4.2018 I TÜV Media I www.mt-medizintechnik.de I G 8770F I ISSN 0344-9416

mt|medizintechnik

Schwerpunktthema:

Innovationen

Internationale best practice im Risikomanagement von Spitälern

Digitaler Wandel – Blockchain im Gesundheitswesen

Mit Risikomanagement zu einem sicheren Krankenhaus

Organ für: fbmt – Fachverband für biomedizinische Technik e.V. · Bundesverband der Sachverständigen für Medizinprodukte e.V.
VDI-Gesellschaft Technologies of Life Sciences

Impressum

mt | medizintechnik

erscheint 6-mal jährlich
138. Jahrgang / Ausgabe 4.2018

Schwerpunktthema
Innovationen

Redaktion
Iris Bings | bings@mt-medizintechnik.de
Unter Mitarbeit von
Markus Kemm | kemm.markus@ crconsultants.de
Daniela Penn | daniela.penn@medisis.de
Frank J. Schmitz | schmitz@mt-medizintechnik.de

Redaktion www.mt-medizintechnik.de
Mirjam Bauer | bauer@mt-medizintechnik.de

Redaktionsbeirat
C. Backhaus | claus.backhaus@fh-muenster.de
C. Bulitta | c.bulitta@oth-aw.de
H.-D. Dejon | HansDieter.Dejon@t-online.de
Martin Fiebich | fiebich@mt-medizintechnik.de
G. Haufe | buero@ibhaufe.de
D. Hochmann | david.hochmann@fh-muenster.de
J. Held | juergen.held@hfg-gmuend.de
A. Keller | andreas.keller@tu-ilmenau.de
M. Kindler | manfred.kindler@fbmt.de
R. Mildner | mildner@tzl.de
M. Regner | maic.regner@uniklinikum-dresden.de
R. Stender | randolph.stender@prosystem-ag.com

Verlag
TÜV Media GmbH
Am Grauen Stein, 51105 Köln
Postfach 903060, 51123 Köln
Tel.: 0221/806-3535, Fax: 0221/806-3510
tuev-media@de.tuv.com
www.tuev-media.de
Geschäftsführerin: Gabriele Landes

Koordination
Cindy Bouchagiar | cindy.bouchagiar@de.tuv.com
Tel.: 0221/806-3507

Anzeigenverwaltung
Gudrun Karafiol-Schober | gudrun.karafiol@de.tuv.com
Tel.: 0221/806-3536

Satz: DSV, Bernd Meier, Stockhausen

Druck: TÜV Media GmbH, Köln

Bezugs- und Lieferbedingungen
Jahresabonnement Inland: 69,90 EUR zzgl. Versandkosten.
Einzelheft: 15,– EUR zzgl. Versandkosten.
Studentenabonnement: 30,– EUR zzgl. Versandkosten.
Preisänderungen vorbehalten.
Kündigung: bis 6 Wochen zum Ende eines Kalenderjahres schriftlich an den Verlag. Inlandspreise inkl. MwSt. Der Abonnementspreis wird jährlich im Voraus in Rechnung gestellt oder bei Teilnahme am Lastschriftverfahren jährlich abgebucht.
Bei Nichterscheinen der Zeitschrift ohne Verschulden des Verlages oder infolge höherer Gewalt entfällt für den Verlag jegliche Lieferpflicht. – Anzeigenpreise nach Tarif vom 1.1.2017. Informationen und Angebote über Netzwerklizenzen erhalten Sie beim Verlag direkt. – Mit der Annahme von Originalbeiträgen zur Veröffentlichung erwirbt der Verlag das uneingeschränkte Verfügungsrecht.

