Sicherheitsmaßnahmen belegt werden:

- zusammenwirkende Verfahren und Prozesse
- Anwendungen mit wichtigen Schnittstellen, z. B. EESSI, Telematik-Infrastruktur
- organisatorische bzw. personelle Verbindungen

Teil 2

4 Katalog der relevanten Sicherheitsanforderungen

Es ist sicherzustellen, dass das Erreichen und Aufrechterhalten des Standes der Technik für die Anwendungen des Anlagenbetriebes bei Kritischen Infrastrukturen in geeigneter Weise in der Organisation des Betreibers verankert ist. Dies sollte durch ein entsprechendes Informationssicherheits-Managementsystem (ISMS) erfolgen.

Die GKV/PV-relevanten Sicherheitsmaßnahmen wurden aufgrund von rechtlich regulatorischen Anforderungen, Geschäftsanforderungen oder von branchenüblichen Best Practices unter Berücksichtigung der Schutzziele festgelegt.

4.1 Informationssicherheitsmanagementsystem (ISMS)

Ein ISMS erfordert die Aufstellung und Einführung von Strukturen, Verfahren und Regeln, um die Informationssicherheit dauerhaft zu definieren, zu steuern, zu kontrollieren, aufrechtzuerhalten und fortlaufend zu verbessern.

Unter Verwendung der ISO 27001 wird die Etablierung eines ISMS mit entsprechender Leitlinie (vgl. ISO 27001, Kapitel 5.2) sowie die Erstellung und Verabschiedung von Richtlinien vorgeschrieben.

Herstellung und Aufrechterhaltung des Standes der Technik setzen voraus, dass die branchenspezifischen Bedingungen, Gefährdungen, Risiken und Sicherheitsanforderungen, die in diesem B3S-GKV/PV beschrieben sind, berücksichtigt und Maßnahmen nach dem B3S umgesetzt werden, um die Kritischen Infrastrukturen ausreichend zu schützen.

GKV/PV-spezifische Hinweise:

Weitergehende spezifische Anforderungen ergeben sich nicht.

Mindestens umzusetzende Anforderungen an ein ISMS nach ISO 27001:

Kap. 4-10	Anforderungen an die Einrichtung, Umsetzung, Aufrechterhaltung und fortlaufende Verbesserung eines ISMS

Mindestens umzusetzende Anforderungen nach ISO 27001 Annex A:

5.1	Informationssicherheitspolitik und -richtlinien
5.5	Kontakt mit Behörden
5.8	Informationssicherheit im Projektmanagement
5.14	Informationsübermittlung
5.15	Zugangssteuerung

4.2 Asset Management

Es ist ein Register zu erzeugen, in welchem ausgehend von den kDL-Prozessen bis hin zu den Systemen die Abhängigkeiten (Auswertung) inventarisiert (eindeutige Namensgebung) und klassifiziert (vorrangig, aber nicht ausschließlich nach Verfügbarkeitsanforderungen) sind.

GKV/PV-spezifische Hinweise:

Weitergehende spezifische Anforderungen ergeben sich nicht.

Mindestens umzusetzende Anforderungen nach ISO 27001 Annex A:

5.9	Inventar der Informationen und anderen damit verbundenen Werte
5.10	Zulässiger Gebrauch von Informationen und anderen damit verbundenen Werten
5.11	Rückgabe von Werten
5.12	Klassifizierung von Informationen
5.13	Kennzeichnung von Informationen
7.10	Speichermedien

4.3 Risikoanalysemethode

Beim Betreiber der Kritischen Infrastruktur muss eine Risikoanalysemethodik konzipiert und umgesetzt sein, die für die Identifizierung der die kDL bedrohenden Risiken inkl. deren Klassifizierung geeignet ist. Die Methodik muss eine Risikobehandlung enthalten, um geeignete Sicherheitsmaßnahmen festzulegen, welche die identifizierten Risiken angemessen behandelt.

Geeignete Risikomethoden sind z. B. die Standards ISO 31000, ISO 27005 oder BSI 200-3, alternativ kann eine eigene Methodik unter Beachtung der Rand- und Rahmenbedingungen der genannten Standards gewählt werden.

Auch der branchenspezifischen Gefährdungslage muss in der Risikoanalyse Rechnung getragen werden, insbesondere in Bezug auf den Schutz der Sozial- und Gesundheitsdaten.

4.3.1 Prozess zum Informationssicherheits-Risikomanagement

Nachfolgend wird ein methodischer Ansatz (RM-Prozess) beschrieben, welcher bewährte Standards u. a. nach ISO 27005, ISO 31000 sowie dem BSI-Standard 200-3 mittels des GKV/PV-Gefährdungskatalog aufgreift und die Kompatibilität zu den Anforderungen nach ISO 27001 sicherstellt sowie vergleichbare und reproduzierbare Ergebnisse im Informationssicherheits-Risikomanagement fördert.

Die Verantwortung für die Auswahl der Risikobehandlungsoptionen und für die Umsetzung der ausgewählten Sicherheitsmaßnahmen verbleibt beim Betreiber.

Der prozessuale Ablauf ist in nachfolgender Abbildung exemplarisch dargestellt:

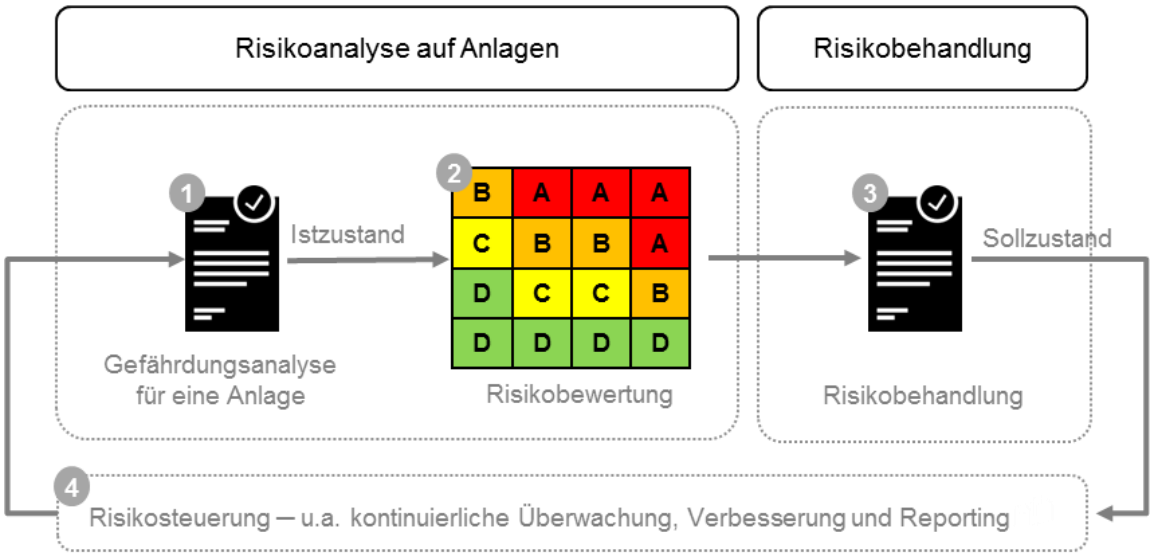

Abbildung 3: RM-Prozess im Überblick

Ausgehend vom Istzustand, welcher den Betrieb der Anlage inklusive der wirksam umgesetzten Sicherheitsmaßnahmen umfasst, ist die Gefährdungsanalyse durchzuführen. Dabei werden die Punkte des Gefährdungskatalogs gegen die relevante IT, insbesondere die kritische Dienstleistung abgeglichen.

Im zweiten Schritt erfolgt eine Risikobewertung je Gefährdung aus dem GKV/PV-Gefährdungskatalog. Die erkannten Risiken (inkl. zu diesem Zeitpunkt implementierter Sicherheitsmaßnahmen) werden dabei anhand Einschränkungsgrad (Auswirkung) und Eintrittswahrscheinlichkeit bewertet und klassifiziert. Im Ergebnis liegt der bewertete Istzustand vor.

Daran schließt sich die Risikobehandlung an, welche die zusätzlich erforderlichen Sicherheitsmaßnahmen definiert. Ziel ist es, die klassifizierten Risiken einer betroffenen kDL auf ein angemessenes Risikoniveau (hier: in die niedrigste Risikoklasse „D“) zu senken.

In der Risikosteuerung erfolgt die kontinuierliche Überwachung der Risiken, deren Reporting und die kontinuierliche Verbesserung.

Grundlage bildet ein auf **2 Skalen** - dem Einschränkungsgrad (Auswirkungen, Schadensausmaß) und den Eintrittswahrscheinlichkeiten - basierendes, **4-stufiges Modell**. Ein bereits etabliertes Risikomanagement kann in diese Methodik eingefügt werden, indem die Betreiber ihre betriebsspezifischen Ausprägungen für den **Einschränkungsgrad "E"** und die die **Eintrittswahrscheinlichkeiten "P"** festlegen.

Die nachfolgende Tabelle verdeutlicht dies schematisch. Hierbei sind die "grau" unterlegten Bereiche von den Betreibern - analog der festgelegten Wertebereiche ihres Risikomanagements - zu konkretisieren. Die Variablen "E" (≈ Einschränkungsgrad) und "P" (≈ Wahrscheinlichkeit) sind für die jeweiligen Stufen festzulegen.

Gewählte vier Stufen bei Einschränkungsgrad und Eintrittswahrscheinlichkeit:

Stufe	Einschränkungsgrad		Eintrittswahrscheinlichkeit	
1	geringe/ keine Auswirkung auf die kDL	**E%** Betroffenheitsgrad (Versicherte) im Rahmen der kDL	**P%** Wahrscheinlichkeit	Unwahrscheinlich
2	mittlere Auswirkung auf die kDL	**E%** Betroffenheitsgrad (z. B. Versicherte) im Rahmen der kDL	**P%** Wahrscheinlichkeit	Wenig wahrscheinlich
3	hohe Auswirkung auf die kDL	**E%** Betroffenheitsgrad (z. B. Versicherte) im Rahmen der kDL	**P%** Wahrscheinlichkeit	Wahrscheinlich
4	kritische Auswirkung auf die kDL	**E%** Betroffenheitsgrad (z. B. Versicherte) im Rahmen der kDL	**P%** Wahrscheinlichkeit	Sehr wahrscheinlich

Tabelle 5: Stufen Einschränkungsgrad und Eintrittswahrscheinlichkeit

Die Zielrichtung der Bemessung muss für kritische Infrastrukturen / kritische Dienstleistungen weniger an den betriebsinternen Ausmaßen als vielmehr an dem Einschränkungsgrad für die Versorgung der gesetzlich Kranken- und Pflegeversicherten orientiert werden.

4.3.2 Schritt 1 – Gefährdungsanalyse

Anhand des GKV/PV-Gefährdungskatalogs (siehe Kapitel 6.3) werden Bedrohungen und Schwachstellen auf die kDL untersucht. Dabei werden Risiken unter Beachtung bereits etablierter Sicherheitsmaßnahmen mit Fokus auf die Schutzziele ermittelt.

4.3.3 Schritt 2 – Risikobewertung

Auf Basis der Einschätzung aller als anwendbar deklarierten Gefährdungen aus dem Gefährdungskatalog können die Risiken hinsichtlich Eintrittswahrscheinlichkeit und Einschränkungsgrad bewertet und in einer Risikomatrix eingestuft werden:

Einschränkungsgrad (E) x Eintrittswahrscheinlichkeit (P) = Risiko

Im Rahmen der Risikobewertung können im individuellen Risikomanagementprozess vom Betreiber vier **Relevanzklassen** gebildet werden, welche mit Handlungsempfehlungen konkretisiert werden sollen.

Die **Relevanzklassen** dienen der **Gewichtung von Risiken** (hier als **Belastung** bezeichnet), sowohl unter den Gesichtspunkten von Eintrittswahrscheinlichkeit (P), als auch potenzieller Auswirkung auf die kDL (Einschränkungsgrad).

Relevanzklasse	Belastung
A (ROT)	aktuell sehr hohe potenzielle Belastung
B (ORANGE)	aktuell hohe potenzielle Belastung
C (GELB)	aktuell mittlere potenzielle Belastung
D (GRÜN)	aktuell geringe potenzielle Belastung

Tabelle 6: Beispielhafte Relevanzklassen

Die ermittelten Risiken werden in einer priorisierten Liste dokumentiert. Die Darstellungsform kann in Form einer Matrix erfolgen, welche die Relevanzklassen visualisiert (hier A bis D):

Einschränkungsgrad (E)	kritische Auswirkung auf kDL	B	A	A	A
	hohe Auswirkung auf kDL	C	B	B	A
	mittlere Auswirkung auf kDL	D	C	C	B
	geringe/ keine Auswirkung auf kDL	D	D	D	D
		P% unwahrscheinlich	P% wenig wahrscheinlich	P% wahrscheinlich	P% sehr wahrscheinlich
		Eintrittswahrscheinlichkeit (P)			

Tabelle 7: Beispielhafte Risikomatrix

4.3.4 Schritt 3 – Risikobehandlung

Anhand der bewerteten Risiken sind die Anforderungen an die Sicherheitsmaßnahmen zur Risikobehandlung abzuleiten. Dabei wird nicht das materielle Schadensausmaß, sondern der Einschränkungsgrad des Anlagenbetriebs bei Eintritt der möglichen Störung ermittelt und bewertet. Die Ergebnisse sind zu begründen und zu dokumentieren.

Zur Risikobehandlung stehen theoretisch die vier klassischen Optionen „vermeiden“, „mindern“, „abwälzen“ und „akzeptieren“ zur Verfügung, die aufzeigen, wie mit identifizierten Risiken grundsätzlich verfahren werden kann.

Aufgrund der Vorgaben des BSIG sind bezüglich der kDL für die Betreiber grundsätzlich nur die Optionen „Risiken vermeiden“ und „Risiken mindern“ zulässig. Die Option der Risikoakzeptanz ist in Bezug auf das Schutzziel Verfügbarkeit nur in begründeten Ausnahmefällen zulässig.

Die Einstufung von Risiken erfolgt aufgrund der zum Zeitpunkt der Risikoanalyse ermittelten Einschränkungsgrade und Eintrittswahrscheinlichkeiten. Daher sind sämtliche Risiken durch den Betreiber regelmäßig zu überprüfen. Es ist zu bewerten, ob zugrunde gelegte Schadenshöhen, Gefährdungen und Sicherheitsmaßnahmen der aktuellen Situation entsprechen oder angepasst werden müssen.

Die Ergebnisse der Risikobewertung sind nachvollziehbar in einem IS-Risikobehandlungsplan, in welchem die relevanten betrachteten kDL und die jeweils auf sie wirkenden Risiken eingestuft worden sind, zu dokumentieren.

Resultierende Sicherheitsmaßnahmen sind – intern und / oder durch (IT-)Dienstleister – zur Umsetzung einzuplanen. Dabei sind für jede Sicherheitsmaßnahme konkrete Zuständigkeiten, Verantwortlichkeiten und Fristen für die Umsetzung festzulegen und zu dokumentieren. Die inhaltlich korrekte und vollständige sowie fristgerechte Umsetzung der Sicherheitsmaßnahmen ist nachzuverfolgen und zu dokumentieren.

4.3.5 Schritt 4 – Risikosteuerung

Das Informationssicherheits-Risikomanagement muss als nachhaltiger Prozess etabliert werden, um die Anforderungen des BSIG zu erfüllen. Dazu müssen Risiken initial identifiziert und dann aktiv gesteuert werden. Dies bedeutet neben der bereits beschriebenen Risikoidentifikation und der Nachverfolgung der Umsetzung festgelegter Sicherheitsmaßnahmen auch, dass die Risikosituation regelmäßig aktualisiert, die Angemessenheit der Sicherheitsmaßnahmen kontrolliert sowie adressatengerecht über die Risikosituation berichtet wird.

Der Informationssicherheits-Risikomanagement-Prozess und seine zugrunde gelegte Methodik inklusive des Gefährdungskatalogs und weiterer mitgeltender Dokumentationen müssen einem kontinuierlichen Verbesserungsprozess (KVP) unterliegen.

GKV/PV-spezifische Hinweise:

Weitergehende spezifische Anforderungen ergeben sich nicht.

Mindestens umzusetzende Anforderungen nach ISO 27001:

Kap. 6.1	Risiken und Chancen müssen bestimmt und betrachtet werden, um sicherzustellen, dass das Informationssicherheitsmanagementsystem seine beabsichtigten Ergebnisse erzielen kann, unerwünschte Auswirkungen zu verhindern oder zu verringern und fortlaufende Verbesserung zu erreichen.

4.4 Continuity- und Notfallmanagement für kDL

Ziel des Continuity Managements ist es, die kDL auch in Störungssituationen zu jeder Zeit in einer angemessenen Mindestqualität aufrechtzuerhalten. Dabei ist es wichtig sicherzustellen, dass eine geeignete Verzahnung des Continuity Managements für die kDL mit den Bereichen, welche die Anforderungen des Business Continuity Managements (BCM[6]) umsetzen, gegeben ist.

Es muss für die kritischen Dienstleistungen kein eigenes BCMS[7] aufgebaut werden, wenn ein BCMS oder ein adäquater Continuity-Management-Prozess für das Unternehmen bereits besteht, dessen Geltungsbereich mindestens die für die kDL relevanten Prozesse abdeckt.

Erreicht werden muss dies durch einen im Vorfeld definierten Plan zur Aufrechterhaltung der kDL. Der oder die (Business) Continuity Plan bzw. Pläne (BCP) muss bzw. müssen dabei der zu erstellenden Strategie für Kontinuität und Wiederanlauf sowie einer im Vorfeld zu erstellenden Business Impact Analyse (BIA) folgen und die Themen Notfall-, Ersatzverfahren und Wiederanlaufplan aufgreifen. Dabei ist zu ermitteln, welche Komponenten zu einem Ausfall der gesamten kDL führen können („Single Point of Failure“) und deshalb mit besonderen Sicherheitsmaßnahmen belegt werden müssen.

Um die kDL möglichst vor Fehlfunktionen der IT, sowohl vorsätzlich als auch unbeabsichtigt ausgelöst, zu schützen, ist eine möglichst robuste bzw. widerstandfähige Systemarchitektur für die kritische Dienstleistung zu wählen.

Sofern Teile oder die Gesamtheit des Anlagenbetriebs für die kDL durch einen Dienstleister ausgeführt werden, sind die Vorgaben und abgeleitete Sicherheitsmaßnahmen zum Continuity Management beim Dienstleister umzusetzen, zu steuern und vom Auftraggeber regelmäßig auf deren Wirksamkeit zu überprüfen.