Titelfoto
© Universität zu Lübeck

Hinweis für Autoren
Unter: www.mt-medizintechnik.de/Kontakt;
Manuskripte sind einzusenden an:
redaktion@mt-medizintechnik.de

G 8770 F
ISSN 0344-9416

Quelle: Universität zu Lübeck

Schwerpunktthema
Innovationen

Jahresüberblick

Heft-Nr.	1	2	3	4	5	6
Schwerpunkt-thema	Hospital 4.0	Strahlen-schutzrecht	OP-Integration	Innovationen	Hygiene	Patienten-sicherheit

Prävention und Reaktion

Internationale best practice *im integralen Risiko-management von Spitälern*

Autoren: M. Gruber, M. Durrer

Die Relevanz des Themas

Am Freitag, 12. Mai 2017 kam es zur vermutlich weltweit größten Cyber-Attacke. In 99 Ländern waren rund 75.000 Computer vom Computervirus *„Wanna Cry"* betroffen. Besonders brisant: Als Angriffsziele der Cyber-Attacke dienten unter anderem auch eine Vielzahl an britischen Spitälern, welche in der Folge ihre IT-Systeme herunterfahren mussten und nicht mehr auf Patientendaten zugreifen konnten. Patienten mussten deshalb in andere Spitäler verlegt und Operationen verschoben werden. Die Telefone blieben an diesem Tag stumm und der Rettungsdienst konnte nur noch eingeschränkt arbeiten.

Dieses Beispiel zeigt deutlich: Spitäler sind besonders verletzlich und deshalb anfällig für eine Vielzahl potenzieller Risiken. Als *kritische soziale Infrastrukturen* haben Spitäler indes eine enorm wichtige Bedeutung für das staatliche Gemeinwesen. Kommt es zu Ausfällen oder zu größeren Beeinträchtigungen bei einem Spital, hat dies nachhaltige Versorgungsengpässe zur Folge, was sich auf die öffentliche Sicherheit auswirken kann.

Spitäler sind zudem hochgradig komplexe Systeme, oft über mehrere Standorte verteilt. Sie bilden dabei ein wesentliches Rückgrat in der nationalen Gesundheitsversorgung und sind Meister im täglichen klinischen Risikomanagement um Leben und Tod. Diese Spitzenleistungen im klinischen Risikomanagement sind jedoch nur die eine Seite der Medaille: Für die Einhaltung internationaler best practice wird heute ein *spitalweites, integrales Risikomanagement-System* verlangt. Dieses fokussiert auf die spitalweiten Risiken und geht somit deutlich weiter als das klinische Risikomanagement.

Im Folgenden geht es darum, ausgewählte Aspekte dieser internationalen best practice im Risikomanagement von Spitälern zu beleuchten.

>> Für eilige Leser

Als ebenso komplexe wie kritische Infrastrukturen benötigen Spitäler ein ganzheitliches Risikomanagement, das im Sinne der best practice internationaler Normen aufgestellt ist und die vorbeugende Risikobeurteilung und reaktive Risikobewältigung gleichermaßen berücksichtigt. Der in diesem Beitrag beschriebene integrale Ansatz umfasst den gesamten normativen Rahmen einer Einrichtung. Er definiert und bewertet Einzelrisiken dreidimensional, indem er sie zu Szenarien verknüpft und auch den möglichen Reputationsschaden in die Betrachtung mit einbezieht. Mithilfe der best practice des integralen Risikomanagements gelingt es, sämtliche Informationen des Prozesses in den Gesamtkontext zu stellen und das Risikoprofil einer Institution unter Beachtung der geforderten Standards zu reduzieren.

Die Bedeutung internationaler best practice im Risikomanagement

Die Ausgestaltung, Implementierung und Überwachung eines integralen Risikomanagement-Systems ist ein unverzichtbarer und auch gesetzlich geforderter Teil der Führung. Unternehmen, Behörden, öffentliche Betriebe und gemeinnützige Einrichtungen müssen sich dieser Aufgabe stellen – gerade in einem wirtschaftlichen und politischen Umfeld, das sich permanent wandelt. Integrales Risikomanagement ist dabei ein zwingend notwendiger Bestandteil der Corporate Governance jeder Organisation, mag sie auch noch so klein sein.

Und was im Kleinen gilt, gilt selbstverständlich auch im Großen. Alle Organisationen haben die Verpflichtung zum integralen Risikomanagement. Deshalb macht integrales Risikomanagement auch vor Spitälern nicht halt, gänzlich ungeachtet ihrer Rechtsform und losgelöst von ihrer privatrechtlichen oder öffentlich-rechtlichen Eigentümerschaft. Die Ausgestaltung, Implementierung und Überwachung eines integralen Risikomanagement-Systems ist somit keine Kür, sondern ist eine gesetzlich geforderte Pflicht in der primären Verantwortung der obersten Führungsebene.

Kein Gesetz wird die Verantwortlichen jedoch im Detail anweisen, was genau zu tun ist, um ihrer Verantwortung gerecht zu werden. Aus diesem Grund ist der hilfsweise Beizug von internationalen Normen unabdingbar. Diese Normen sind Ausdruck eines weltweiten Konsenses und stellen somit die international anerkannte best practice im Risikomanagement dar. Im Bereich des Risikomanagements gilt dies

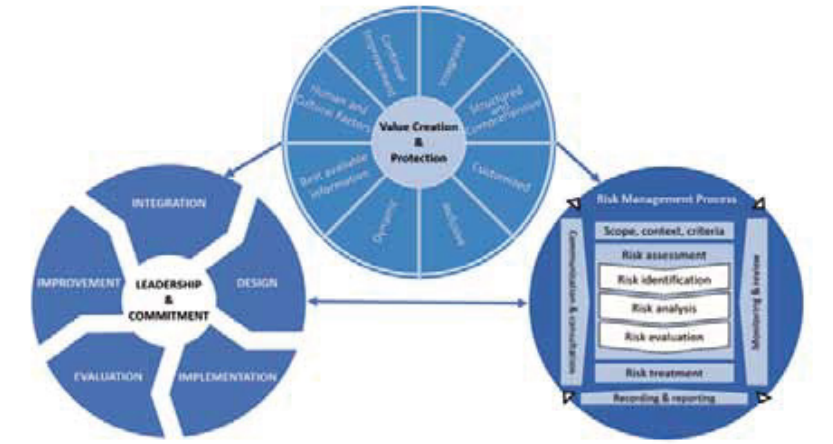

Bild 1: Die Norm ISO 31000:2018

insbesondere für die Norm ISO 31000, welche von der OECD bereits im Jahr 2014 *„de facto"* als *„world standard"* bezeichnet worden ist. Diese ist eine der weltweit meistgenutzten ISO-Normen und wird in der aktuellen Version 2018 dargestellt (**Bild 1**).

Eine Alternative zu ISO 31000:2018 stellt die vom US-amerikanischen *„Committee of Sponsoring Organizations of the Treadway Commission"* (COSO) herausgegebene Norm *„Enterprise Risk Management – Integrating with Strategy and Performance"* dar, welche ebenfalls auf internationalem Konsens basiert und in der aktuellen Version 2017 visualisiert worden ist (**Bild 2**).

Da diese internationalen Normen von privatrechtlichen Organisationen erlassen werden, stellen sie keine Rechtsnormen (im Rechtssinne) dar. Obwohl sie deshalb nicht per se rechtsverbindlich sind, setzen die internationalen Normen anerkanntermaßen den relevanten Maßstab für die weltweit anzuwendende Sorgfalt bei der Ausgestaltung, Implementierung und Überwachung eines integralen Risikomanagement-Systems, auch in einem Spital.

Ein nicht-existentes, mangelhaftes oder ungenügend überwachtes integrales Risikomanagement-System führt nach dem gewöhnlichen Lauf der Dinge und der allgemeinen Lebenserfahrung zu einem Vermögensschaden und kann folglich zivilrechtliche Haftungsansprüche gegen die Verantwortlichen auslösen. In einem Schadensfall hat die oberste Führungsebene des Spitals zu beweisen, dass sie sorgfältig gehandelt hat. Die Anwendung einer international anerkannten Norm und somit die Einhaltung von internationaler best practice im Risikomanagement hilft, diesen Beweis rechtsgültig zu erbringen. Dies ist umso wichtiger, als in der Regel bereits einfache Fahrlässigkeit das Verschulden und somit die persönliche Haftung der obersten Führungsebene des Spitals begründen kann.

Was bedeutet *„integrales"* Risikomanagement?

Sowohl ISO 31000:2018 wie auch das Framework von COSO stellen umfassende *Risikomanagement-Systeme* dar, welche die maßgeblichen Rahmenbedingungen und somit die Grundlagen für das Gelingen des *Risikomanagement-Prozesses* abgeben. Der Risikomanagement-Prozess stellt dabei den Kern dieser beiden Normen dar und umfasst sowohl bei ISO 31000 wie auch beim COSO-Framework die Prozessschritte der *Risikobeurteilung* (mit den Teilschritten Identifikation, Analyse und Bewertung) und der *Risikobewältigung*.