Für die kDL müssen Übungen – wo erforderlich unter Einbezug von Dienstleistern und Fachverantwortlichen – sowie Systemtests durchgeführt werden, um die Wirksamkeit im Notfall sicherzustellen.

Dies muss unter Wahrung der Vorgaben des im Continuity Management geforderten Notfallmanagements erfolgen. Dabei ist im Rahmen von Übungen sowie bei Training seltener Ereignisse sicherzustellen, dass Kommunikationswege definiert und anwendbar sind. Die Erkenntnisse aus den Übungen müssen dokumentiert und zur kontinuierlichen Verbesserung der Planungen herangezogen werden.

GKV/PV-spezifische Hinweise:

Anforderungen an Verfügbarkeiten für Prozesse der kDL sind im Kapitel 1.1.2 beschrieben.

Notfallübungen sollen jährlich unter Einbeziehung der relevanten Parteien (z. B. Fachverantwortliche, Dienstleister) und Rollen durchgeführt werden.

Mindestens umzusetzende Anforderungen nach ISO 27001 Annex A:

5.29	Informationssicherheit bei Störungen
5.30	IKT-Bereitschaft für Business Continuity
8.14	Redundanz von informationsverarbeitenden Einrichtungen

[6] BCM und BCMS werden in der folgenden Norm behandelt: EN ISO 22301 – Sicherheit und Resilienz – Business Continuity Management System - Anforderungen

[7] Das BCMS umfasst den organisatorischen Aufbau, Leitlinien, Planungstätigkeiten, Verantwortlichkeiten, Verfahren, Prozesse und Ressourcen.

Mindestens umzusetzende Vorgaben nach ISO 22301:

6.1	Maßnahmen zum Umgang mit Risiken und Möglichkeiten
6.2	Ziele zur Aufrechterhaltung der Betriebsfähigkeit und Planung zu deren Erreichung
8.1	Betriebliche Planung und Steuerung
8.2	Business Impact-Analyse und Risikobeurteilung
8.3	Strategien und Lösungen zur Aufrechterhaltung der Betriebsfähigkeit
8.4	Pläne und Verfahren zur Aufrechterhaltung der Betriebsfähigkeit
8.5	Übungsprogramm

4.5 Branchenspezifische Technik

Eine technisch bedingte, branchenspezifische Gefährdungslage, die gesondert im Sinne der kDL zu betrachten wäre, existiert nicht. Die technischen Sicherheitsmaßnahmen dieses B3S-GKV/PV sind auf Anwendbarkeit im Rahmen der Risikobetrachtung zu überprüfen (siehe Kapitel 4.6).

GKV/PV-spezifische Hinweise:

Anforderungen an den Betreiber, welche sich aufgrund der branchenspezifischen Vorgaben zu Ausgabe und Betrieb der eGK ergeben, sind zu beachten, insbesondere auch die Prozesse im Zusammenhang mit der Ausstellung von Berechtigungsscheinen als Notfall-/ Ausweichverfahren bei nachhaltigen Störungen der Telematik-Infrastruktur.

Umzusetzende Vorgaben nach ISO 27001:

Die anwendbaren technischen Sicherheitsmaßnahmen sind dem Kapitel 4.6 zu entnehmen.

4.6 Technische Informationssicherheit – Kategorien von Sicherheitsanforderungen

Die nachfolgende Tabelle greift die vom BSI für einen B3S empfohlenen technischen Anforderungen auf und bildet sie auf die korrespondierenden Maßnahmen des Annex A der ISO 27001 ab.

Sind genannte Kategorien von Sicherheitsanforderungen im Kontext des B3S beim Betreiber nicht relevant oder nicht anwendbar, so ist dies nachvollziehbar darzulegen.

GKV/PV-spezifische Hinweise:

Weitergehende spezifische Anforderungen ergeben sich nicht.

Mindestens umzusetzende Anforderungen nach ISO 27001 Annex A:

ISO 27001 – Annex A Maßnahmen *(nur technische Maßnahmen)*		A1 Absicherung von Netzübergängen	A2 Sichere Interaktion im Internet	A3 Sichere Software (insbes. Vermeidung von offenen Sicherheitslücken)	A4 Sichere und zuverlässige Hardware	A5 Sichere Authentisierung	A6 Verschlüsselung	A7 Sonstiges	Branchenrelevanz für GKV/PV
5.14	Informationsübermittlung		x				x		Ja
5.15	Zugangssteuerung	x				x			Ja
5.16	Identitätsmanagement					x			Ja
5.17	Authentisierungsinformationen					x			Ja
5.18	Zugangsrechte					x			Ja
6.7	Remote-Arbeit	x							Ja
7.4	Physische Sicherheitsüberwachung							x	Ja
7.7	Aufgeräumte Arbeitsumgebung und Bildschirmsperren				x				Ja
7.10	Speichermedien			x	x		x		Ja
7.14	Sichere Entsorgung oder Wiederverwendung von Geräten und Betriebsmitteln			x	x				Ja
8.1	Endpunktgeräte des Benutzers	x			x		x		Ja
8.2	Privilegierte Zugangsrechte				x	x			Ja
8.3	Informationszugangsbeschränkung					x			Ja
8.4	Zugriff auf den Quellcode			x		x		x	Ja
8.5	Sichere Authentisierung					x			Ja
8.6	Kapazitätssteuerung				x			x	Ja
8.7	Schutz gegen Schadsoftware	x	x	x	x			x	Ja
8.8	Handhabung von technischen Schwachstellen	x		x	x			x	Ja
8.9	Konfigurationsmanagement		x	x					Ja
8.11	Datenmaskierung						x		Ja

ISO 27001 – Annex A Maßnahmen *(nur technische Maßnahmen)*		A1 Absicherung von Netzübergängen	A2 Sichere Interaktion im Internet	A3 Sichere Software (insbes. Vermeidung von offenen Sicherheitslücken)	A4 Sichere und zuverlässige Hardware	A5 Sichere Authentisierung	A6 Verschlüsselung	A7 Sonstiges	Branchenrelevanz für GKV/PV
8.13	Sicherung von Informationen			x			x	x	Ja
8.14	Redundanz von informationsverarbeitenden Einrichtungen				x				Ja
8.15	Protokollierung	x	x	x	x				Ja
8.17	Uhrensynchronisation							x	Ja
8.18	Gebrauch von Hilfsprogrammen mit privilegierten Rechten				x	x		x	Ja
8.19	Installation von Software auf Systemen im Betrieb		x	x	x				Ja
8.20	Netzwerksicherheit	x	x						Ja
8.21	Sicherheit von Netzwerkdiensten	x	x	x			x		Ja
8.22	Trennung von Netzwerken	x	x	x					Ja
8.24	Verwendung von Kryptographie						x		Ja
8.26	Anforderungen an die Anwendungssicherheit		x				x		Ja
8.30	Ausgegliederte Entwicklung				x				Ja
8.31	Trennung von Entwicklungs-, Test- und Produktionsumgebungen			x					Ja
8.32	Änderungssteuerung			x	x				Ja

Tabelle 8: Mapping Annex A ISO 27001 zu technischen Sicherheitsmaßnahmen BSI

4.7 Personelle und organisatorische Sicherheit

Anforderungen an den Einstellungs-, Veränderungs- und Austrittsprozess (sog. EVA-Prozess) von geeigneten Mitarbeitern, Auftragnehmern und Dritten sowie an die Sensibilisierung, Ausbildung und Schulung bezüglich Informationssicherheit sind zu definieren, um Risiken bei der Nutzung von informationsverarbeitenden Einrichtungen zu minimieren.

Dazu gehört eine Beschreibung von Verfahren zur Überprüfung von Bewerbern, Auftragnehmern und Dritten und zur vertraglichen Verpflichtung auf Sicherheitsvorschriften und -verantwortlichkeiten. Weiterhin sind Festlegungen zum Management von Identitäten, Berechtigungen und Kompetenzen, der ordnungsgemäßen Rückgaben von organisationseigenen Werten bei Einstellungen, Änderungen oder bei Beendigung des Vertrags- oder Anstellungsverhältnisses vorzusehen.

Entsprechend der Aufbauorganisation sind Rollenzuweisungen / Berechtigungen (siehe auch Kapitel 4.13) und Ressourcen zu definieren und zu etablieren. Gegebenenfalls sind Festlegungen zu treffen, z. B. zum Vieraugenprinzip oder zu Funktionstrennungen.

Ein Verfahren, um bei Beschäftigten, Dienstleistern und Dritten ein angemessenes Maß an Bewusstsein für die Schutzziele der Informationssicherheit zu schaffen, muss etabliert sein.

Um ein angemessenes Bewusstsein für die Schutzziele der Informationssicherheit des Unternehmens zu erreichen, müssen alle Beschäftigten einer Organisation entsprechend geschult werden. Diese Awareness-Maßnahmen sollen zu Beginn des Beschäftigungsverhältnisses sowie in angemessenen und regelmäßigen Abständen erfolgen. Ziel muss es sein, das grundlegende Bewusstsein aller Beschäftigten für die Themen der Informationssicherheit zu stärken und diesen Personenkreis weiter zu sensibilisieren. Dabei sind aktuelle gesetzliche und gesellschaftliche Entwicklungen sowie die Compliance (siehe Kapitel 4.15) zu beachten.

Beschäftigte, die im Rahmen ihrer Tätigkeit einen Zugriff auf besonders sensible und schützenswerte Informationen haben, z. B. Personalverantwortliche und Systemadministratoren, sollen explizite und erweiterte Schulungen erhalten. So sollen über die Grundlagenschulung hinaus, weitergehende bedarfsgerechte und risikoorientierte Schulungsinhalte vermittelt werden. Bei der Feststellung des Schulungsbedarfe und der Schulungsinhalte handelt es sich um einen dynamischen Prozess, der kontinuierlich bewertet und den aktuellen Entwicklungen angepasst werden muss.

Die oberste Leitung des jeweiligen Betreibers muss in Bezug auf das Informationssicherheits- und das Risiko-Managementsystem (ISMS, RMS) Führung und Verpflichtung zeigen. In einer Managemententscheidung müssen die Informationssicherheits- und die Risikomanagementleitlinie(-politik) sowie die Informationssicherheitsziele festgelegt werden. Die strategische Ausrichtung der Organisation muss die Themen der Informationssicherheit entsprechend beachten. Der weitere Ausbau, die fortlaufende Eignung, Angemessenheit und Wirksamkeit des ISMS muss, im Rahmen des kontinuierlichen Verbesserungsprozesses, gesichert und optimiert werden. Dafür angemessene Ressourcen sind von der Unternehmensleitung bereitzustellen.

GKV/PV-spezifische Hinweise:

Die oben genannten Vorgaben sollten für alle Beschäftigten von Betreibern einer kDL in der GKV/PV einheitlich etabliert werden. Besonderheiten ergeben sich aus den Regelungen des § 35 SGB I i.V.m. § 1 des Gesetzes über die förmliche Verpflichtung nichtbeamteter Personen (Verpflichtungsgesetz) sowie den weiteren Regelungen zum Sozialdatenschutz in §§ 67 ff. SGB X.

Mindestens umzusetzende Anforderungen nach ISO 27001 inklusive Annex A:

Kap. 7.2	Kompetenz
Kap. 7.3	Bewusstsein
5.2	Informationssicherheitsrollen und -verantwortlichkeiten
5.3	Aufgabentrennung
5.4	Verantwortlichkeiten der Leitung
5.16	Identitätsmanagement
5.37	Dokumentierte Betriebsabläufe
6.1	Sicherheitsüberprüfung

6.2	Beschäftigungs- und Vertragsbedingungen
6.3	Informationssicherheitsbewusstsein, -ausbildung und -schulung
6.4	Maßregelungsprozess
6.5	Verantwortlichkeiten bei Beendigung oder Änderung der Beschäftigung
6.6	Vertraulichkeits- oder Geheimhaltungsvereinbarungen
6.7	Remote-Arbeit
7.7	Aufgeräumte Arbeitsumgebung und Bildschirmsperren

4.8 Bauliche / physische Sicherheit

Es sind Anforderungen an die physische Sicherheit von Gebäuden, Räumlichkeiten und Standorten sowie an Betriebsmittel (z. B. IT-Ausstattung, Infrastrukturkomponenten usw.) zu erstellen, mit dem Ziel, den Verlust, die Beschädigung, den Diebstahl, die Kompromittierung oder die Unterbrechung der kDL zu verhindern.

In jedem Fall sind die Maßnahmen aus der Orientierungshilfe des BSI für einen B3S zur baulichen / physischen Sicherheit zu berücksichtigen:

- A 5.15 Zugangssteuerung
- A 7.11 Versorgungseinrichtungen
- A 8.14 Redundanz von informationsverarbeitenden Einrichtungen

Konkret und abhängig von der Gefährdungslage sind z. B. folgende Maßnahmen zu ergreifen:

- Maßnahmen gegen umfeldbezogene Gefährdungen (z. B. Naturkatastrophen, Unfälle).
- Physischer Schutz: Bauliche Sicherheit bezüglich Fenster, Türen, Brandabschnitte, Trassenverläufe.
- Brandmelde- und Löschtechnik: Brand und Rauchdetektion (z. B. mit Aufschaltung auf die Feuerwehr), Löschanlagen, Etablierung von Abschaltfunktionen für Anlagen und weitere Maßnahmen zur Schadensbegrenzung.
- Sicherheitssysteme zur Zutrittskontrolle: Zutrittskontrollanlage, Einbruchmeldeanlage, Aufschaltung auf ständig besetzte Sicherheitszentrale.
- Versorgungseinrichtungen: Nach einschlägigen Normen erbrachte Installation mit Überspannungsschutz und entsprechender Notstromversorgung (z. B. Dieselaggregat, Netzsynchronisationsanlage), Wasserversorgung.
- Raumlufttechnische Einrichtungen: Kühlung und Klimatisierung der IT-Infrastruktur und der Infrastrukturkomponenten sind durch Kühlmechanismen gewährleistet.
- Wartung und Instandhaltung: Einrichtungen werden regelmäßig geprüft, die regelmäßige Wartung ist durch entsprechende Pläne und Verträge sichergestellt.

GKV/PV-spezifische Hinweise:

Weitergehende spezifische Anforderungen ergeben sich nicht.

Mindestens umzusetzende Anforderungen nach ISO 27001 Annex A:

7.1	Physische Sicherheitsperimeter
7.2	Physischer Zutritt
7.3	Sichern von Büros, Räumen und Einrichtungen
7.4	Physische Sicherheitsüberwachung
7.5	Schutz vor physischen und umweltbedingten Bedrohungen
7.6	Arbeiten in Sicherheitsbereichen
7.8	Platzierung und Schutz von Geräten und Betriebsmitteln
7.9	Sicherheit von Werten außerhalb der Räumlichkeiten
7.11	Versorgungseinrichtungen
7.12	Sicherheit der Verkabelung
7.13	Instandhaltung von Geräten und Betriebsmitteln

4.9 Vorfallserkennung und -bearbeitung

Anforderungen an eine frühestmögliche Erkennung, die Meldung, die Dokumentation und an die Reaktion von Angriffen und IT-Vorfällen/Störungen (Incidents) müssen spezifiziert werden. Dabei ist zwischen Angriffen und IT-Vorfällen/Störungen zu unterscheiden. Die Vorfallsarten sind entsprechend zu bewerten und nachzuverfolgen.

Es sind technische Vorkehrungen (z. B. Intrusion Detection und Intrusion Prevention Systeme) zur Vorfallserkennung und zur Unterstützung der Vorfallsbehebung zu etablieren (siehe auch Kapitel 4.6 und 4.16).

Ein Prozess zum Vorfallsmanagement mit unverzüglichen Meldepflichten sowie der Betrieb einer jederzeit erreichbaren Kontaktstelle gegenüber dem BSI müssen organisiert und umgesetzt sein.

Im Rahmen der Behandlung von Vorfällen sollten Vorgehensweisen für den Fall des Einsatzes forensischer Mittel (Hilfe zur Abwägung zwischen Schadensbegrenzung und Wiederherstellung der kDL einerseits und Beweissicherung, Einschaltung von Behörden und Experten andererseits) vorgesehen und im Ablauf berücksichtigt werden.

Die folgende Darstellung zeigt einen generischen und exemplarischen Ablauf zur operativen Umsetzung des „Umgangs mit Vorfällen“ (Incident-Prozess) inkl. Des Lernens aus Vorfällen. Die Ausprägung dieses Prozesses ist an der individuellen Aufbau- und Ablauforganisation des Betreibers und betroffener Dienstleister auszurichten und muss die Schnittstellen zum Continuity- und Notfallmanagement (siehe Kapitel 4.4) und zum Problem-Management[8] mit aufgreifen.

Für Betreiber kritischer Anlagen sind die Meldepflichten nach § 8b Absatz 4 BSIG zu beachten.

[8] Problem-Management analysiert mögliche oder bereits eingetretene Angriffe und Vorfälle und identifiziert daraus Probleme. Ein wesentliches Ziel ist hierbei die 'dauerhafte Problemlösung'.

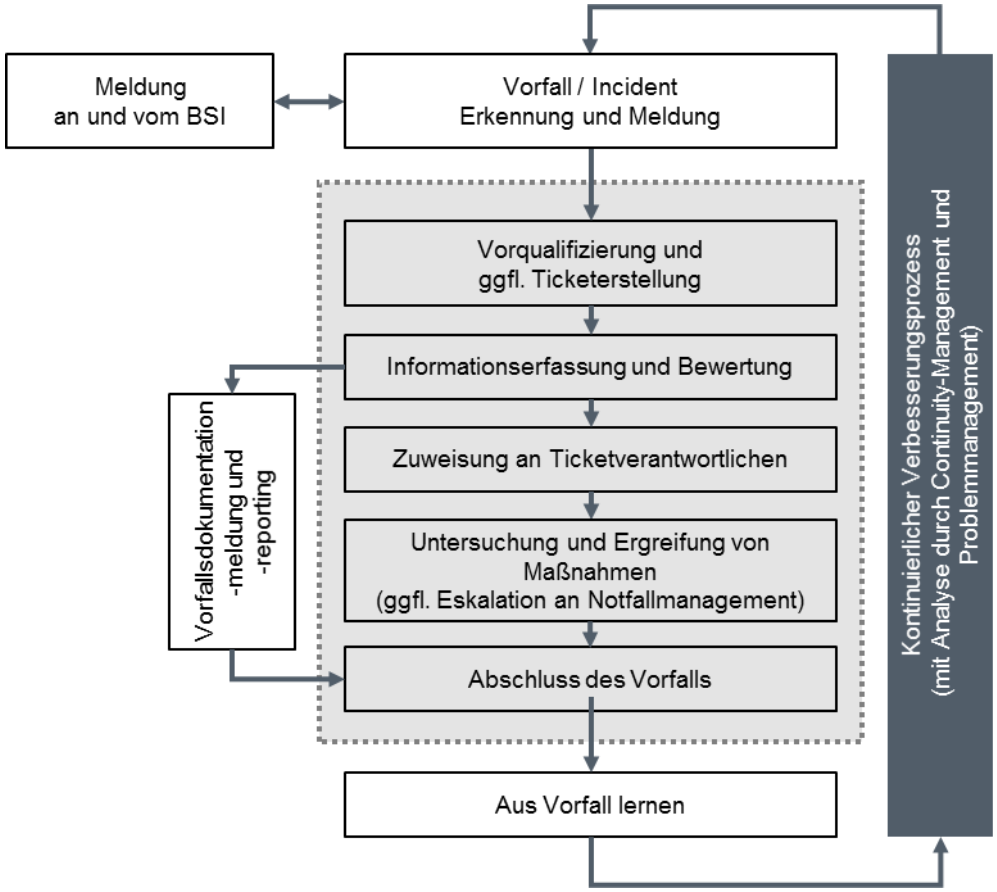

Abbildung 4: Ablauf zur operativen Umsetzung des „Umgangs mit Vorfällen“

GKV/PV-spezifische Hinweise:

Weitergehende spezifische Anforderungen ergeben sich nicht.

Mindestens umzusetzende Anforderungen nach ISO 27001 Annex A:

5.24	Planung und Vorbereitung der Handhabung von Informationssicherheitsvorfällen
5.25	Beurteilung und Entscheidung über Informationssicherheitsereignisse
5.26	Reaktion auf Informationssicherheitsvorfälle
5.27	Erkenntnisse aus Informationssicherheitsvorfällen
5.28	Sammeln von Beweismaterial
6.8	Meldung von Informationssicherheitsereignissen
8.16	Überwachung von Aktivitäten

4.10 Überprüfung im laufenden Betrieb

Für die Überprüfung und Weiterentwicklung eines angemessenen und funktionstüchtigen Sicherheitsniveaus nach Stand der Technik sind für den Betrieb der Anlagen kontinuierliche Prüfungen und Übungen dem Risiko entsprechend durchzuführen. Diese sollen z. B. Penetrationstests, prozessuale, technische oder organisatorische Audits (wie z. B. systematische Log-Auswertungen), Revisionen und Übungen mit relevanten Dienstleistern im Kontext der Erbringung der kDL umfassen und auch außerhalb des vom BSIG vorgegebenen Prüfzyklus und Prüfumfangs oder bei nicht zuverlässig erklärbaren Beeinträchtigungen erfolgen.

GKV/PV-spezifische Hinweise:

Technische Überprüfungen (z. B. Penetrationstests) sollen jährlich mit jeweils wechselnden Schwerpunkten durchgeführt werden.

Mindestens umzusetzende Anforderungen nach ISO 27001 Annex A:

5.35	Unabhängige Überprüfung der Informationssicherheit
5.36	Einhaltung von Richtlinien, Vorschriften und Normen für die Informationssicherheit
8.15	Protokollierung
8.29	Sicherheitsprüfung in Entwicklung und Abnahme
8.32	Änderungssteuerung
8.34	Schutz der Informationssysteme während Tests im Rahmen von Audits

4.11 Externe Informationsversorgung und Unterstützung

Der Betreiber einer Anlage/ eines Systems der GKV/PV sollte – insbesondere als KRITIS-Betreiber – externe Informationen/ Dienstleistungen zur IT-Sicherheit – wie z. B. die des BSI – regelmäßig in Anspruch nehmen, für seine Organisationbelange auswerten und geeignete Sicherheitsmaßnahmen hieraus ableiten.

Für den Fall von Störungen für seinen Anlagen-/ Systembetrieb müssen entsprechende Kontakte zu geeigneten und kundigen Herstellern und Experten jederzeit verfügbar sein.

Erfolgt der Betrieb durch einen Dienstleister, muss dieser analog über entsprechende Informationsquellen und Zugriff auf Spezialisten verfügen.

GKV/PV-spezifische Hinweise:

Weitergehende spezifische Anforderungen ergeben sich nicht.

Mindestens umzusetzende Anforderungen nach ISO 27001 Annex A:

5.6	Kontakt mit speziellen Interessensgruppen

4.12 Lieferanten, Dienstleister und Dritte

Der Betreiber hat geeignete Vorkehrungen (z. B. vertragliche Regelungen, SLAs oder Monitoring) für extern erbrachte Dienstleistungen zu treffen, wenn er IT-Komponenten oder Anwendungen von Lieferanten bezieht (z. B. Eingangsprüfungen, Sicherheitstests). Damit sollen externe Dienstleister sicher und mit entsprechender Qualität in den Betrieb der kDL oder in die Wartung von Systemen sowie Komponenten eingebunden bzw. eigene Leistungen geeignet an Externe (inkl. Arbeitsgemeinschaften, siehe auch Kapitel 1.2) ausgelagert werden.

Um Anforderungen bei der externen Partei durchsetzen zu können, müssen entsprechende vertragliche Regelungen vereinbart werden. Die Vertragsentwürfe müssen vor ihrem Abschluss hinsichtlich ihrer Vollständigkeit und inhaltlichen Richtigkeit überprüft werden, wobei Anforderungen von zentralen Organisationseinheiten (z. B. Justiziariat, Einkauf, Datenschutz) zu berücksichtigen sind.

Die vertraglichen Vereinbarungen müssen in regelmäßigen Abständen überprüft und ggf. angepasst werden. Gründe für Anpassungen sind z. B. Änderungen in der Dienstleistungserbringung oder veränderte gesetzliche oder Sicherheitsanforderungen. Insbesondere sollen gemäß ISO 27002, Punkt 5.22 folgende Anforderungen umgesetzt werden:

e. Durchführung von Lieferanten- und Unterlieferanten-Audits in Verbindung mit der Überprüfung der ggf. verfügbaren Auditberichte sowie Nachverfolgung der festgestellten Probleme,
f. Bereitstellung von Informationen zu Informationssicherheitsvorfällen und Überprüfung dieser Informationen entsprechend den vertraglichen Anforderungen sowie jedweder unterstützenden Richtlinien und Verfahren.

Von den Betreibern ist zu dokumentieren, welche Dienstleister durch eine Störung ihrer Leistungserbringung die Funktionstüchtigkeit der Krankenkasse oder die Sicherheit der verarbeiteten Versicherteninformationen beeinträchtigen könnten.

GKV/PV-spezifische Hinweise:

Eine Besonderheit für die GKV/PV sind gemäß § 85 SGB IV die Einholung einer Genehmigung (z. B. Erwerb und Leasing von Grundstücken, Errichtung, Erweiterung oder Umbau von Gebäuden) bzw. die vorherige Anzeige (z. B. Ankauf, Leasing, Anmietung oder Beteiligung an Datenverarbeitungsanlagen und -systemen) bei der Aufsichtsbehörde.

Weiterhin ist gemäß § 80 SGB X die vorherige Anzeige der Verarbeitung von Sozialdaten im Auftrag bei der Rechts- oder Fachaufsichtsbehörde erforderlich und gemäß § 197b SGB V das Verbot der Auslagerung wesentlicher Aufgaben zu beachten.

Sofern eine Störung der Verfügbarkeit, Integrität oder Vertraulichkeit der informationstechnischen Systeme, Komponenten oder Prozesse eines IT-Dienstleisters zu einer Beeinträchtigung der Funktionsfähigkeit der jeweiligen Krankenkasse oder der Sicherheit der verarbeiteten Versicherteninformationen führen kann, muss die Krankenkasse durch geeignete vertragliche Vereinbarungen sicherstellen, dass die Einhaltung des branchenspezifischen Sicherheitsstandards B3S-GKV/PV gewährleistet wird (vgl. §392 Abs. 6 SGB V).

Der Betreiber der kritischen Anlage bleibt bei Beauftragung eines Dienstleisters für die Umsetzung des B3S-GKV/PV und für die abschließende Risikoeinschätzung im Kontext seiner kDL-Prozesse verantwortlich und entscheidet, ob ein Restrisiko vertretbar ist oder nicht. Es sind angemessene organisatorische und technische Vorkehrungen zur Vermeidung von Störungen umzusetzen. Organisatorische und technische Vorkehrungen sind angemessen, wenn der dafür erforderliche Aufwand nicht außer Verhältnis zu den Folgen eines Ausfalls oder einer Beeinträchtigung der betroffenen Kritischen Infrastruktur steht (§ 8a Abs. 1 BSIG).

Vor diesem Hintergrund sind nachfolgend die zentralen Anforderungen des B3S-GKV/PV als Mindestanforderungen zusammengefasst. Diese müssen im Rahmen der Risikobewertung des Auftraggebers um weitergehende Absicherungsmaßnahmen ergänzt werden, wenn das Restrisiko der Verarbeitung ansonsten als nicht akzeptabel eingeschätzt wird.

Eine vertragliche Vereinbarung zur Gewährleistung der Einhaltung des B3S-GKV/PV ist mit IT- Dienstleistern, zu treffen, die

a) IT-Dienstleistungen im Rahmen der gesetzlichen Aufgabenerfüllung der Krankenkasse erbringen,

b) bei Störungen ihrer Dienstleistung die Funktionsfähigkeit der Krankenkasse oder

c) die Sicherheit der verarbeiteten Versicherteninformationen gefährden.

Die entsprechende vertragliche Vereinbarung muss folgende Regelungen enthalten:

Der Auftragnehmer, welcher IT-Dienstleistungen im Sinne dieses B3S erbringt, muss mindestens

A) ein System zur Angriffserkennung gemäß Ziffer 4.16 betreiben,

B) spezifische Anforderungen des Auftraggebers an die Verfügbarkeit, z. B. im Rahmen von Service Level Agreements, akzeptieren (vgl. auch *Tabelle 3: Prozesse der kDL und Verfügbarkeitsanforderungen*),

C) Risiken für die Informationssicherheit seiner Dienstleistungen erkennen und nach Stand der Technik angemessen mitigieren; Risikoakzeptanz oder Risikotransfer sind nicht zulässig, wenn Risiken noch durch angemessene Maßnahmen vermieden oder reduziert werden können (vgl. Ziffer 3.2),

D) den Auftraggeber über den Eintritt oder den möglichen Eintritt von Sicherheitsvorfällen für seine Dienste unverzüglich informieren,

E) Maßnahmen und Pläne zur Aufrechterhaltung oder Wiederherstellung seiner Dienstleistung etabliert haben (vgl. Abschnitt 4.4 und ISO 27002, 5.22, lit. k)

F) dem Auftraggeber Überprüfungen einschließlich Inspektionen ermöglichen.

Nimmt ein Dienstleister die Unterstützung eines weiteren Dritten in Anspruch, um Dienstleistungen im Namen des Auftraggebers zu erbringen, so sind diesem Dritten dieselben Pflichten aufzuerlegen, die in dem Vertrag zwischen dem Auftraggeber und dem Dienstleister festgelegt sind. Die Durchsetzung und die Überwachung dieser Pflichten obliegt dabei dem Dienstleister.

Mindestens umzusetzende Anforderungen nach ISO 27001 Annex A:

5.14	Informationsübermittlung
5.19	Informationssicherheit in Lieferantenbeziehungen
5.20	Behandlung von Informationssicherheit in Lieferantenvereinbarungen
5.21	Umgang mit der Informationssicherheit in der Lieferkette der Informations- und Kommunikationstechnologie (IKT)
5.22	Überwachung, Überprüfung und Änderungsmanagement von Lieferantendienstleistungen
8.30	Ausgegliederte Entwicklung

4.13 Zugangs- und Zugriffskontrolle

Der Betreiber einer Anlage / eines Systems der GKV/PV muss für einen angemessenen Schutz der Informationen durch technische, prozessuale und organisatorische Maßnahmen zum Zugangs- und Zugriffsschutz sorgen. Es sind Anforderungen an den Zugang zu Anlagen/Systemen und die Zugriffsrechte (u.a. über Berechtigungskonzeptionen) festzulegen. Ziel ist, unbefugte Zugänge und Zugriffe durch Regelungen zur Vergabe, Überprüfung und Entzug von Nutzerkonten und -rechten sowie zur Nutzerauthentifizierung zu verhindern.

Die Vorgaben müssen gleichermaßen für Beschäftigte des Betreibers sowie für Externe gelten.

Für die Vergabe, die Überprüfung und den Entzug von Nutzerkonten und -rechten müssen übergreifende und anwendungsspezifische Regelungen (z. B. Regelprozesse mit klaren Rollen und Verantwortlichkeiten) festgelegt werden, damit der individuelle Schutzbedarf einer Anlage bzw. eines Systems und die hiermit verbundenen Risiken angemessen berücksichtigt werden können.

Die Zuordnung von Berechtigungen zu Benutzern muss über die Verwendung von Rollen erfolgen, sofern dies systemseitig möglich ist. Bei der Konzeption von Rollen müssen Funktionstrennungsaspekte eingehalten werden. Des Weiteren müssen bei der Konzeption von Rollen und Zuordnung von Benutzerrechten zu den Rollen die Grundsätze „need to know“ und „need to use“ berücksichtigt werden. Die Erstellung, Änderung und Löschung/Deaktivierung von Rollen sowie deren Vergabe und Entzug muss systemseitig, und sicher protokolliert werden.

Besondere Benutzerrechte wie z. B. für Administratoren bzw. Superuser müssen sehr restriktiv vergeben werden. Für die Nutzung dieser Nutzerrechte müssen separate, von den Standardbenutzerkonten getrennte Benutzerkonten vergeben werden. Zugriffe von Administratoren und Superuser müssen im Rahmen der datenschutzrechtlichen Möglichkeiten protokolliert werden. Weiterhin ist ein Review-Prozess für besonders privilegierte Zugriffe (z. B. in Notfallprozeduren) zu etablieren.

Übergreifend ist festzulegen, auf welche Netzwerke und Netzwerk-Dienste zugegriffen werden darf. Es bedarf Regelungen zur sicheren Authentifizierung, Protokollierung und Kommunikation in Netzwerken.

Für einen sicheren Zugang zu Anwendungen und deren Informationen und Daten ist ein sicherer Authentifizierungsmechanismus erforderlich. Für die Vergabe und Verwaltung von Passwörtern müssen Anforderungen u. a. hinsichtlich Qualität und Komplexität gemäß dem jeweils geltenden Stand der Technik definiert werden, aber auch Prozesse zum sicheren Umgang mit Initialpasswörtern sowie einer sicheren Rücksetzung im Bedarfsfalle etabliert werden.

GKV/PV-spezifische Hinweise:

Weitergehende spezifische Anforderungen ergeben sich nicht.

Mindestens umzusetzende Anforderungen nach ISO 27001 Annex A:

5.15	Zugangssteuerung
5.16	Identitätsmanagement
5.17	Authentisierungsinformationen
5.18	Zugangsrechte
8.2	Privilegierte Zugangsrechte
8.3	Informationszugangsbeschränkung
8.5	Sichere Authentisierung
8.18	Gebrauch von Hilfsprogrammen mit privilegierten Rechten

4.14 Anschaffung, Entwicklung und Instandhaltung von (IT-)Anwendungen bzw. (IT-)Systemen

Der Betreiber einer Anlage/ eines Systems der GKV/PV muss für einen angemessenen Schutz der Informationen und Prozesse durch technische, prozessuale und organisatorische Maßnahmen zur Anschaffung, Entwicklung und Instandhaltung von (IT-)Anwendungen bzw. (IT-)Systemen sorgen. Hierzu bedarf es Vorgaben sowie konkreter Maßnahmen zu deren Umsetzung.

Bei der Beschaffung von Informationssystemen sollen alle Sicherheitsanforderungen der Organisation identifiziert und die zu beziehenden Systemkomponenten auf die Einhaltung überprüft und formal freigegeben werden.

IT-Systeme und Komponenten müssen in regelmäßigen Abständen gemäß den Herstellerangaben gewartet und ausgetauscht werden. Beim Austausch von IT-Systemen und Komponenten müssen, die sich hierauf befindlichen Daten datenschutzkonform gelöscht werden.

Es müssen übergeordnete Regelungen zur Software-Entwicklung festgelegt und umgesetzt werden. Die Einhaltung der Sicherheitsanforderungen muss begleitend zum Entwicklungsprozess erfolgen.

Für Software-Entwicklungen müssen dem Produktivsystem ähnliche, jedoch systemisch getrennte Entwicklungs- und Testumgebungen genutzt werden.

Änderungen an Software und Systemkomponenten müssen über einen geordneten Prozess im Rahmen des Patch- und Changemanagements geplant und vorgenommen werden. In Bezug auf notwendige Ad-hoc-Änderungen (z. B. Reaktion auf „Zero-Day-Exploits“) müssen in dem Prozess entsprechende Regelungen festgelegt werden.

Eine Funktionskontrolle inkl. Abnahme soll die spätere operative Nutzung simulieren und somit potenzielle Schwächen und Fehler der geplanten Änderungen im System offenbaren.

GKV/PV-spezifische Hinweise:

Weitergehende spezifische Anforderungen ergeben sich nicht.

Mindestens umzusetzende Anforderungen nach ISO 27001 Annex A:

8.4	Zugriff auf den Quellcode
8.10	Löschung von Informationen
8.11	Datenmaskierung
8.25	Lebenszyklus einer sicheren Entwicklung
8.27	Sichere Systemarchitektur und Entwicklungsgrundsätze
8.28	Sicheres Coding
8.29	Sicherheitsprüfung in Entwicklung und Abnahme
8.31	Trennung von Entwicklungs-, Test- und Produktionsumgebungen
8.32	Änderungssteuerung
8.33	Testdaten

4.15 Compliance

Der Betreiber muss zur Vermeidung von Verstößen gegen gesetzliche, regulatorische oder vertragliche Anforderungen die relevanten rechtlich-regulatorischen Vorgaben, vertragliche Pflichten und weitere Compliance Anforderungen (z. B. unternehmensinterne Regelungen) identifizieren, dokumentieren und regelmäßig aktualisieren.

Die Datenschutzanforderungen müssen gemäß den gesetzlichen Anforderungen wie z. B. dem BDSG (neu) und der EU-DSGVO erfüllt werden. Es muss ferner sichergestellt werden, dass erforderliche Vertraulichkeits- und Geheimhaltungsvereinbarungen identifiziert und mit allen relevanten Parteien spezifische Regelungen (z. B. über Verträge) geschlossen werden.

Es müssen Regelungen getroffen werden, damit sicherheitsrelevante Vorgaben auch in Projekten eingehalten werden.

GKV/PV-spezifische Hinweise:

Spezifische gesetzliche Vorgaben an die GKV/PV ergeben sich aus dem SGB, dem BDSG (neu) bzw. der EU-DSGVO und dem BSIG. Zum Beispiel ist die „Wahrung des Sozialgeheimnisses“ nach § 35 SGB I bei der Verarbeitung der Daten von Versicherten sicherzustellen, um das Grundrecht der Versicherten auf informationelle Selbstbestimmung zu schützen.