Traditionellerweise wird namentlich die letztgenannte *„Risikobewältigung"* vor allem *präventiv* verstanden. Danach sollen mittels *planerischer* Bewältigungsmaßnahmen die Eintrittshäufigkeit und das Schadensausmaß eines Risikos verringert werden. Demgegenüber zeichnet sich der *integrale Ansatz* insbesondere dadurch aus, dass ergänzend zu den präventiven auch *reaktive* Risikobewältigungsmaßnahmen auszuarbeiten sind. Diese umfassen gemäß der österreichischen Regel ONR 49000 ff. das Notfallmanagement, das Crisis Management (CM) sowie das Business Continuity Management (BCM). Integrales Risikomanagement bedeutet deshalb, dass für jedes Risiko ein angemessenes Notfall-, Krisen- und Kontinuitätsmanagement *geplant und eingeübt* werden muss.

Integrales Risikomanagement bedeutet ferner, dass auch das interne Kontrollsystem (IKS) einen integralen Bestandteil des Risikomanagement-Systems darstellt. Die Pflicht zur Ausgestaltung, Implementierung und Überwachung eines integralen Risikomanagement-Systems umfasst somit auch die materiellen Gehalte des IKS, des CM und des BCM. Dieses integrale Systemverständnis hat den unschlagbaren Vorteil, dass etwaige Doppelspurigkeiten bereits im Keim erstickt und Schnittstellen im Ansatz eliminiert werden, da nur *ein einziges System* zu bewirtschaften ist [1]. Dies führt auch dazu, dass lediglich *eine einzige Risikobeurteilung* über die gesamte Unternehmung (hier: das Spital) notwendig ist.

Risikobeurteilung hin, Risikobewältigung her: Damit ist an dieser Stelle zu klären, was heute unter dem Begriff „Risiko" zu verstehen ist.

Was bedeutet *„Risiko"* heute?

Traditionellerweise liegt dem Risikomanagement ein *zielorientiertes Risikoverständnis* zugrunde. Ein Risiko ist gemäß dieser Auffassung die Auswirkung von *Unsicherheit auf Ziele*. Der Begriff *„Risiko"* ist somit per Definition auf *„Ziele"* ausgerichtet. Dieses traditionelle Verständnis geht indes zu wenig weit, denn oftmals sind die Ziele der Unternehmung nicht nach der SMART-Methode ausformuliert, sie sind also alles andere als

S = specific (spezifisch);
M = measurable (messbar);
A = achievable (erreichbar);
R = reasonable (realistisch);
T = time-bound (terminiert).

Sind demnach bereits die Ziele nicht präzise definiert, fehlt es in der Folge auch an der Präzisi-

Bild 2: *„Enterprise Risk Management – Integrating with Strategy and Performance"* von COSO

on in der Risikobeurteilung. Und die in der Praxis oft verwendeten, zumindest klar quantifizierten *finanziellen Ziele* eines Spitals erweisen sich im Hinblick auf das integrale Risikomanagement als zu eng gefasst.

Die oberste Führungsebene eines Spitals ist deshalb gehalten, weiterzudenken und den *gesamten normativen Rahmen* als relevante Messgröße in die durch Risiken gefährdete Zone miteinzubeziehen. Dieser normative Rahmen steht denn auch am Ausgangspunkt für die Ausgestaltung und Implementierung des ISO- und COSO-konformen Risiko-Management-Systems NEXTREMIS®. Das aufbauende Fundament des normativen Rahmens bilden dabei die *Werte* der Organisation. Diese (immateriellen) Werte stellen wiederum die Grundlage für die Konkretisierung der *Vision* sowie des *Leitbildes* dar (**Bild 3**). Erst danach werden daraus die mittelfristigen strategischen und finanziellen Ziele des Spitals abgeleitet.

Gemäß unserer Erfahrung ist somit der normative Rahmen bei Weitem die geeignete Messgröße hinsichtlich der Risikodefinition, wird letztere doch um weiche Faktoren (die sog. *„intangibles"*) erweitert.