Mindestens umzusetzende Anforderungen nach ISO 27001 Annex A:

5.31	Juristische, gesetzliche, regulatorische und vertragliche Anforderungen
5.32	Geistige Eigentumsrechte
5.33	Schutz von Aufzeichnungen
5.34	Datenschutz und Schutz von personenbezogenen Daten (PbD)
6.6	Vertraulichkeits- oder Geheimhaltungsvereinbarungen

4.16 Systeme zur Angriffserkennung

Der Betreiber hat gemäß BSIG ab dem 1. Mai 2023 in angemessener Weise auch Systeme zur Angriffserkennung (SzA) einzusetzen. Die eingesetzten Systeme müssen geeignete Parameter und Merkmale aus dem laufenden Betrieb kontinuierlich und automatisch erfassen und auswerten. Sie sollten dazu in der Lage sein, fortwährend Bedrohungen zu identifizieren und zu vermeiden sowie für eingetretene Störungen geeignete Beseitigungsmaßnahmen vorzusehen. Dabei soll der Stand der Technik eingehalten werden. Organisatorische und technische Vorkehrungen sind angemessen, wenn der dafür erforderliche Aufwand nicht außer Verhältnis zu den Folgen eines Ausfalls oder einer Beeinträchtigung der betroffenen kritischen Anlage steht.

Gemäß BSIG definiert der Gesetzgeber die Systeme zur Angriffserkennung wie folgt:

> *„[…] Systeme zur Angriffserkennung im Sinne dieses Gesetzes sind durch technische Werkzeuge und organisatorische Einbindung unterstützte Prozesse zur Erkennung von Angriffen auf informationstechnische Systeme. Die Angriffserkennung erfolgt dabei durch Abgleich der in einem informationstechnischen System verarbeiteten Daten mit Informationen und technischen Mustern, die auf Angriffe hindeuten […]“*

Bei der Auswahl der umzusetzenden Anforderungen stützt sich dieser B3S auf die Empfehlungen des BSI in der „Orientierungshilfe zum Einsatz von Systemen zur Angriffserkennung“ mit Stand vom 26.09.2022.

Es müssen durch den Betreiber die erforderlichen technischen, organisatorischen und personellen Rahmenbedingungen geschaffen werden, um die Systeme zur Angriffserkennung adäquat in die bestehende IT-Infrastruktur im Anwendungsbereich dieses B3S zu integrieren und zu betreiben. Informationen zu aktuellen Angriffsmustern für technische Verwundbarkeiten/Schwachstellen sind fortlaufend für die im Anwendungsbereich eingesetzten IT-Systeme einzuholen und die zur effektiven Angriffserkennung erforderliche Hard- und Software ist durchgängig auf einem aktuellen Stand zu halten. Signaturen von Detektionssystemen müssen ebenfalls aktuell sein. Sofern keine schwerwiegenden Gründe der Betriebssicherheit dagegensprechen, sind alle relevanten IT-Systeme so zu konfigurieren, dass Versuche, bekannte Schwachstellen auszunutzen, im Einklang mit anderen gesetzlichen Bestimmungen (z. B. DSGVO) auch erkannt werden können.

GKV/PV-spezifische Hinweise:

Keine.

Mindestens umzusetzende Anforderungen:

SzA-P-1a	Protokollierung (Planung)	In der Planungsphase sollte, basierend auf den Ergebnissen der Risikoanalyse und in Anbetracht der kritischen Prozesse des Betreibers, eine schrittweise Vorgehensweise für die Umsetzung der Protokollierung geplant werden. Die Schritte müssen dabei so gewählt werden, dass eine angemessene Sichtbarkeit innerhalb angemessener Zeit erzielt wird. Es muss eine spezifische Sicherheitsrichtlinie vom ISB gemeinsam mit den Fachverantwortlichen erstellt werden. Darin müssen nachvollziehbare Anforderungen und Vorgaben beschrieben sein, wie die Protokollierung zu planen, aufzubauen und sicher zu betreiben ist. Außerdem muss geregelt werden, wie, wo und was zu protokollieren ist. Art und Umfang der in der Sicherheitsrichtlinie beschriebenen Protokollierungen soll sich am Schutzbedarf der Information orientieren.
SzA-P-1b	Protokollierung (Planung)	Der Betreiber muss alle zur wirksamen Angriffserkennung auf System- bzw. Netzebene notwendigen Protokoll- und Protokollierungsdaten erheben, speichern und für die Auswertung bereitstellen, um sicherheitsrelevante Ereignisse erkennen und bewerten zu können. Die zur Speicherung notwendigen Systeme und deren IT-Sicherheitsvorkehrungen müssen schon in der Planung bedacht werden. Da die Protokollierung teilweise auch datenschutzrechtlich relevante Datensätze beinhalten kann, muss der legale Umgang mit diesen bei der Planung einbezogen werden. Eventuelle Persönlichkeitsrechte bzw. Mitbestimmungsrechte der Mitarbeitervertretungen müssen gewahrt werden. Es muss sichergestellt sein, dass alle weiteren relevanten gesetzlichen Bestimmungen beachtet werden. Sollten branchenspezifische weitergehende gesetzliche oder regulatorische Anforderungen an die Protokollierung bestehen, müssen diese ebenfalls umgesetzt werden. Falls betriebs- und sicherheitsrelevante Ereignisse nicht auf einem IT-System protokolliert werden können, müssen zusätzliche IT-Systeme zur Protokollierung (z.B. von Ereignissen auf Netzebene) integriert werden.
SzA-P-1c	Protokollierung (Planung)	Im Rahmen der Planung müssen alle Systeme identifiziert werden, die zur Aufrechterhaltung der kritischen Dienstleistung maßgeblich sind, damit deren Protokoll- und Protokollierungsdaten später erfasst werden können.

SzA-P-1d	Protokollierung (Planung)	Sind die bestehenden Systeme nicht in der Lage, auskömmliche Protokoll- und Protokollierungsdaten bereit zu stellen, sollte die Protokollierungsinfrastruktur so angepasst und/oder durch zusätzliche Maßnahmen, Software oder Systeme ergänzt werden, dass Detektion und Reaktion im entsprechend der Risikoanalyse notwendigen Rahmen möglich sind.
SzA-P-1e	Protokollierung (Planung)	Die Ergebnisse der Planungsphase müssen in einer geeigneten Form dokumentiert werden. Die Dokumentation muss alle Netzbereiche, die Protokoll- und Protokollierungsdatenquellen, deren Beziehungen untereinander und den Datenfluss der Protokoll- und Protokollierungsdaten im Anwendungsbereich umfassen. Hierbei ist ein angemessener Abstraktions- und Detailgrad zu wählen, sodass der effektive Einsatz von SzA bewertet werden kann. Um dies zu unterstützen, sollte insbesondere eine Gruppierung gleicher Systemgruppen innerhalb der Dokumentation erfolgen. Darüber hinaus muss für jedes System bzw. für jede Systemgruppe dokumentiert werden, welche Ereignisse dieses bzw. diese protokolliert.
SzA-P-1f	Protokollierung (Planung)	Es muss ein Prozess eingerichtet werden, der sicherstellt, dass die Protokollierung bei Veränderungen im Anwendungsbereich (Changes) entsprechend angepasst wird. Hierbei ist der Prozess in die allgemeine Änderungssteuerung (vgl. 8.32 aus Kapitel 4.6) zu integrieren.
SzA-P-2a.A1	Protokollierung (Umsetzung)	Es muss eine spezifische Sicherheitsrichtlinie erstellt werden, die insbesondere beschreibt, wie, wo und was zu protokollieren ist. Diese Richtlinie muss den zuständigen Beschäftigten bekannt sein und als Grundlage für ihre Arbeit dienen. Wird die Richtlinie geändert oder wird von den Vorgaben abgewichen, muss das mit dem Informationssicherheitsbeauftragtem (ISB) abgestimmt und dokumentiert werden. Es muss regelmäßig geprüft und dokumentiert werden, ob die Richtlinie noch korrekt umgesetzt wird.
SzA-P-2a.A3	Protokollierung (Umsetzung)	Alle sicherheitsrelevanten Ereignisse müssen protokolliert werden. In den Komponenten vorhandene spezielle Protokollierungsfunktionen müssen nach Herstellervorgaben benutzt werden. In angemessenen Intervallen muss stichpunktartig überprüft werden, ob die Protokollierung noch korrekt funktioniert. Diese Intervalle sind in der Richtlinie (siehe SzA-P-2a.A1) zu dokumentieren.
SzA-P-2a.A4	Protokollierung (Umsetzung)	Die Systemzeit aller protokollierenden Komponenten muss synchron sein und bei Verwendung mit einheitlichen Datums- und Zeitformaten interpretiert werden.
SzA-P-2a.A5	Protokollierung (Umsetzung)	Es muss sichergestellt sein, dass alle relevanten gesetzlichen und vertraglichen Bestimmungen beachtet werden. Protokollierungsdaten müssen nach einem festgelegten Prozess gelöscht werden. Es muss technisch unterbunden werden, dass Protokollierungsdaten unkontrolliert gelöscht oder verändert werden. Gesetzlich vorgeschriebene Lösch- bzw. Speicherfristen müssen eingehalten werden.
SzA-P-2b	Protokollierung (Umsetzung)	Alle gesammelten sicherheitsrelevanten Protokoll- und Protokollierungsdaten müssen an für den jeweiligen Netzbereich zentralen Stellen gespeichert werden. Die Zahl an zentralen Stellen zur Speicherung sollte mög-

		lichst geringgehalten werden und sich mindestens an funktionalen Einheiten orientieren, sodass der Zugriff auf die gespeicherten Daten einfach erfolgen kann. Die Protokollierungsinfrastruktur muss dazu ausreichend dimensioniert sein. Dafür müssen genügend technische, finanzielle und personelle Ressourcen verfügbar sein.
SzA-P-2c	Protokollierung (Umsetzung)	Die gesammelten Protokoll- und Protokollierungsdaten müssen gefiltert, normalisiert, aggregiert und korreliert werden. Die so bearbeiteten Protokoll- und Protokollierungsdaten müssen geeignet verfügbar gemacht werden, damit sie ausgewertet werden können.
SzA-P-2d	Protokollierung (Umsetzung)	Für die Erzielung einer angemessenen Sichtbarkeit von Angriffen sollten die Protokollierungsdatenquellen auf Netzebene von außen (Netzgrenzen) nach innen (Netzbereiche) erschlossen werden.
SzA-P-2e	Protokollierung (Umsetzung)	Die Systemebene (kritische Anwendungen und Applikationen) sollte ausgehend von den zentralen, kritischen Systemen, wie z. B. Anwendungs- und Datenbankserver, Proxies, Gateways, Perimeterschutz, IPS/IDS, Web Application Firewalls (WAF), Anti-Malware-Komponenten, erschlossen werden. Die Priorisierung zur Auswahl der Protokollierungsdatenquellen sollte ausgehend von der Kritikalität der Systeme abgeleitet werden.
SzA-P-2f	Protokollierung (Umsetzung)	Nach erfolgreicher Umsetzung muss geprüft werden, ob alle geplanten Protokollierungsdatenquellen gemäß der Planung umgesetzt wurden.
SzA-D-1	Detektion (Planung)	Bei der Auswahl und dem Einsatz von Detektionsmaßnahmen muss eine umfassende und effiziente Abdeckung der Bedrohungslandschaft erzielt werden. Dazu müssen die Ergebnisse der Risikoanalyse sowie die Größe und Struktur des Unternehmens in der Planung einbezogen werden. Die Definition und Eintrittsschwellen eines Vorfalls (Sicherheitsvorfalls) sollten sich nach dem Schutzbedarf der betroffenen Geschäftsprozesse, IT-Systeme bzw. Anwendungen richten
SzA-D-2a.A1	Detektion (Umsetzung)	Es muss eine spezifische Sicherheitsrichtlinie für die Detektion sicherheitsrelevanter Ereignisse erstellt werden. Die spezifische Sicherheitsrichtlinie muss allen im Bereich Detektion zuständigen Mitarbeitenden bekannt und grundlegend für ihre Arbeit sein. Wird die Richtlinie geändert oder wird von den Vorgaben abgewichen, muss das mit dem ISB abgestimmt und dokumentiert werden. Es muss regelmäßig geprüft und dokumentiert werden, ob die Richtlinie noch korrekt umgesetzt wird.
SzA-D-2a.A2	Detektion (Umsetzung)	Bei der Auswertung von Protokollierungsdaten muss sichergestellt sein, dass alle relevanten gesetzlichen und vertraglichen Bestimmungen beachtet werden. Die gesammelten Meldungen (zu sicherheitsrelevanten Vorfällen) sollten in verbindlich festgelegten Zeiträumen stichpunktartig kontrolliert werden.
SzA-D-2a.A3	Detektion (Umsetzung)	Für sicherheitsrelevante Ereignisse müssen geeignete Melde- und Alarmierungswege festgelegt und dokumentiert werden. Es muss bestimmt werden, welche Stellen wann zu informieren sind. Es muss aufgeführt sein, wie die jeweiligen Personen erreicht werden können. Je nach Dringlichkeit muss ein sicherheitsrelevantes Ereignis über verschiedene Kommunikationswege gemeldet werden.

		Alle Personen, die für die Meldung bzw. Alarmierung relevant sind, müssen über ihre Aufgaben informiert sein. Alle Schritte des Melde- und Alarmierungsprozesses müssen ausführlich beschrieben sein. Die eingerichteten Melde- und Alarmierungswege sollten regelmäßig geprüft, erprobt und ggf. aktualisiert werden.
SzA-D-2a.A4	Detektion (Umsetzung)	Jeder Benutzer muss dahingehend sensibilisiert werden, dass er Ereignismeldungen seines Endgerätes nicht einfach ignoriert oder schließt; er muss die Meldungen entsprechend der Alarmierungswege an die verantwortliche Stelle (siehe auch Kapitel 4.9) weitergeben. Jeder Beschäftigte muss einen von ihm erkannten Sicherheitsvorfall unverzüglich der verantwortlichen Stelle (siehe Kapitel 4.9) melden.
SzA-D-2a.A5	Detektion (Umsetzung)	Falls eingesetzte Systeme oder Anwendungen über Funktionen verfügen, mit denen sich sicherheitsrelevante Ereignisse detektieren lassen, dann müssen diese aktiviert und benutzt werden. Falls ein sicherheitsrelevanter Vorfall vorliegt, dann müssen die Meldungen der betroffenen Systeme ausgewertet und zusätzlich die protokollierten Ereignisse anderer Systeme überprüft werden. Es muss geprüft werden, ob zusätzliche Schadcodescanner auf zentralen Systemen installiert werden sollten. Falls zusätzliche Schadcodescanner eingesetzt werden, dann müssen diese es über einen zentralen Zugriff ermöglichen, ihre Meldungen und Protokolle auszuwerten. Es muss sichergestellt sein, dass die Schadcodescanner sicherheitsrelevante Ereignisse automatisch an die Zuständigen melden. Die Zuständigen müssen die Meldungen auswerten und untersuchen.
SzA-D-2b	Detektion (Umsetzung)	Alle Protokoll- und Protokollierungsdaten müssen kontinuierlich überwacht und ausgewertet werden. Dies sollte automatisiert werden, wenn bei relevanten Ereignissen eine unmittelbare Alarmierung der Verantwortlichen gewährleistet ist. Die Prüfung des Ereignisses und ggf. die Reaktion muss innerhalb einer der Risikoanalyse entsprechend geringen Zeitspanne erfolgen. Es müssen Mitarbeitende des Betreibers bzw. Mitarbeitende von Dienstleistern benannt werden, die dafür zuständig sind. Müssen die verantwortlichen Mitarbeitenden aktiv nach sicherheitsrelevanten Ereignissen suchen, z. B. wenn sie IT-Systeme kontrollieren oder testen, müssen solche Aufgaben in entsprechenden Verfahrensanleitungen dokumentiert sein. Für die Detektion von sicherheitsrelevanten Ereignissen müssen genügend personelle Ressourcen bereitgestellt werden.
SzA-D-2c	Detektion (Umsetzung)	Es müssen Schadcodedetektionssysteme eingesetzt und zentral verwaltet werden. Anhand des Netzplans muss festgelegt werden, welche Netzsegmente durch zusätzliche Detektionssysteme geschützt werden müssen. Insbesondere müssen die im Netzplan definierten Übergänge zwischen internen und externen Netzen um netzbasierte Intrusion Detection Systeme (NIDS) ergänzt werden.
SzA-D-2d	Detektion (Umsetzung)	Damit die Protokoll- und Protokollierungsdaten korreliert und abgeglichen werden können, sollten sie alle zeitlich synchronisiert werden. Die gesammelten Ereignismeldungen müssen regelmäßig auf Auffälligkeiten kontrolliert werden. Damit sicherheitsrelevante Ereignisse auch nachträglich erkannt werden können, müssen die Signaturen der Detektions-/Preventionssysteme immer auf aktuellem Stand sein.

		Diese Anforderungen können durch den Einsatz eines Security Operation Center (SOC) und die Umsetzung eines Security Information und Event Management (SIEM) sowie von Intrusion Detection Systemen (IDS) und Intrusion Prevention Systemen (IPS) erreicht werden.
SzA-D-2e	Detektion (Umsetzung)	Um neue Erkenntnisse über sicherheitsrelevante Ereignisse für den eigenen Informationsverbund zu gewinnen, müssen externe Quellen herangezogen werden. Da Meldungen über unterschiedliche Kanäle in eine Institution gelangen, muss sichergestellt sein, dass diese Meldungen von den Mitarbeitenden auch als relevant erkannt und an die richtige Stelle weitergeleitet werden. Informationen aus zuverlässigen Quellen müssen grundsätzlich ausgewertet werden. Alle gelieferten Informationen müssen danach bewertet werden, ob sie relevant für den eigenen Informationsverbund sind. Ist dies der Fall, müssen die Informationen entsprechend der Sicherheitsvorfallbehandlung eskaliert werden.
SzA-D-2f	Detektion (Umsetzung)	Sofern eine automatisierte Auswertung der Protokoll- und Protokollierungsdaten nicht möglich ist, müssen Mitarbeitende bzw. Mitarbeitende von Dienstleistern speziell damit beauftragt werden, alle relevanten Protokoll- und Protokollierungsdaten (bei dem Verdacht auf sicherheitsrelevante Ereignisse) auszuwerten. Die Auswertung der Protokoll- und Protokollierungsdaten sollte bei diesen höher priorisiert sein, als ihre übrigen Aufgaben. Dieses Personal sollte spezialisierte weiterführende Schulungen und Qualifikationen erhalten. Ein Personenkreis muss benannt werden, der für das Thema Auswertung von Protokolldaten verantwortlich ist.
SzA-D-2g	Detektion (Umsetzung)	Es müssen zentrale Komponenten eingesetzt werden, um sicherheitsrelevante Ereignisse zu erkennen und auszuwerten. Zentrale automatisierte Analysen mit Softwaremitteln müssen dazu eingesetzt werden, um alle in der Systemumgebung anfallenden Protokoll- und Protokollierungsdaten aufzuzeichnen, in Bezug zueinander zu setzen und sicherheitsrelevante Vorgänge sichtbar zu machen. Alle eingelieferten Protokoll- und Protokollierungsdaten müssen lückenlos in der Protokollverwaltung einsehbar und auswertbar sein. Die Daten müssen kontinuierlich ausgewertet werden. Werden definierte Schwellenwerte überschritten, muss automatisch alarmiert werden. Das zuständige Personal muss sicherstellen, dass bei einem Alarm nach fachlicher Bewertung und innerhalb einer der Risikoanalyse entsprechend geringen Zeitspanne eine qualifizierte und dem Bedarf entsprechende Reaktion eingeleitet wird. Die Systemverantwortlichen müssen regelmäßig die Analyseparameter auditieren und anpassen, falls dies erforderlich ist. Zusätzlich müssen bereits überprüfte Protokoll- und Protokollierungsdaten regelmäßig hinsichtlich sicherheitsrelevanter Ereignisse automatisch untersucht werden.
SzA-D-2h	Detektion (Umsetzung)	Als eine zentrale Grundvoraussetzung für die effektive Detektion müssen zudem Informationen zu aktuellen Angriffsmustern für technische Verwundbarkeiten/Schwachstellen fortlaufend für die im Anwendungsbereich eingesetzten Systeme eingeholt werden. Dazu müssen fortlaufend Meldungen der Hersteller (Hard- und Software), von Behörden, den Medien und weiterer relevanter Stellen geprüft werden und in dokumentierte Prozesse des Schwachstellenmanagements einfließen.
SzA-D-2i	Detektion (Umsetzung)	Bei der Umsetzung von Detektionsmechanismen sollte initial eine Kalibrierung durchgeführt werden, um festzustellen, welche sicherheitsrelevanten Ereignisse im Normalzustand auftreten (Baselining). Dazu sollte bewertet werden, ob dieser Normalzustand in Hinblick auf die Zahl der

		falsch positiven Meldungen hingenommen werden kann oder ob Änderungen vorzunehmen sind. Die Kalibrierung sollte bei Änderungen innerhalb des Anwendungsbereichs oder der Bedrohungslage erneut durchgeführt werden.
SzA-D-2j	Detektion (Umsetzung)	Die sicherheitsrelevanten Ereignisse müssen überprüft und dahingehend bewertet werden, ob sie auf einen Sicherheitsvorfall (qualifiziertes sicherheitsrelevantes Ereignis) hindeuten. Die zur Angriffserkennung eingesetzten Systeme sollten, in eindeutig zuordenbaren Fällen, eine automatisierte Qualifizierung ermöglichen. Nur qualifizierte sicherheitsrelevante Ereignisse sollten den Prozess der Reaktion auslösen. Die Qualifizierung sollte in automatisiert nicht eindeutig zuordenbaren Fällen manuell durch festgelegte Verantwortliche vorgenommen werden. Basierend auf den gewonnenen Erkenntnissen der Qualifizierung müssen die Detektionsmechanismen nachjustiert werden.
SzA-R-1.A1	Reaktion	Ein Sicherheitsvorfall muss klar definiert und so weit wie möglich von Störungen abgegrenzt sein. Alle an der Behandlung von Sicherheitsvorfällen beteiligten Beschäftigten müssen die Definition kennen.
SzA-R-1.A2	Reaktion	Eine Richtlinie zur Behandlung von Sicherheitsvorfällen muss erstellt werden. Darin müssen Zweck und Ziel definiert sowie alle Aspekte der Behandlung von Sicherheitsvorfällen geregelt werden. So müssen Verhaltensregeln für die verschiedenen Arten von Sicherheitsvorfällen beschrieben sein. Zusätzlich muss es für alle Beschäftigten zielgruppenorientierte und praktisch anwendbare Handlungsanweisungen geben. Weiterhin sollten die Schnittstellen zu anderen Managementbereichen berücksichtigt werden, z. B. zum Notfallmanagement (siehe Kapitel **Fehler! Verweisquelle konnte nicht gefunden werden.**). Die Richtlinie muss allen Beschäftigten bekannt sein. Sie muss mit dem IT-Betrieb abgestimmt und durch die oberste Leitung verabschiedet sein. Die Richtlinie muss regelmäßig geprüft und aktualisiert werden.
SzA-R-1.A3	Reaktion	Es muss geregelt werden, wer bei Sicherheitsvorfällen wofür verantwortlich ist. Für alle Beschäftigten müssen diesbezüglich Aufgaben und Kompetenzen festgelegt werden. Insbesondere Beschäftigte, die Sicherheitsvorfälle bearbeiten sollten, müssen über ihre Aufgaben und Kompetenzen unterrichtet werden. Dabei muss auch geregelt sein, wer die mögliche Entscheidung für eine forensische Untersuchung trifft, nach welchen Kriterien diese vorgenommen wird und wann sie erfolgen soll. Die Ansprechpartner für alle Arten von Sicherheitsvorfällen müssen den Beschäftigten bekannt sein. Kontaktinformationen müssen immer aktuell und leicht zugänglich sein.
SzA-R-1.A4	Reaktion	Von einem Sicherheitsvorfall müssen alle betroffenen internen und externen Stellen zeitnah informiert werden. Dabei muss geprüft werden, ob der Datenschutzbeauftragte, der Betriebs- und Personalrat sowie die Rechtsabteilung einbezogen werden müssen. Ebenso müssen die Meldepflichten für Behörden und regulierte Branchen berücksichtigt werden. Außerdem muss gewährleistet sein, dass betroffene Stellen über die erforderlichen Maßnahmen informiert werden.
SzA-R-1.A5	Reaktion	Damit ein Sicherheitsvorfall erfolgreich behoben werden kann, muss der Zuständige zunächst das Problem eingrenzen und die Ursache finden.

		Danach muss er die erforderlichen Maßnahmen auswählen, um das Problem zu beheben. Der Leiter des IT-Betriebs muss seine Freigabe erteilen, bevor die Maßnahmen umgesetzt werden. Anschließend muss die Ursache beseitigt und ein sicherer Zustand hergestellt werden. Eine aktuelle Liste von internen und externen Sicherheitsexperten muss vorhanden sein, die bei Sicherheitsvorfällen für Fragen aus den erforderlichen Themenbereichen hinzugezogen werden können. Es müssen sichere Kommunikationsverfahren mit diesen internen und externen Stellen etabliert werden.
SzA-R-1.A6	Reaktion	Nach einem Sicherheitsvorfall müssen die betroffenen Komponenten vom Netz genommen oder gesperrt werden. Die von einem Angriff betroffenen Komponenten sollten einem Penetrationstest unterzogen werden, bevor sie wieder eingesetzt werden. Zudem müssen alle erforderlichen Daten gesichert werden, die Aufschluss über die Art und Ursache des Problems geben könnten. Auf allen betroffenen Komponenten müssen das Betriebssystem und die Anwendungen auf Veränderungen untersucht werden. Die Originaldaten müssen von schreibgeschützten Datenträgern wieder eingespielt werden. Dabei müssen alle sicherheitsrelevanten Konfigurationen und Patches mit aufgespielt werden. Wenn Daten aus Datensicherungen wieder eingespielt werden, muss sichergestellt sein, dass diese vom Sicherheitsvorfall nicht betroffen waren. Nach einem Angriff müssen alle Zugangsdaten auf den betroffenen Komponenten geändert werden, bevor sie wieder in Betrieb genommen werden. Bei der Wiederherstellung der sicheren Betriebsumgebung müssen die Benutzer in die Anwendungsfunktionstests einbezogen werden. Nachdem alles wiederhergestellt wurde, müssen die Komponenten inklusive der Netzübergänge gezielt überwacht werden.
SzA-R-2.A8	Reaktion	Für den Umgang mit Sicherheitsvorfällen sollten geeignete Organisationsstrukturen festgelegt werden. Es sollte ein Sicherheitsvorfall-Team aufgebaut werden, dessen Mitglieder je nach Art des Vorfalls einberufen werden können. Auch wenn das Sicherheitsvorfall-Team nur für einen konkreten Fall zusammentritt, sollten bereits im Vorfeld geeignete Mitglieder benannt und in ihre Aufgaben eingewiesen sein. Es sollte regelmäßig geprüft werden, ob die Zusammensetzung des Sicherheitsvorfall-Teams noch angemessen ist und ggf. angepasst werden muss.
SzA-R-2.A10	Reaktion	Parallel zur Ursachenanalyse eines Sicherheitsvorfalls sollte entschieden werden, ob es wichtiger ist, den entstandenen Schaden einzudämmen oder den Vorfall aufzuklären. Um die Auswirkung eines Sicherheitsvorfalls abschätzen zu können, sollten ausreichend Informationen vorliegen. Für ausgewählte Szenarien sollten daher bereits im Vorfeld Worst-Case-Betrachtungen durchgeführt werden.
SzA-R-2.A11	Reaktion	Ein einheitliches Verfahren sollte festgelegt werden, um Sicherheitsvorfälle und Störungen einzustufen. Das Einstufungsverfahren für Sicherheitsvorfälle sollte zwischen Sicherheitsmanagement und der Störungs- und Fehlerbehebung (Incident Management) abgestimmt sein.
SzA-R-2.A12	Reaktion	Die Schnittstellen zwischen Störungs- und Fehlerbehebung, Notfallmanagement und Sicherheitsmanagement sollten analysiert werden. Dabei

		sollten auch eventuell gemeinsam benutzbare Ressourcen identifiziert werden. Die bei der Störungs- und Fehlerbehebung beteiligten Beschäftigten sollten für die Behandlung von Sicherheitsvorfällen sowie für das Notfallmanagement sensibilisiert werden. Das Sicherheitsmanagement sollte lesenden Zugriff auf eingesetzte Incident-Management-Werkzeuge haben.
SzA-R-2.A13	Reaktion	Die Behandlung von Sicherheitsvorfällen sollte mit dem Notfallmanagement abgestimmt sein. Falls es in der Institution eine spezielle Rolle für Störungs- und Fehlerbehebung gibt, sollte auch diese mit einbezogen werden.
SzA-R-2.A14	Reaktion	Es sollte eine Eskalationsstrategie formuliert werden. Diese sollte zwischen den Verantwortlichen für Störungs- und Fehlerbehebung und dem Informationssicherheitsmanagement abgestimmt werden.
SzA-R-2.A15	Reaktion	Den Beschäftigten des Service Desk sollten geeignete Hilfsmittel zur Verfügung stehen, damit sie Sicherheitsvorfälle erkennen können. Sie sollten den Schutzbedarf der betroffenen Systeme und Anwendungen kennen und ausreichend geschult sein, um die zur Verfügung gestellten Hilfsmittel selbst anwenden zu können.
SzA-R-2.A16	Reaktion	Die Behebung von Sicherheitsvorfällen sollte nach einem standardisierten Verfahren dokumentiert werden. Es sollten alle durchgeführten Aktionen inklusive der Zeitpunkte sowie die Protokolldaten der betroffenen Komponenten dokumentiert werden. Dabei sollte die Vertraulichkeit bei der Dokumentation und Archivierung der Berichte gewährleistet sein. Die benötigten Informationen sollten in die jeweiligen Dokumentationssysteme eingepflegt werden, bevor der Vorfall als beendet und als abgeschlossen markiert wird. Im Vorfeld sollten mit dem ISB die dafür erforderlichen Anforderungen an die Qualitätssicherung definiert werden.
SzA-R-2.A17	Reaktion	Sicherheitsvorfälle sollten standardisiert nachbereitet werden. Die oberste Leitung sollte jährlich über die Sicherheitsvorfälle unterrichtet werden. Besteht sofortiger Handlungsbedarf, muss die Leitung umgehend informiert werden.
SzA-R-2.A18	Reaktion	Nachdem ein Sicherheitsvorfall analysiert wurde, sollte untersucht werden, ob die Prozesse und Abläufe im Rahmen der Behandlung von Sicherheitsvorfällen geändert oder weiterentwickelt werden müssen. Dabei sollten alle Personen, die an dem Vorfall beteiligt waren, über ihre jeweiligen Erfahrungen berichten. Es sollte geprüft werden, ob es neue Entwicklungen im Bereich Incident Management und in der Forensik gibt und ob diese in die jeweiligen Dokumente und Abläufe eingebracht werden können. Werden Hilfsmittel und Checklisten eingesetzt, z. B. für Service-Desk-Beschäftigte, sollte geprüft werden, ob diese um relevante Fragen und Informationen zu erweitern sind.
SzA-R-3	Reaktion	Bei einem sicherheitsrelevanten Ereignis müssen die eingesetzten Detektionssysteme das Ereignis automatisch melden und in Netzen, wo durch die automatische Reaktion die kritische Dienstleistung nicht gefährdet wird, mit geeigneten Schutzmaßnahmen reagieren. In Netzen, wo die kritische Dienstleistung durch die Umsetzung nicht gefährdet wird, muss es

		möglich sein, automatisch in den Datenstrom einzugreifen, um einen möglichen Sicherheitsvorfall zu unterbinden. Sollte eine automatische Reaktion nicht möglich sein, muss über manuelle Prozesse sichergestellt werden, dass der mögliche Sicherheitsvorfall unterbunden wird. Der Ausschluss von Netzen oder Netzsegmenten von einer automatischen Reaktion, bzw. dem Eingriff in den Datenstrom muss schlüssig begründet sein.
SzA-R-4	Reaktion	Festgestellte Sicherheitsvorfälle müssen behandelt werden.
SzA-R-5	Reaktion	Bei Störungen und Sicherheitsvorfällen muss überprüft werden, ob diese den Kriterien der Meldepflicht nach § 8b Abs. 3 BSIG entsprechen und die unverzügliche Meldung an das BSI notwendig ist.
SzA-R-6	Reaktion	Die eingesetzten SzA sollten automatisiert Maßnahmen zur Vermeidung und Beseitigung von angriffsbedingten Störungen ergreifen können, sofern das zu Grunde liegende sicherheitsrelevante Ereignis eindeutig qualifizierbar ist. Dabei muss gewährleistet sein, dass ausschließlich automatisiert ergriffene Maßnahmen nicht zu einer relevanten Beeinträchtigung der kritischen Dienstleistung des Betreibers führen können.
SzA-R-7	Reaktion	Die eingesetzten SzA sollten auch eine nicht-automatisierte Qualifizierung und Behandlung von Ereignissen unterstützen.

Mindestens umzusetzende Anforderungen nach ISO 27001 Annex A:

5.7	Informationen über die Bedrohungslage
8.16	Überwachung von Aktivitäten

4.17 Anforderungen beim Einsatz von Cloud-Lösungen

Mit dem stetig zunehmenden Einsatz von cloudbasierten IT-Diensten im Kranken- und Pflegekassenumfeld ergeben sich zusätzliche Sicherheitsanforderungen, welche beim Erbringen von kritischen Dienstleistungen in einer Cloud-Umgebung berücksichtigt werden müssen. Dies gilt insbesondere, da der KRITIS-Betreiber bei der Nutzung von Cloud-Diensten einen Teil der Hoheit und Kontrolle abgibt. Je nach Ausprägung des Cloud-Betriebsmodells kann dies die Daten, die Prozesse, die Applikationen, den Betrieb, die Infrastruktur und die Kontrolle über die Informationssicherheit betreffen.

Cloud-Dienste sollten strategisch geplant und (Sicherheits-)Anforderungen, Verantwortlichkeiten und Schnittstellen sorgfältig definiert und vereinbart werden. Dabei muss eine bewusste Entscheidung getroffen werden, ob und welche kDL ganz oder teilweise in einer Cloud-Umgebung betrieben werden sollen. Zu berücksichtigen ist auch, dass durch die Cloud-Nutzung neu entstehende Risiken (wie z. B. technische Probleme beim Cloud-Betreiber) bei der Erbringung der kDL nicht an Dritte abgewälzt werden dürfen. Insbesondere die Verfügbarkeit der kDL darf nicht durch Cloud-Dienstleistungen reduziert werden, die Verantwortung hierfür verbleibt beim KRITIS-Betreiber.

Zusätzlich muss bei der Einführung von Cloud-Diensten das Thema Governance berücksichtigt werden (z. B. Vertragsgestaltung, die Umsetzung von Mandantenfähigkeit, die Sicherstellung von Portabilität unterschiedlicher Services, das Monitoring der Service-Erbringung, das Sicherheitsvorfallmanagement sowie Datenschutzaspekte). Wird die Auslagerung eines Dienstes beendet, ist sicherzustellen, dass die Daten und die Funktionalität wieder in die Hoheit des KRITIS-Betreibers zurückgeholt und beim Cloud-Anbieter

vollständig gelöscht werden. Eine vertragliche Regelung und Vorgehensweise zur Exit-Strategie sollte bereits mit Vertragsabschluss vereinbart werden.

Bei der Einführung und Nutzung von Cloud-Diensten sind die Anforderungen des Bundesamts für Soziale Sicherung (BAS) an Cloud-basierte IT-Lösungen in der Sozialversicherung[9] zu berücksichtigen. Konkrete Verarbeitungsbefugnisse müssen sich direkt aus den jeweiligen Sozialgesetzbüchern (SGB) ergeben.

Für die risikoorientierte Bewertung von Cloud-Diensten ist der „Cloud Computing Compliance Criteria Catalogue“ des BSI (kurz: BSI C5) zu beachten. Der BSI C5 beschreibt Mindestanforderungen an die Informationssicherheit für Cloud-Dienste.

Bei der Verarbeitung von Sozial- und Gesundheitsdaten muss gemäß § 393 Absatz 3 SGB V ein C5-Testat oder mindestens ein gleichwertiges Testat vorliegen. Bzgl. des Typs des C5-Testats und der Gleichwertigkeit sind die Ausführungen in § 393 Absatz 4 SGB V zu beachten.

Mindestens umzusetzende Anforderungen nach ISO 27001 Annex A:

5.23	Informationssicherheit für die Nutzung von Cloud-Diensten
8.10	Löschung von Informationen

4.18 Cyber-Security und -Hygiene

Die fortschreitende Digitalisierung eröffnet auch für die Prozesse in der gesetzlichen Kranken- und Pflegeversicherung neue Potenziale und Synergien. Gleichzeitig wächst jedoch auch das Bedrohungspotenzial durch zunehmend zielgerichtete, technologisch ausgereiftere und komplexere Angriffe auf Systemdienste und Dienstanbieter. Cyberangriffen – also Angriffen aus dem Cyber-Raum mit Informations- und Kommunikationstechnik muss daher auch von Kranken- und Pflegekassen sowie deren IT-Dienstleistern mit weiteren Maßnahmen begegnet werden.