Mit der Ausrichtung des Risikobegriffs auf den normativen Rahmen einher geht sodann die Festlegung der individuellen *Risikopolitik* und der *Risikokultur*, welche aus der Unternehmenspolitik und aus der Unternehmenskultur des Spitals abzuleiten sind und mit diesen in Einklang stehen müssen. Die schriftlich festzuhaltende Risikopolitik zeigt dabei auf, wie das Spital mit Risiken umgeht und worin die Risikomanagement-Ziele bestehen. Um das Risikobewusstsein zu stärken, ist die Risikopolitik im Spital aktiv zu kommunizieren. Die Risikokultur bildet sich hingegen durch das Denken und Handeln aller Mitarbeitenden sowie durch das Vorleben durch die oberste Führungsebene des Spitals heraus.

Der normative Rahmen sowie die Risikopolitik und die Risikokultur werden in NEXTREMIS® wie folgt visualisiert (**Bild 4**).

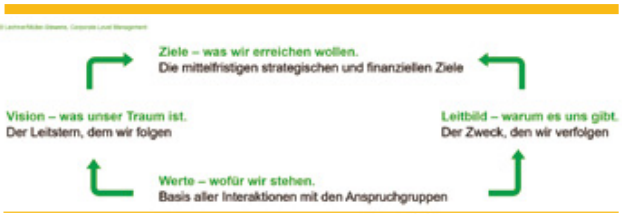

Bild 3: Definition des normativen Rahmens als Grundlage von NEXTREMIS®

Bild 4: Die umsetzungsorientierte Visualisierung von NEXTREMIS® zu ISO 31000 und ONR 49000

Was bedeutet *„Management"* heute?

Wer glaubt, lediglich die Hierarchie-Stufe *„Management"* müsse Risiken managen, der irrt. Denn gemeint ist vorliegend nicht die Hierarchiestufe *„Management"*, auch wenn die internationalen Normen hinsichtlich der Verantwortung in einem ersten Schritt *„Top-Down"* ansetzen und das Überwachungsorgan sowie das Management als Verantwortliche für das System und den Prozess des Risikomanagements in die Pflicht nehmen.

Ergänzend zum Top-Down-Ansatz tritt jedoch immer auch der *„Bottom-Up"*-Ansatz hinzu, also der Einbezug aller Mitarbeitenden mit klaren Kommunikationswegen (auch unter Einbezug des Critical Incident Reporting Systems CIRS), dies in Einklang mit der Risikopolitik und der Risikokultur des Spitals.

In der Regel kann das Überwachungsorgan die konkrete Ausgestaltung, die Implementierung und die Überwachung des Risikomanagements an das operative Management delegieren. Dies wird insbesondere im Modell der *„Three Lines of Defense"* ersichtlich, welches drei voneinander unabhängige Ebenen unterhalb der Unternehmensführung umfasst, die bei der Steuerung der spitalweiten Risiken mitwirken (**Bild 5**).

Besonders wichtig dabei ist, dass bei einer Delegation *klare Berichterstattungswege* implementiert werden. Die First Line untersteht dabei in der Regel direkt dem Management und legt diesem Rechenschaft über die Prozesse ab. Auch der Risikomanager und somit die Second Line untersteht primär dem Management. In der Praxis verfügt diese Second Line aber immer öfter über eine zusätzliche, direkte Berichterstattungslinie zum Überwachungsorgan. Und die Third Line berichtet in der Regel direkt an das Überwachungsorgan, welches für das integrale Risikomanagement als Ganzes verantwortlich ist – und dies auch bei einer Delegation bleibt.

Im Ergebnis bedeutet dies nichts weniger, als dass das Risikomanagement-System als *ständiges Traktandum* an den Führungssitzungen des Überwachungsorgans wie auch des Managements aufs Tapet gehört.

Bei Lichte besehen hat das Überwachungsorgan sogar die Möglichkeit, die externen Auditoren der Revisionsstelle als vierte Verteidigungslinie ins Risikomanagement miteinzubeziehen. Generell ist leider festzustellen, dass das Konzept der drei (bzw. vier) Verteidigungslinien vom Überwachungsorgan noch viel zu häufig mit voneinander hermetisch abgeschotteten Silos gleichgesetzt wird, die nicht miteinander kommunizieren. Dabei wäre es für das Überwachungsorgan ja ein Leichtes, diese zu osmotischen, stetig miteinander kommunizierenden Gefäßen zu transformieren.