Mit dem Gesetz zur Beschleunigung der Digitalisierung des Gesundheitswesens (DigiG) und den damit einhergehenden Anpassungen im SGB V und SGB XI reagiert der Gesetzgeber auf die geänderte Bedrohungslage. Spezifische gesetzliche Vorgaben an die GKV/PV ergeben sich aus § 392 Abs. 4 SGB V sowie § 103a SGB XI mit der Forderung, darauf hinzuwirken, dass

- geeignete Maßnahmen zur Erhöhung der Cybersecurity-Awareness ergriffen werden (vgl. Kapitel 4.7),
- Systeme zur Angriffserkennung, die geeignete Parameter und Merkmale aus dem laufenden Betrieb kontinuierlich und automatisch erfassen und auswerten einzusetzen (siehe Kapitel 4.16).

Hieraus ergeben sich insbesondere folgende Fähigkeiten, die durch die Kranken- und Pflegekassen realisiert werden müssen:

1. Fähigkeit zur Gewährleistung eines angemessenen Problembewusstseins bezüglich der Cybersicherheits-Bedrohungslage, zur Erkennung von Cybersicherheitsangriffen und der Reaktion auf diese.
2. Fähigkeit zur fortlaufenden Erkennung von Bedrohungen in Bezug auf kDL.
3. Fähigkeit zur Vorhersage, Vermeidung und Beseitigung von Sicherheitsereignissen und Störungen in Bezug auf kDL.
4. Fähigkeit, dass Nr. 2 und Nr. 3 innerhalb der gesamten kritischen Dienstleistung – auch bei der Nutzung von IT-Dienstleistern – gewährleistet wird.

[9] Rundschreiben des BAS vom 22.03.2019: „Anforderungen an Cloud-basierte IT-Lösungen in der Sozialversicherung“

Die Realisierung kann mit der Umsetzung der nachfolgend aufgeführten Anforderungen des Annex A der ISO 27001 erfolgen.

GKV/PV-spezifische Hinweise:

Aus dem Dokument „Gemeinsame Grundsätze Technik für die elektronische Datenübermittlung gemäß § 95 SGB IV“ ergeben sich auch Anforderungen an die dort angewendeten Sicherheitsverfahren, die bei der Umsetzung/Implementierung zu berücksichtigen sind.

Mindestens umzusetzende Anforderungen nach ISO 27001 Annex A:

5.7	Informationen über die Bedrohungslage
5.19	Informationssicherheit in Lieferantenbeziehungen
5.20	Behandlung von Informationssicherheit in Lieferantenvereinbarungen
5.21	Umgang mit der Informationssicherheit in der Lieferkette der Informations- und Kommunikationstechnologie
5.22	Überwachung, Überprüfung und Änderungsmanagement von Lieferantendienstleistungen
5.23	Informationssicherheit für die Nutzung von Cloud-Diensten
5.24	Planung und Vorbereitung der Handhabung von Informationssicherheitsvorfällen
5.25	Beurteilung und Entscheidung über Informationssicherheitsereignisse
5.26	Reaktion auf Informationssicherheitsvorfälle
5.27	Erkenntnisse aus Informationssicherheitsvorfällen
5.29	Informationssicherheit bei Störungen
5.30	IKT-Bereitschaft für Business-Continuity
6.3	Informationssicherheitsbewusstsein, -ausbildung und -schulung
6.8	Meldung von Informationssicherheitsereignissen
8.7	Schutz gegen Schadsoftware
8.8	Handhabung von technischen Schwachstellen
8.11	Datenmaskierung
8.12	Verhinderung von Datenlecks
8.16	Überwachung von Aktivitäten
8.23	Webfilterung

4.19 Künstliche Intelligenz

Sofern eine Kranken- oder Pflegekasse im Rahmen ihrer Aufgabenerfüllung Verfahren der künstlichen Intelligenz einsetzt, sind die entsprechenden Anforderungen der KI-Verordnung zu beachten.

Der Einsatz von KI-Systemen muss auf der Basis einer Risikobewertung erfolgen und dem Schutzbedarf der verarbeiteten Informationswerte entsprechen.

Die Definition von Anforderungen für die Einrichtung, Umsetzung, Aufrechterhaltung und fortlaufende Verbesserung der KI-Systeme ist Voraussetzung für deren Integration in bestehende Prozesse. Dafür kann die Erarbeitung von ethischen Grundsätzen, unter Bezugnahme auf die ISO 42001, eine Grundlage bilden.

Die Vorgaben aus der Norm ISO 42001 sind ergänzend zu den hier bereits erwähnten Normen ISO 27001 & 27002 bei der Nutzung und Entwicklung von KI-Systemen zu berücksichtigen.

Mit dem EU-AI-Act und der ISO 42001 wird ein Rahmenwerk bereitgestellt, das Verfahren, Regeln, Definitionen und Risiko-Management-Leitlinien bietet. Damit sollen Risiken der betrieblichen Aspekte von KI-Systemen minimiert sowie rechtliche bzw. regulatorische Anforderungen auf Basis der Verordnung erfüllt werden.

GKV/PV-spezifische Hinweise:

Weitergehende spezifische Anforderungen ergeben sich nicht.

Teil 3

5 Nachweisbarkeit der Umsetzung (Audit, Nachweise und Angemessenheit)

5.1 Eingangsbetrachtung

Durch ein Umsetzen der Anforderungen dieses B3S-GKV/PV implementiert ein Betreiber angemessene und dokumentierte organisatorische und technische Vorkehrungen zur Vermeidung von IT-Ausfällen und IT-Störungen seiner kritischen Dienstleistungen im Rahmen seines Verwaltungs- und Zahlungssystems für gesetzlich Kranken- und Pflegeversicherte.

Der B3S-GKV/PV stellt Verfahren und Maßnahmen zur Verfügung, mit deren Umsetzung KRITIS-Betreiber der GKV die Anforderungen des § 8a Absatz 1 BSIG erfüllen können. Der B3S kann damit den Stand der Technik für die GKV abbilden und Betreibern als Konkretisierung der umzusetzenden Maßnahmen dienen.

Die Wahl einer geeigneten Prüfgrundlage für Prüfungen gemäß § 8a Absatz 3 BSIG obliegt generell den Audit durchführenden Personen. Die Prüfenden müssen dabei selbst sicherstellen, dass die verwendete Prüfgrundlage zur Bewertung geeignet ist und ob ein KRITIS-Betreiber ein hinreichendes IT-Sicherheitsniveau im Sinne des § 8a Absatz 1 BSIG erreicht hat. Der B3S-GKV/PV kann dabei als Ausgangspunkt für die Erstellung einer Prüfgrundlage für Prüfungen gemäß § 8a Absatz 3 BSIG verwendet werden.

5.2 Audit, Nachweise und Angemessenheit

Die Betreiber kritischer Dienstleistungen haben die Erfüllung der Anforderungen mittels der Einreichungsblätter für Betreiber Kritischer Infrastrukturen[10] fristgerecht nach aktuell geltendem BSIG nachzuweisen.

Audits müssen von Auditoren mit nachgewiesener Prüfungskompetenz durchgeführt werden. Ein Auditteam muss dabei die Anforderungen aus der „Orientierungshilfe zu Nachweisen gemäß § 8a (3) BSIG“ erfüllen, so dass alle geforderten Kompetenzbereiche (Audit, IT-Sicherheit und Branchenexpertise gemäß BSI) abgedeckt sind. Vom BSI sind darüber hinaus „Grundsätzliche Anforderungen im Nachweisverfahren (GAiN)“ erstellt, die ebenso zu beachten sind.

[10] https://www.bsi.bund.de/DE/Themen/KRITIS-und-regulierte-Unternehmen/Kritische-Infrastrukturen/KRITIS-Nachweise/kritis-nachweise_node.html

Nachfolgend ist der übergeordnete Auditprozess schematisch dargestellt:

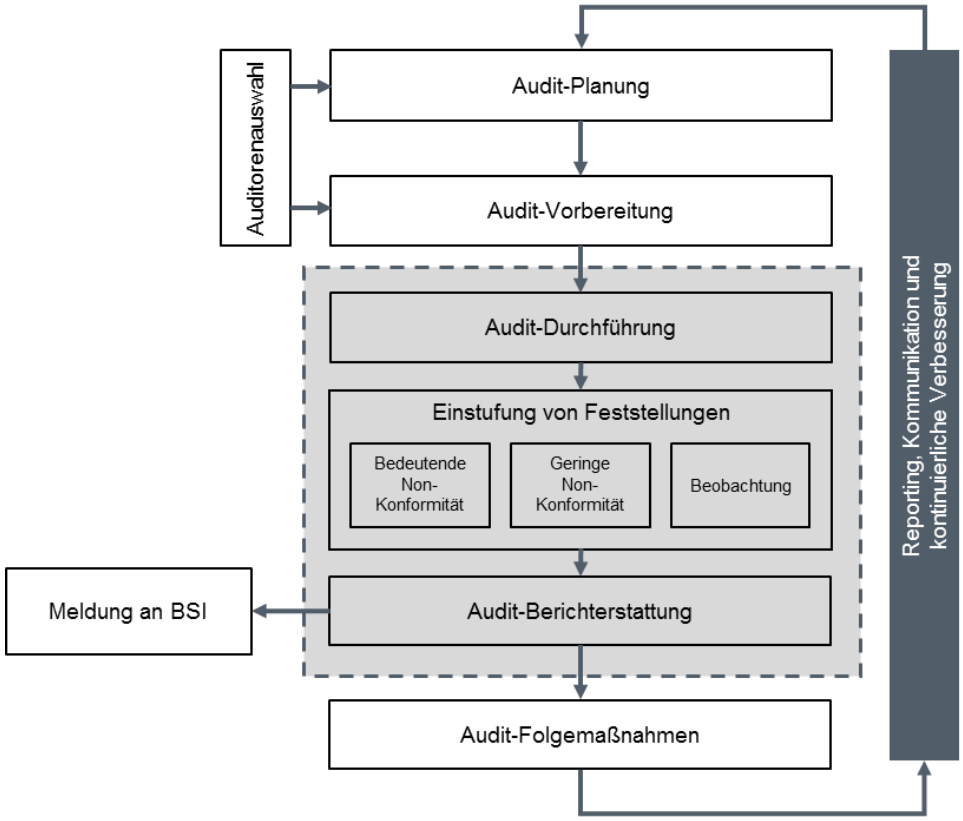

Abbildung 5: Schematischer Gesamtablauf eines Audits

Die Audit-Durchführung und Ergebnisdokumentation erfolgt gemäß den Vorgaben des BSI anhand der zum Auditzeitpunkt aktuellen Fassung der „Orientierungshilfe zu Nachweisen gemäß § 8a (3) BSIG“.

Für die im Auditbericht erhobenen Feststellungen sind abhängig von deren Einstufung adäquate Folgemaßnahmen zur Korrektur vom Betreiber festzulegen und im Rahmen des kontinuierlichen Verbesserungsprozesses umzusetzen.

6 Anhang

6.1 Normative Anforderungen und Regelwerke

Folgende Normen und Regelwerke sind nach diesem Branchenstandard explizit zu berücksichtigen:

- BSI-Gesetz (BSI-G) - Gesetz über das Bundesamt für Sicherheit in der Informationstechnik vom 01.12.2021
- BSI-Kritisverordnung (BSI-Kritis-V) - Verordnung zur Bestimmung Kritischer Infrastrukturen nach dem BSI-Gesetz vom 22.04.2016
- DIN EN ISO/IEC 27001:2024-01 – Informationssicherheit, Cybersicherheit und Datenschutz – Informationssicherheitsmanagementsysteme – Anforderungen (ISO/IEC 27001:2022); Deutsche Fassung EN ISO/IEC 27001:2023
- DIN EN ISO/IEC 27002:2024-01 – Informationssicherheit, Cybersicherheit und Schutz der Privatsphäre – Informationssicherheitsmaßnahmen (ISO/IEC 27002:2022); Deutsche Fassung EN ISO/IEC 27002:2022
- DIN ISO/IEC 27005:2011-06 – Informationstechnik – IT-Sicherheitsverfahren – Informationssicherheits-Risikomanagement
- DIN ISO/IEC 42001:2023 Information Technology Artificial Intelligence Management System
- DSAnpUG-EU (umgangssprachlich: BDSG neu) Gesetz zur Anpassung des Datenschutzrechts an die Verordnung (EU) 2016/679 und zur Umsetzung der Richtlinie (EU) 2016/680 (Datenschutz-Anpassungs- und -Umsetzungsgesetz EU / DSAnpUG-EU)
- EN ISO 22301:2020-06 – Sicherheit und Resilienz – Business Continuity Management System – Anforderungen
- EU-Datenschutzgrundverordnung (EU-DSGVO)
- ISO 19011:2018-10 – Leitfaden zur Auditierung von Managementsystemen
- ISO/IEC 27007:2022-10 – Informationstechnik – Sicherheitsverfahren – Leitfäden für das Auditieren von Informationssicherheits-Managementsystemen
- KI-Verordnung - VERORDNUNG (EU) 2024/1689 DES EUROPÄISCHEN PARLAMENTS UND DES RATES vom 13. Juni 2024
- Kriterienkatalog C5 (C5:2020) - Cloud Computing Compliance Criteria Catalogue des BSI
- Sozialgesetzbuch (SGB)

6.2 Zuordnung der Gefährdungen und Bedrohungen

Die nachfolgenden Tabellen zeigen die Zuordnung der Gefährdungen und Bedrohungen des Gefährdungskataloges GKV/PV zur Orientierungshilfe des BSI:

Kennung aus dem IT-Grundschutz	KRITIS relevante elementare Gefährdung aus der B3S-Orientierungshilfe	Zuordnung im Gefährdungskatalog GKV/PV
G 0.1	Feuer	E02
G 0.2	Ungünstige klimatische Bedingungen	E01, P05
G 0.3	Wasser	E02
G 0.4	Verschmutzung, Staub, Korrosion	E02, P04, P05, T17
G 0.5	Naturkatastrophen	E01
G 0.6	Katastrophen im Umfeld	E01, E02
G 0.7	Großereignisse im Umfeld	E01, E02, E03
G 0.8	Ausfall oder Störung der Stromversorgung	P03
G 0.9	Ausfall oder Störung von Kommunikationsnetzen	V01, T03, T09, T18
G 0.10	Ausfall oder Störung von Versorgungsnetzen	V01
G 0.11	Ausfall oder Störung von Dienstleistern	O01, O02, O06
G 0.12	Elektromagnetische Störstrahlung	P04
G 0.13	Abfangen kompromittierender Strahlung	nicht relevant im GKV/PV-Umfeld
G 0.14	Ausspähen von Informationen/Spionage	V02, V04
G 0.15	Abhören	T10
G 0.16	Diebstahl von Geräten, Datenträgern und Dokumenten	V01, P04
G 0.17	Verlust von Geräten, Datenträgern und Dokumenten	P04, U04
G 0.18	Fehlplanung oder fehlende Anpassung	V10, O03, O04, O07, O15, T03, T04
G 0.19	Offenlegung schützenswerter Informationen	V07, V08, T10
G 0.20	Informationen oder Produkte aus unzuverlässiger Quelle	V03, V05, V06, V10, O15
G 0.21	Manipulation von Hard- und Software	T11
G 0.22	Manipulation von Informationen	V05
G 0.23	Unbefugtes Eindringen in IT-Systeme	V04, V06, V09, T11, T12, T13, T14, T15
G 0.24	Zerstörung von Geräten oder Datenträgern	V01, P04, U04, T01, T17
G 0.25	Ausfall von Geräten oder Systemen	T17
G 0.26	Fehlfunktion von Geräten oder Systemen	T16, T17
G 0.27	Ressourcenmangel	O04, T03
G 0.28	Software-Schwachstellen oder -fehler	U02, O04, O08, O11, T04
G 0.30	Unberechtigte Nutzung oder Administration von Geräten und Systemen	V02, V05, V06, T05, T08
G 0.31	Fehlerhafte Nutzung oder Administration von Geräten und Systemen	U01, U03

Kennung aus dem IT-Grundschutz	KRITIS relevante elementare Gefährdung aus der B3S-Orientierungshilfe	Zuordnung im Gefährdungskatalog GKV/PV
G 0.32	Missbrauch von Berechtigungen	V02, V06, T05
G 0.33	Personalausfall	O12, O13, O14
G 0.34	Anschlag	E02, V01
G 0.35	Nötigung, Erpressung oder Korruption	V03
G 0.36	Identitätsdiebstahl	V02, V03, T05
G 0.37	Abstreiten von Handlungen	T07
G 0.39	Schadprogramme	V04, V10, T11, T12, T13, T14, T15
G 0.40	Verhinderung von Diensten (Denial of Service)	T03, T09
G 0.41	Sabotage	V01
G 0.42	Social Engineering	V03
G 0.43	Einspielen von Nachrichten	T04, T05, T06
G 0.44	Unbefugtes Eindringen in Räumlichkeiten	P02, V01
G 0.45	Datenverlust	V05, U04, T01
G 0.46	Integritätsverlust schützenswerter Informationen	T02
G 0.47	Schädliche Seiteneffekte IT-gestützter Angriffe	T12, T13, T17

Kennung	Besonders zu berücksichtigendes Bedrohungsszenario aus der B3S-Orientierungshilfe	Zuordnung im Gefährdungskatalog GKV/PV
B 1	Ausnutzung von Zero-Day Schwachstellen	T14
B 2	Schadsoftware in E-Mail-Anhängen	T12
B 3	Advanced Persistent Threat (APT)-Angriffe	T15
B 4	Ransomware	T13
B 5	Daten-Exfiltration	V07, V08