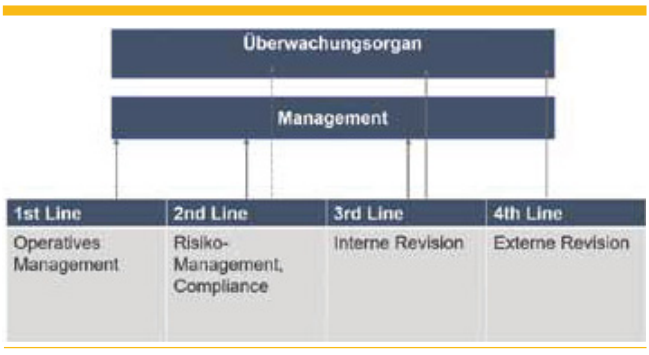

Bild 5: Three-Lines-of-Defense-Modell. Oder eben Four.

Was bedeutet Risikobeurteilung heute?

Eine der größten Herausforderungen ist es, in der *Risikobeurteilung* die unternehmensweiten Risiken zu *identifizieren*, zu *analysieren* und zu *bewerten*. Diese anspruchsvolle Aufgabe muss heute auf der Basis von *„best available information"* erfolgen, was systematisches und konsequentes Denken und Handeln voraussetzt.

a) Risiko-Identifikation
Oft fehlt es an Vorstellungskraft zur Schlüsselfrage des Risikomanagements, die da lautet: *„Was kann passieren?"* Diesem Umstand kann beispielsweise mittels der *„Guided Brainstorming"*-Methode begegnet werden, mit der visualisierte Gefahren auf ihren Risikogehalt für das Spital in einer möglichst interdisziplinär zusammengesetzten Steuerungsgruppe durchgearbeitet werden (**Bild 6**).

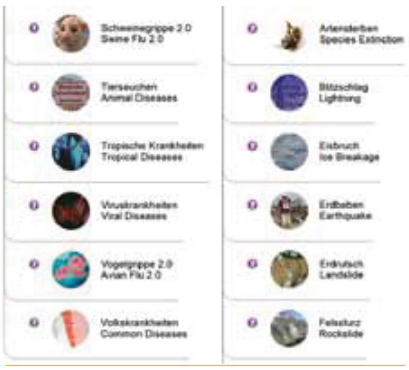

Bild 6: Beispiel eines „Guided Brainstorming" im RISKMONITOR® mit laufend kuratierten Inhalten

Generell ist festzuhalten, dass das risikobasierte (und per se tabulose) Brainstorming in Teams eine spezifische Dynamik aufweist und damit auch den Praktikern einen großen Mehrwert bietet: Denn deren Erfahrung fließt umgehend in die Ausgestaltung und betriebliche Einpassung des Risikomanagement-Systems ein. So wird das Risikomanagement Teil der eigenen Risikokultur. Und nur so kann es organisationsweit täglich gelebt werden.
Aus Erfahrung lässt sich zudem feststellen, dass die „Guided Brainstorming"-Methode sowohl für das erstmalige Aufsetzen des Prozesses als auch für die spätere Aktualisierung der bestehenden Inhalte in Spitälern hocheffizient und zielführend ist.

b) Risiko-Analyse
Die vorgängig identifizierten Gefahren sind nach Ursache und Wirkung zu analysieren, und zwar so: *Eine* bestimmte Ursache mit *einer* bestimmten Wirkung. Dabei stehen folgende Kombinationen aus Ursache-Wirkungs-Zusammenhängen zur Verfügung, die einen ersten Hinweis auf die Priorisierung liefern:

1) Interne Ursache mit interner Wirkung;
2) Externe Ursache mit interner Wirkung;
3) Interne Ursache mit externer Wirkung;
4) Externe Ursache mit externer Wirkung.