6.3 Gefährdungskatalog GKV/PV

Typ	Beschreibung	Zuordnung IT-Schutzziele				Standardvorgaben nach ISO 27001
		Vert.	Int.	Verf.		
Elementare Gefährdungen / höhere Gewalt						
E01	Auswirkungen von klimatischen Bedingungen oder extremen Umweltereignissen (z. B. Hochwasser, Erdbeben, Vulkanausbruch, Orkan, Kälte/Hitze)			x		5.7, 5.29, 7.5, 7.8, 7.11, 8.13, 8.14
E02	Ausfall von Gebäudeteilen (z. B. durch Feuer, Kontamination oder Wassereinbruch)			x		5.29, 7.5, 7.8, 8.13, 8.14
E03	Streik oder Besetzung von Gebäuden / Gebäudeteilen durch Aktivisten			x		5.29, 7.4, 7.5, 8.13, 8.14
Physische Gefährdungen						
P01	Unzureichende oder fehlende Alarmierungseinrichtungen und / oder Überwachungsmaßnahmen			x		5.1, 5.28, 5.29, 6.8, 7.2, 7.3, 7.4, 7.5, 7.13, 8.14
P02	Unautorisierter Zutritt, unzureichendes oder fehlendes physisches Sicherheitszonenkonzept	x		x		5.15, 7.1, 7.2, 7.3, 7.4, 7.5
P03	Zusammenbruch der elektrischen Versorgung (intern sowie extern)			x		5.29, 7.5, 7.11, 7.12, 8.13, 8.14
P04	Mangelhafte Kennzeichnung / Lagerung / Entsorgung von Betriebsmitteln, IT-Komponenten oder Dokumenten	x		x		5.8, 5.9, 5.10, 5.11, 5.12, 5.13, 5.31, 5.33, 5.34, 7.7, 7.8, 7.9, 7.10, 7.11, 7.12, 7.14, 8.1, 8.12
P05	Beeinträchtigung der IT durch ungünstige Arbeits- oder Umgebungsbedingungen (z. B. kritische Temperatur, Luftfeuchtigkeit, Strahlung, Staub)			x		5.10, 5.29, 7.5, 7.8, 7.12, 8.13, 8.14

Typ	Beschreibung	Zuordnung IT-Schutzziele				Standardvorgaben nach ISO 27001
		Vert.	Int.	Verf.		
Vorsätzliche Handlungen						
V01	Einbruch, Vandalismus, Sabotage, Diebstahl an und von Einrichtungen, Geräten oder Übertragungswegen	x		x		5.15, 5.29, 7.1, 7.3, 7.4, 7.5, 8.13, 8.14
V02	Entwenden von Identitäten oder Authentifizierungsinformationen (z. B. durch Phishing- oder Spoofing-Angriffe)	x	x			5.17, 5.28, 6.3, 6.4, 8.5, 8.7, 8.26
V03	Gezielter Angriff (z. B. Social Engineering oder Spear-Phishing)	x	x			5.4, 5.26, 5.27, 5.28, 6.3, 6.8, 8.7, 8.16, 8.19, 8.23
V04	Gezielte, offensive Cyberattacken durch Hacktivisten oder staatliche Akteure	x	x	x		5.5, 5.6, 5.7, 5.15, 5.18, 5.23, 5.24, 5.25, 5.26, 5.27, 5.28, 5.29, 6.8, 6.8, 8.2, 8.7, 8.8, 8.13, 8.14, 8.15, 8.16, 8.20, 8.21, 8.22, 8.29
V05	Manipulation von Daten (z. B. löschen / modifizieren von Dateien oder Datensätzen)		x	x		5.3, 5.7, 5.15, 5.16, 5.17, 5.18, 5.23, 5.28, 6.4, 8.2, 8.3, 8.5, 8.10, 8.11, 8.15, 8.16, 8.17, 8.18, 8.19
V06	Unautorisierter Zugang zu Anwendungen und Netzwerken und Zugriff auf deren Informationen	x	x			5.7, 5.15, 5.16, 5.17, 5.18, 5.19, 5.20, 5.22,5.23, 6.4, 8.2, 8.3, 8.5, 8.15, 8.16, 8.18, 8.20, 8.21, 8.22, 8.26
V07	Unautorisierte Kenntnisnahme oder Exfiltration von Daten	x				5.4, 5.7, 5.10, 5.12, 5.13, 5.14, 5.15, 5.16, 5.17, 5.18, 5.19, 5.20, 5.22,5.23, 5.31, 5.32, 5.33 5.34, 6.1, 6.2, 6.3, 6.4, 6.6, 7.10, 8.2, 8.3, 8.5, 8.6, 8.7, 8.8, 8.11, 8.12, 8.15, 8.16, 8.18, 8.20, 8.21, 8.22, 8.26

Typ	Beschreibung	Zuordnung IT-Schutzziele				Standardvorgaben nach ISO 27001
		Vert.	Int.	Verf.		
V08	Unautorisierte Öffentlichmachung von Informationen (Vertraulichkeitsverlust z. B. von Geschäftsinformationen, Versichertendaten oder Authentifizierungsinformationen)	x	x			5.4, 5.5, 5.10, 5.12, 5.13, 5.14, 5.23, 5.31, 5.32, 5.34, 6.1, 6.2, 6.3, 6.4, 6.6, 7.10, 8.3, 8.11, 8.12, 8.16, 8.23
V09	Verstärkter Angriff auf Teile der Infrastruktur infolge des vermehrten Einsatzes mobilen Arbeitens	x	x	x		5.4, 5.10, 5.14, 5.23, 5.27, 5.31, 6.3, 6.6, 6.7, 7.14, 8.1, 8.16, 8.19, 8.21
V10	Beschaffung, Installation oder Nutzung von nicht lizensierter oder nicht freigegebener Soft- oder Hardware	x	x	x		5.4, 5.7, 6.3, 6.4, 8.2, 8.16, 8.19, 8.23
Unbeabsichtigte Fehler						
U01	Menschlicher Fehler in Betrieb, Nutzung oder Handhabung (z. B. von Informationen, Geräten, Betriebsmitteln)	x	x	x		5.13, 5.10, 5.23, 5.37, 6.3, 7.10, 8.12, 8.13, 8.23
U02	Fehler in der Softwareentwicklung, Customizing oder Konfiguration von Soft- und Hardware	x	x	x		5.19, 5.20, 5.22, 5.37, 6.3, 8.9, 8.32, 8.13, 8.25, 8.27, 8.29, 8.30, 8.31, 8.32, 8.33
U03	Ungeeigneter Umgang mit Zugangskennungen und/oder Passwörtern (z. B. Verwendung von Trivial- oder Standardpasswörtern, Weitergabe)	x	x	x		5.7, 5.14, 5.15, 5.16, 5.17, 5.18, 5.19, 5.20, 5.22, 5.23, 5.27, 6.3, 6.8, 8.2, 8.3, 8.18
U04	Verlust, vergessen, verlieren von Informationen / Daten / Datenträgern / Ausrüstung	x		x		5.9, 5.11, 5.27, 5.36, 6.3, 6.8, 7.8, 7.9, 7.10, 8.1, 8.12
Organisatorische Schwächen						
O01	Ausfall von Lieferketten, Outsourcing-Partnern oder Dienstleistern			x		5.2, 5.9, 5.19, 5.20, 5.21, 5.22, 5.23, 8.6, 8.14, 8.32

Typ	Beschreibung	Zuordnung IT-Schutzziele				Standardvorgaben nach ISO 27001
		Vert.	Int.	Verf.		
O02	Unzureichende oder fehlende Regelungen und Kontrollfunktionen bei ausgelagerten Dienstleistungen (z. B. durch SLAs, Monitoring)	x	x	x		5.2, 5.19, 5.20, 5.21, 5.22, 5.23, 5.37, 8.14, 8.16
O03	Nicht nachvollziehbare Änderungen an Konfigurationen durch unzureichendes Change Management oder fehlendes bzw. fehlerhaftes Rollback	x	x	x		5.4, 5.37, 6.3, 8.8, 8.9, 8.15, 8.25, 8.32
O04	Negative Auswirkungen bei Änderungen an: ▪ Prozessen und Verfahren ▪ Daten oder Informationen ▪ Software ▪ Infrastruktur ▪ Kommunikationseinrichtungen	x	x	x		5.9, 5.10, 5.37, 6.3, 7.12, 7.13, 8.4, 8.6, 8.8, 8.9, 8.10, 8.11, 8.13, 8.14, 8.25, 8.27, 8.29, 8.30, 8.31, 8.32, 8.33
O05	Unvorhergesehene negative Effekte durch Änderungen von rechtlichen oder regulatorischen Vorgaben	x	x	x		5.5, 5.6, 5.23, 5.31, 8.14, 8.32
O06	Unzureichende Berücksichtigung von Informationssicherheitsvorgaben (z. B. in Vorhaben / Projekten, beim Dienstleister)	x	x	x		5.1, 5.2, 5.8, 5.19, 5.22, 5.23, 6.3
O07	Unzureichende Koordination / Kommunikation von IT-betrieblichen Abläufen (z. B. Nutzung Wartungsfenster, Einspielen von Softwareupdates, Komponententausch)	x	x	x		5.2, 5.22, 5.28, 5.37, 6.8, 8.19, 8.29, 8.31, 8.32
O08	Unzureichendes oder fehlendes Patch Management	x	x	x		8.8, 8.9, 8.19
O09	Unzureichende oder fehlende Asset Verwaltung (z. B. für Hardware, Software, weitere Geräte)	x		x		5.9, 5.10, 5.11, 5.12, 5.13, 5.32
O10	Unzureichende oder fehlende Notfallplanung und Tests			x		5.29, 8.14, 8.29, 8.31

Typ	Beschreibung	Zuordnung IT-Schutzziele				Standardvorgaben nach ISO 27001
		Vert.	Int.	Verf.		
O11	Fehlende oder unzureichende Testung von Software	x	x	x		5.3, 5.4, 5.24, 5.31, 5.34, 5.36, 8.8, 8.27, 8.29, 8.30, 8.32, 8.33, 8.28
O12	Ausfall von (Schlüssel-)Personal			x		5.29
O13	Mangel an Fachkräften für den Betrieb der Infrastruktur	x	x	x		5.4, 6.1, 6.3
O14	Auswirkungen von Pandemien wie z. B. Personaleinsatzeinschränkungen	x	x	x		5.29, 8.14
O15	Mangelnde Wartung / Instandhaltung bzw. fehlender Support / Service des Herstellers			x		5.3, 7.13
O16	Unzureichende Detektionsmaßnahmen (fehlende Transparenz, Echtzeit-Analyse und Reaktionsprozesse)	x	x	x		5.3, 5.10, 5.15, 5.17, 5.18, 5.22, 5.24, 5.25, 5.26, 5.28, 5.33, 5.34, 5.36, 6.8, 8.2, 8.7, 8.8, 8.13, 8.15, 8.16, 8.17, 8.18, 8.19, 8.29, 8.32, 8.34, 8.35
Technische Schwachstellen und Bedrohungen						
T01	Technisch bedingter Verlust von Daten und Informationen (z. B. durch Festplattenfehler, fehlendes oder fehlerhaftes Backup)		x	x		5.4, 5.5, 5.7, 5.9, 5.10, 5.11, 5.12, 5.13, 5.23, 5.29, 5.32, 5.33, 5.34, 5.37, 6.3, 6.7, 7.10, 8.24, 7.1, 7.2, 7.3, 7.5, 7.6, 7.7, 7.8, 7.9, 7.10, 7.12, 7.13, 7.14, 8.1, 8.6, 8.13, 8.14, 8.25, 8.32, 8.33, 8.34
T02	Integritätsverlust von Daten und Informationen (z. B. während Erstellung, Transport, Sicherung)		x			5.7, 5.10, 5.14, 5.15, 5.23, 5.29, 5.31, 5.32, 5.33, 5.34, 5.37, 7.7, 7.10, 7.12, 8.1, 8.13, 8.14, 8.26, 8.31, 8.32, 8.34

Typ	Beschreibung	Zuordnung IT-Schutzziele				Standardvorgaben nach ISO 27001
		Vert.	Int.	Verf.		
T03	Unzureichendes Kapazitäts-management für Anwendun-gen, Netze, Speichermedien			x		5.7, 5.10, 5.23, 5.29, 5.37, 8.6, 8.14, 8.20, 8.32
T04	Negative Effekte durch veral-tete oder inkompatible Soft-ware oder Hardware (inklusive „end of life“, z. B. bezüglich Versionen, Typen, Protokolle)	x	x	x		5.6, 5.7, 5.10, 5.23, 5.27, 5.28, 5.29, 6.8, 8.13, 8.14, 8.19, 8.20, 8.29, 8.30, 8.31, 8.32
T05	Unzureichende oder zu schwache Identifikation / Au-thentifizierung (z. B. Kennwort-komplexität)	x	x			5.7, 5.15, 5.17, 5.23
T06	Ungeeignete oder fehlende Verschlüsselungsmechanis-men (z. B. Hash-Funktionen, Datenbanken, Datenträger)	x	x			5.7, 5.23, 5.31, 8.21, 8.24
T07	Unzureichendes technisches Monitoring, Logging, Analyse und Reporting		x	x		5.7, 5.10, 5.15, 5.18, 5.23, 5.31, 5.34, 8.15, 8.17, 8.34
T08	Unsichere Default-Einstellun-gen, unzureichende Härtungs-maßnahmen bei Hardware / Software oder fest konfigu-rierte Zugangsinformationen (z. B. Hersteller-Accounts)	x	x	x		5.7, 5.23, 5.27, 8.2, 8.4, 8.5, 8.15, 8.18, 8.19, 8.21, 8.26, 8.29, 8.31, 8.32
T09	(Distributed) Denial of Service			x		5.7, 5.15, 5.23, 5.24, 5.25, 5.26, 5.27, 5.28, 5.29, 6.8, 8.14, 8.15, 8.20, 8.21
T10	Abhören und unbefugte Auf-zeichnung von Kommunikation	x				5.7, 5.14, 5.15, 5.23, 5.24, 5.25, 5.26, 5.27, 5.28, 5.29, 6.8, 7.3, 8.1, 8.14, 8.20, 8.21, 8.22, 8.24

Typ	Beschreibung	Zuordnung IT-Schutzziele				Standardvorgaben nach ISO 27001
		Vert.	Int.	Verf.		
T11	Einbruchsversuche in Anwendungen sowie Infrastrukturkomponenten und Geräte (z. B. Hacking, Ausnutzen OWASP-Schwachstellen)	x	x	x		5.7, 5.15, 5.23, 5.24, 5.25, 5.26, 5.27, 5.28, 5.29, 6.8, 7.3, 8.7, 8.8, 8.13, 8.14, 8.15, 8.20, 8.21, 8.22
T12	Schadsoftware in Anhängen bzw. über Links in E-Mails	x	x	x		5.7, 5.14, 5.15, 5.23, 5.24, 5.25, 5.26, 5.27, 5.28, 6.3, 6.8, 8.3, 8.7, 8.8, 8.13, 8.15, 8.19, 8.20, 8.21, 8.22, 8.23, 8.26
T13	Eingeschleuste Ransomware oder vergleichbare Schadsoftware	x	x	x		5.7, 5.15, 5.23, 5.24, 5.25, 5.26, 5.27, 5.28, 5.29, 6.8, 8.7, 8.8, 8.13, 8.14, 8.15, 8.19, 8.20, 8.21, 8.22, 8.23
T14	Ausnutzen von Zero-Day-Exploits in IT-Systemen	x	x	x		5.5, 5.6, 5.7, 5.15, 5.23, 5.24, 5.25, 5.26, 5.27, 5.28, 5.29, 6.8, 8.3, 8.8, 8.13, 8.14, 8.15, 8.20, 8.21, 8.22
T15	Advanced Persistent Threats (APT)	x	x	x		5.5, 5.6, 5.7, 5.15, 5.18, 5.23, 5.24, 5.25, 5.26, 5.27, 5.28, 5.29, 6.8, 7.3, 7.5, 8.2, 8.8, 8.13, 8.14, 8.15, 8.20, 8.21, 8.22
T16	Fehlfunktion oder Ausfall zentraler IT-Services (z. B. DNS, LDAP, Active Directory, Zeitsynchronisation)	x	x	x		5.7, 5.10, 5.15, 5.23, 5.24, 5.25, 5.26, 5.27, 5.28, 5.29, 6.8, 8.4, 8.14, 8.15, 8.17, 8.20, 8.21, 8.22, 8.29, 8.32
T17	Technischer Zusammenbruch oder Ausfall von Hard- oder Software (z. B. durch Beschädigung oder als Folge der Ausnutzung von Schwachstellen)			x		5.7, 5.23, 5.29, 5.37, 7.1, 7.2, 7.3, 7.5, 7.6, 7.8, 7.11, 7.12, 7.13, 8.6, 8.14, 8.20, 8.21, 8.31, 8.32

Typ	Beschreibung	Zuordnung IT-Schutzziele				Standardvorgaben nach ISO 27001
		Vert.	Int.	Verf.		
T18	Technischer Zusammenbruch oder Ausfall von Kommunikationsdiensten und Verbindungen (z. B. durch Beschädigung oder als Folge der Ausnutzung von Schwachstellen)			x		5.7, 5.10, 5.23, 5.24, 5.25, 5.26, 5.27, 5.28, 5.29, 6.8, 7.5, 7.11, 7.12, 7.13, 8.14, 8.20, 8.21

6.4 Maßnahmen im Kontext der GKV/PV spezifischen Gefährdungslage

Tabelle ISO 27001 - Annex A mit ausgewählten Maßnahmen und der Gründe für deren Auswahl.

Legende:
rRA: rechtlich regulatorische Anforderungen
GA: Geschäftsanforderungen
BP: angewandte Best Practices

ISO 27001 - Annex A		Zuordnung zu Schutzzielen				Branchenspezifische Notwendigkeit			Anwendbar GKV/PV
		Verf.	Integ.	Vert.	.	rRA	GA	BP	
5.1	Informationssicherheitspolitik und -richtlinien	x	x	x		x	x	x	Ja
5.2	Informationssicherheitsrollen und -verantwortlichkeiten	x	x	x		x		x	Ja
5.3	Aufgabentrennung		x	x		x		x	Ja
5.4	Verantwortlichkeiten der Leitung	x	x	x		x	x		Ja
5.5	Kontakt mit Behörden					x			Ja
5.6	Kontakt mit speziellen Interessengruppen					x			Ja
5.7	Informationen über die Bedrohungslage	x	x	x		x		x	Ja
5.8	Informationssicherheit im Projektmanagement	x	x	x			x	x	Ja
5.9	Inventar der Informationen und anderen damit verbundenen Werte	x	x	x			x	x	Ja
5.10	Zulässiger Gebrauch von Informationen und anderen damit verbundenen Werten	x	x	x			x	x	Ja
5.11	Rückgabe von Werten	x		x			x	x	Ja
5.12	Klassifizierung von Informationen	x	x	x				x	Ja
5.13	Kennzeichnung von Informationen	x	x	x				x	Ja
5.14	Informationsübermittlung	x	x	x		x	x	x	Ja
5.15	Zugangssteuerung	x	x	x		x	x	x	Ja
5.16	Identitätsmanagement		x	x		x	x	x	Ja
5.17	Authentisierungsinformationen		x	x		x	x	x	Ja
5.18	Zugangsrechte		x	x		x	x	x	Ja
5.19	Informationssicherheit in Lieferantenbeziehungen	x	x	x		x	x	x	Ja

ISO 27001 - Annex A		Zuordnung zu Schutzzielen				Branchenspezifische Notwendigkeit			Anwendbar GKV/PV
		Verf.	Integ.	Vert.	.	rRA	GA	BP	
5.20	Behandlung von Informationssicherheit in Lieferantenvereinbarungen	x	x	x		x	x	x	Ja
5.21	Umgang mit der Informationssicherheit in der Lieferkette der Informations- und Kommunikationstechnologie (IKT)	x	x	x		x	x	x	Ja
5.22	Überwachung, Überprüfung und Änderungsmanagement von Lieferantendienstleistungen	x	x	x		x	x	x	Ja
5.23	Informationssicherheit für die Nutzung von Cloud-Diensten	x	x	x		x	x	x	Ja
5.24	Planung und Vorbereitung der Handhabung von Informationssicherheitsvorfällen	x	x	x		x	x	x	Ja
5.25	Beurteilung und Entscheidung über Informationssicherheitsereignisse	x	x	x		x	x	x	Ja
5.26	Reaktion auf Informationssicherheitsvorfälle	x	x	x		x	x	x	Ja
5.27	Erkenntnisse aus Informationssicherheitsvorfällen	x	x	x		x	x	x	Ja
5.28	Sammeln von Beweismaterial	x	x	x		x	x		Ja
5.29	Informationssicherheit bei Störungen	x	x	x		x		x	Ja
5.30	IKT-Bereitschaft für Business-Continuity	x				x	x	x	Ja
5.31	Juristische, gesetzliche, regulatorische und vertragliche Anforderungen	x	x	x		x	x	x	Ja
5.32	Geistige Eigentumsrechte	x				x	x	x	Ja
5.33	Schutz von Aufzeichnungen	x	x	x		x	x	x	Ja
5.34	Datenschutz und Schutz von personenbezogenen Daten (PbD)	x	x	x		x	x	x	Ja
5.35	Unabhängige Überprüfung der Informationssicherheit	x	x	x		x		x	Ja
5.36	Einhaltung von Richtlinien, Vorschriften und Normen für die Informationssicherheit	x	x	x		x	x	x	Ja
5.37	Dokumentierte Betriebsabläufe	x	x	x		x	x	x	Ja
6.1	Sicherheitsüberprüfung		x	x			x	x	Ja
6.2	Beschäftigungs- und Vertragsbedingungen	x	x	x		x	x		Ja
6.3	Informationssicherheitsbewusstsein, -ausbildung und -schulung	x	x	x			x	x	Ja

ISO 27001 - Annex A		Zuordnung zu Schutzzielen				Branchenspezifische Notwendigkeit			Anwend-bar GKV/PV
		Verf.	Integ.	Vert.	.	rRA	GA	BP	
6.4	Maßregelungsprozess	x	x	x		x	x		Ja
6.5	Verantwortlichkeiten bei Beendigung oder Änderung der Beschäftigung	x	x	x		x	x	x	Ja
6.6	Vertraulichkeits- oder Geheimhaltungsvereinbarungen			x		x	x	x	Ja
6.7	Remote-Arbeit	x	x	x		x	x	x	Betreiber-spezifisch
6.8	Meldung von Informationssicherheitsereignissen	x	x	x		x	x	x	Ja
7.1	Physische Sicherheitsperimeter	x	x	x		x	x	x	Ja
7.2	Physischer Zutritt	x	x	x		x	x	x	Ja
7.3	Sichern von Büros, Räumen und Einrichtungen	x	x	x		x	x	x	Ja
7.4	Physische Sicherheitsüberwachung	x	x	x		x		x	Ja
7.5	Schutz vor physischen und umweltbedingten Bedrohungen	x					x	x	Ja
7.6	Arbeiten in Sicherheitsbereichen	x	x	x		x	x	x	Ja
7.7	Aufgeräumte Arbeitsumgebung und Bildschirmsperren		x	x			x	x	Ja
7.8	Platzierung und Schutz von Geräten und Betriebsmitteln	x					x	x	Ja
7.9	Sicherheit von Werten außerhalb der Räumlichkeiten	x	x	x			x	x	Ja
7.10	Speichermedien	x	x	x		x	x		Ja
7.11	Versorgungseinrichtungen	x					x	x	Ja
7.12	Sicherheit der Verkabelung	x	x	x				x	Ja
7.13	Instandhaltung von Geräten und Betriebsmitteln	x	x					x	Ja
7.14	Sichere Entsorgung oder Wiederverwendung von Geräten und Betriebsmitteln			x		x	x	x	Ja
8.1	Endpunktgeräte des Benutzers	x	x	x			x	x	Ja
8.2	Privilegierte Zugangsrechte	x	x	x		x	x	x	Ja
8.3	Informationszugangsbeschränkung		x	x		x	x	x	Ja
8.4	Zugriff auf den Quellcode		x	x		x		x	Ja

ISO 27001 - Annex A		Zuordnung zu Schutzzielen				Branchenspezifische Notwendigkeit			Anwend-bar GKV/PV
		Verf.	Integ.	Vert.	.	rRA	GA	BP	
8.5	Sichere Authentisierung		x	x			x	x	Ja
8.6	Kapazitätssteuerung	x					x	x	Ja
8.7	Schutz gegen Schadsoftware	x	x	x				x	Ja
8.8	Handhabung von technischen Schwach-stellen	x	x	x		x		x	Ja
8.9	Konfigurationsmanagement	x	x	x			x	x	Ja
8.10	Löschung von Informationen		x	x		x	x	x	Ja
8.11	Datenmaskierung			x		x	x	x	Ja
8.12	Verhinderung von Datenlecks			x			x	x	Ja
8.13	Sicherung von Informationen	x	x			x	x	x	Ja
8.14	Redundanz von informationsverarbeiten-den Einrichtungen	x				x		x	Ja
8.15	Protokollierung	x	x	x		x	x	x	Ja
8.16	Überwachung von Aktivitäten	x	x	x		x		x	Ja
8.17	Uhrensynchronisation		x				x	x	Ja
8.18	Gebrauch von Hilfsprogrammen mit privi-legierten Rechten	x	x	x			x	x	Ja
8.19	Installation von Software auf Systemen im Betrieb	x	x	x		x	x	x	Ja
8.20	Netzwerksicherheit	x		x				x	Ja
8.21	Sicherheit von Netzwerkdiensten	x	x	x				x	Ja
8.22	Trennung von Netzwerken	x	x	x				x	Ja
8.23	Webfilterung		x	x				x	Ja
8.24	Verwendung von Kryptographie	x	x	x			x	x	Ja
8.25	Lebenszyklus einer sicheren Entwicklung	x	x	x		x		x	Ja
8.26	Anforderungen an die Anwendungssicher-heit		x	x				x	Ja
8.27	Sichere Systemarchitektur und Entwick-lungsgrundsätze	x	x	x			x	x	Ja
8.28	Sichere Codierung	x	x	x	x		x	x	Ja
8.29	Sicherheitsprüfung bei Entwicklung und Abnahme	x	x	x		x	x	x	Ja

ISO 27001 - Annex A		Zuordnung zu Schutzzielen				Branchenspezifische Notwendigkeit			Anwend-bar GKV/PV
		Verf.	Integ.	Vert.	.	rRA	GA	BP	
8.30	Ausgegliederte Entwicklung	x	x	x			x		Ja
8.31	Trennung von Entwicklungs-, Test- und Produktionsumgebungen		x	x		x	x	x	Ja
8.32	Änderungssteuerung	x	x	x		x	x	x	Ja
8.33	Testdaten		x	x		x	x	x	Ja
8.34	Schutz der Informationssysteme während Tests im Rahmen von Audits	x	x	x		x	x	x	Ja

6.5 Dokumentenhistorie

Version	Status	Datum	Erläuterung der Änderung	Verfasser / Verfasserin
0.1-0.4	Erstellung	11.10.2017 – 02.09.2018	Initiale Erstellung	Arbeitsgruppe B3S GKV/PV (vdek, BARMER, TK, DAKG)
0.4-0.9	Überarbeitung	03.09.2018 – 11.10.2018	Einarbeitung der Hinweise des BSI vom 31.08.2018 und inhaltliche Überarbeitung sowie QS	Arbeitsgruppe B3S GKV/PV (vdek, BARMER, TK, DAKG)
1.0	Eignungsprüfung	12.10.2018	Einreichung beim BSI zur Erst-Eignungsprüfung	Arbeitsgruppe B3S GKV/PV (vdek, BARMER, TK, DAKG)
1.1	Finalisierung	21.12.2018	Finalisierung nach Einarbeitung der Rückmeldungen von BSI, BVA und BBK	Arbeitsgruppe B3S GKV/PV (vdek, BARMER, TK, DAKG)
1.2	Überarbeitung und Eignungsprüfung	27.08.2020 – 04.11.2020	Diverse redaktionelle Korrekturen; Umstellung in Kapitel 1; Anpassung der kDL-Prozesse (Aufnahme Verletztengeld, Anpassung zu Ersatz- und Berechtigungsscheinen); Zulassen einer vergleichbaren Methodik in Kapitel 3; Einreichung beim BSI zur erneuten Eignungsprüfung	Arbeitsgruppe B3S GKV/PV (vdek, BARMER, TK, DAKG)
1.3	Überarbeitung und Eignungsprüfung	16.08.2022 – 25.11.2022	Redaktionelle Korrekturen wegen Übernahme des B3S im BAK GKV; Ergänzung und Umformulierung (Kapitel 4.8); Hinzufügen eines Abschnitts über Systeme zur Angriffserkennung (Kapitel 4.17); Hinzufügen eines Abschnitts zu Cloud Computing (Kapitel 4.18); Anpassung des Gefährdungskatalogs (Kapitel 6.3 sowie Kapitel 6.2); Integration der Änderungen aus OH B3S V1.1 (Kapitel 6.5)	BAK Gesetzliche Krankenversicherungen im UP KRITIS (BARMER, DAK-Gesundheit, IKK classic, TK, vdek)

1.4	Überarbeitung und Eignungs-prüfung	31.03.2023 – 20.01.2025	Redaktionelle Anpassungen aufgrund der Anmerkungen des BSI; Übergang zur ISO 27001:2024-01; Zusammenlegung der Kapitel Continuity- und Notfallma-nagement; Kap. 3.2 Beschränkung der Behandlungsalternativen für Risiken – Angemessenheit von Maßnahmen. Ergänzungen Kap. 4.12 und 4.17 aufgrund Digital-G so-wie Kap. 4.16 SzA (fehlende MUSS-Kriterien). Neues Kapitel 4.18 Cyber-Security und -Hygiene, Neues Kapitel 4.19 Künstli-che Intelligenz Anhang 6.5 Mapping der B3S-Orientierungshilfe auf ISO 27001 entfernt	BAK Gesetzliche Kranken-versicherungen im UP KRITIS

6.6 Abkürzungsverzeichnis

Abkürzung	Bedeutung
B3S	Branchenspezifische Sicherheitsstandards
BAS	Bundesamt für Soziale Sicherung (ehemals Bundesversicherungsamt [BVA])
BBK	Bundesamt für Bevölkerungsschutz und Katastrophenhilfe
BCM	Business Continuity Management
BCMS	Business Continuity Management System
BCP	Business Continuity Plan
BIA	Business Impact Analysis
BDSG	Neufassung des Bundesdatenschutzgesetzes ab 2018 (siehe auch Datenschutz-Anpassungs- und -Umsetzungsgesetz EU (DSAnpUG-EU))
BMI	Bundesministerium des Inneren, für Bau und Heimat
BSI	Bundesamt für Sicherheit in der Informationstechnik
BSIG	Gesetz über das Bundesamt für Sicherheit in der Informationstechnik (BSI-Gesetz)
EESSI	Elektronischer Austausch von Informationen betreffend der Sozialen Sicherheit
EU-DSGVO	Verordnung (EU) 2016/679 (Datenschutz-Grundverordnung)
GoB	Grundsätze ordnungsgemäßer Buchführung
ICS	Industrial Control System (ICS) Security befasst sich mit der IT-Sicherheit in den Bereichen Fabrikautomation und Prozesssteuerung. D.h. Cyber-Sicherheit in Industrieanlagen und -steuerungen
IDS	Intrusion Detection System
IPS	Intrusion Prevention System
ISMS	Informationssicherheits-Managementsystem (engl. Information Security Management System)
ISO/IEC	IEC International Organization for Standardization / International Electrotechnical Commission
IT-SCM	IT Service Continuity Management
kDL	kritische Dienstleistung
KI	Künstliche Intelligenz
NIST	National Institute of Standards and Technology

Abkürzung	Bedeutung
OWASP	Open Web Application Security Project
QS	Qualitätssicherung
UP	Unabhängige Partnerschaft KRITIS, Initiative zur Zusammenarbeit von Wirtschaft und Staat zum Schutz Kritischer Infrastrukturen in Deutschland

6.7 Glossar

Begriff	Definition
(Sicherheits-)Anforderung	Eine Anforderung ist eine Aussage über die notwendige Beschaffenheit oder Fähigkeit, welche • eine (IT-)Anwendung bzw. ein (IT-) System oder • Bestandteile davon oder • ein Prozess erfüllen muss, um einer Norm oder einer Spezifikation zu entsprechen.
(IT-)Anwendung bzw. (IT-)System	Weit gefasster Oberbegriff für Aufgabenbearbeitungen mithilfe eines Softwaresystems; der Begriff wird im Sinn von „Anwendung der EDV" für spezielle betriebliche Aufgaben, besonders für Aufgaben der Fachabteilungen verwendet.
Anlage	Im Sinne der KRITIS-relevanten Kernprozesse unterstützen Anlagen maßgeblich die kritische Dienstleistung. Einer Anlage sind folgende Bestandteile zuzurechnen: • Betriebsstätten mit Gebäuden, die zur Erbringung der kritischen Dienstleistung erforderlich sind, • Prozesse und Verfahren zum Betrieb des integrierten Anwendungssystems inklusive notwendiger Informationen, Daten, Maschinen und Geräte sowie • Nebeneinrichtungen (u. a. vor- und nachgelagerte Systeme), die zur Erbringung der kritischen Dienstleistung erforderlich sind. Es sind sowohl technische als auch prozessuale und organisatorischen Aspekte zu berücksichtigen.
Audit	Gemäß ISO 22301 definiert als: „Systematischer, unabhängiger und dokumentierter Prozess zur Erlangung von Auditnachweisen und zu deren objektiver Auswertung, um zu ermitteln, inwieweit die Auditkriterien erfüllt sind".
Business Continuity Management	Gemäß ISO 22301 definiert als: „Ganzheitlicher Managementprozess, der potenzielle Bedrohungen für Organisationen und die Auswirkungen ermittelt, die diese Bedrohungen, falls sie umgesetzt werden, womöglich auf die Geschäftsabläufe haben und der ein Gerüst zum Aufbau der Belastbarkeit einer Organisation im Verbund mit der Fähigkeit einer effektiven Reaktion, die die Interessen ihrer zentralen Interessensgruppen, das Ansehen, die Marke und die wertschöpfenden Tätigkeiten sichert, bereitstellt".
Business Continuity Management System	Gemäß ISO 22301 ist BCMS definiert als: „Teil des Gesamt-Managementsystems zur Einführung und Umsetzung, den Betrieb sowie die Überwachung, Überprüfung, Verwaltung und Verbesserung der Aufrechterhaltung der Betriebsfähigkeit". Das Managementsystem umfasst den organisatorischen Aufbau, Leitlinien, Planungstätigkeiten, Verantwortlichkeiten, Verfahren, Prozesse und Ressourcen.
Betreiber	Der Betreiber ist eine natürliche oder juristische Person, die unter Berücksichtigung der rechtlichen, wirtschaftlichen und tatsächlichen Umstände bestimmenden Einfluss auf die Beschaffenheit und den Betrieb einer Anlage oder Teilen davon ausübt.

Begriff	Definition
Cyber-Hygiene	Verschiedene grundlegende Verfahren und Herangehensweisen, welche allgemein zu einer Verbesserung des Cybersicherheitsniveaus einer Einrichtung führen können. Dies beinhaltet beispielsweise ein Patchmanagement, Regelungen für sichere Passwörter, die Einschränkung von Zugriffskonten auf Administratorenebene, Netzwerksegmentierungen, sowie Backup- und Sicherungskonzepte für Daten. Ebenfalls gehören hierzu allgemeine Informations- und Schulungsmaßnahmen, um das allgemeine Bewusstsein der Mitarbeiter für die Risiken im Zusammenhang mit IKT-Produkten zu schärfen.
EESSI	Elektronischer Austausch von Informationen betreffend der Sozialen Sicherheit: Verzeichnis der Institutionen. Das Verzeichnis enthält nationale Institutionen (öffentliche und private) in den Sektoren Gesundheitsvorsorge, Renten, Arbeitslosigkeit und Familienleistungen.
Geschäftsprozess	Ein Geschäftsprozess ist eine Menge logisch verknüpfter Tätigkeiten, die ausgeführt werden, um ein bestimmtes geschäftliches oder betriebliches Ziel zu erreichen.
integriertes Anwendungssystem	Ein integriertes Anwendungssystem umfasst zugehörige Infrastrukturen, Netzwerk- und Kommunikationseinrichtungen sowie Hardware, System- und Anwendungssoftware und ist im Bereich der gesetzlichen Kranken- und Pflegeversicherung wie folgt charakterisiert: • Das System übernimmt Aufgaben aus mehreren Funktionsbereichen, • die einzelnen Verarbeitungsbereiche werden zu einem Gesamtsystem verknüpft, • Daten werden im Normalfall in der Verarbeitungskette elektronisch erfasst und dann systemintern verarbeitet.
IT-Service	Ein IT-Service besteht aus einer Kombination von Personen, Infrastrukturen, Dienstleistern, IT-Technologien, Prozessen und deren Daten und Informationen. Ein IT-Service basiert auf dem Einsatz der Informationstechnologie zur Unterstützung der Geschäftsprozesse.
kritische Dienstleistung (kDL)	Eine Dienstleistung zur Versorgung der Allgemeinheit nach der BSI-KritisV, deren Ausfall oder Beeinträchtigung zu erheblichen Versorgungsengpässen oder zu Gefährdungen der öffentlichen Sicherheit führen würde.
(Sicherheits-)Maßnahme	Eine (Sicherheits-)Maßnahme dient dazu, eine (Sicherheits-)Anforderung operativ umzusetzen.
Nebeneinrichtungen	Solche Einrichtungen, die der allg. Nutzung von Anlagen im Sinne des BSIG dienen, u. a. Austauschschnittstellen (Zugang zum Internet), Vor- und Zuliefersysteme, Automatisierungswerkzeuge (z. B. Dunkelverarbeitung).