Dabei bezieht sich die *„interne Wirkung"* immer auf die Entität, für welche das Risikomanagement-System unternehmensweit designt wird, vorliegend also auf das Spital als solches.
An dieser Stelle ist mit Nachdruck darauf hinzuweisen, dass jedes so nach Ursache und Wirkung analysierte Risiko daraufhin zu überprüfen ist, ob bei einem allfälligen Eintritt Menschen zu Schaden kommen können, ein Risikoeintritt in der Konsequenz somit Verletzte und/oder Tote bewirken kann. Dies nicht zuletzt mit Blick auf die *Fürsorgepflicht* des Spitals als Arbeitgeber.

c) Risiko-Bewertung
In der Praxis immer noch häufig anzutreffen sind Risikobewertungs-Methoden, die auf zwei Achsen die „Eintrittswahrscheinlichkeit" mit dem „Finanziellen Schaden" koppeln und das Ergebnis zweidimensional etwa wie folgt darstellen (**Bild 7**).

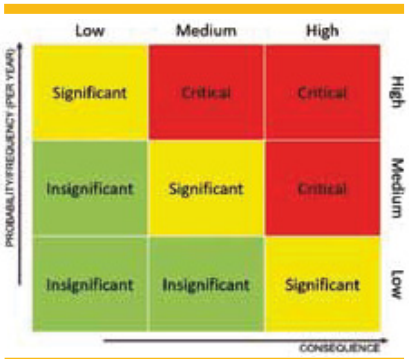

Bild 7: Zweidimensionale Heatmap

Immer wieder stellen wir fest, dass die Berechnung einer Eintrittswahrscheinlichkeit viele überfordert und lediglich eine *Scheinsicherheit* gebiert: Denn was genau lässt sich schon daraus ableiten, dass ein Risiko mit einer Wahrscheinlichkeit von z. B. 37 % eintritt? In der Praxis fällt es den Involvierten deutlich leichter, mit der *„Häufigkeit"* zu rechnen, will heißen, eine Beurteilung vorzunehmen, wie *häufig* ein identifiziertes und analysiertes Ereignis auf der Zeitachse eintreffen kann. Ob dabei mit drei, vier oder fünf Farben gearbeitet wird, aus denen sich die *„Heatmap"* genannte Auswertung ergibt, ist nicht entscheidend. Gemäß unserer Beobachtung hat sich in der Praxis die Bewertung mit einer Fünferskala bestens bewährt.
Nun ist heute jedermann klar, dass die Welt nicht bloß aus flachen zwei Dimensionen besteht, sondern dass die Menschheit sich seit je im dreidimensionalen Raum bewegt. Gleiches gilt nach dem neuesten Stand der Entwicklung auch für das Risikomanagement: Risiken sind danach nicht länger zweidimensional zu bewerten, sondern *dreidimensional*, dies unter Einbezug des Reputationsschadens (**Bild 8**). Wegleitend für diesen neuen, dreidimensionalen Bewertungsansatz war die Erkenntnis, dass der finanzielle Schaden aus einem Ereignis für ein Spital zwar eher gering, ein damit verbundener Reputationsschaden aber u. U. existenziell sein kann. Wichtig ist dabei, dass die dreidimensionalen Bewertungskriterien für jedes Spital individuell festgelegt werden.
Aber eben: Mit dieser Ausdehnung der Bewertung in die nächste räumliche Dimension bleiben Einzelrisiken immer noch in sich geschlossene singuläre Trabanten. Um wie viel realitätsnaher wäre es denn, wenn wir diese singulären Einzelrisiken zu ganzen Szenarien verknüpfen könnten, am liebsten gleich per drag&drop wie in **Bild 9**? Das geht heute technisch alles – und selbstverständlich sind auch diese Szenarien im Sinne von Ursache-Wirkungs-Ketten dreidimensional zu bewerten.

Bild 8: Risiken werden in NEXTREMIS® dreidimensional bewertet (unter Einbezug des Reputationsschadens)

Bild 9: Von Einzelrisiken zu Szenarien per drag&drop: Ausschnitt aus einer strategischen Führungsübung mit Reflexwirkungen auf Spitäler (am Beispiel von koordinierten Terroranschlägen gegen mehrere kritische Infrastrukturen). Visualisierung durch die beiden Verfasser.

Heikle Fragen in Bezug auf die Risikobewertung stellen sich bei Spitälern immer wieder: Etwa wie sie Risiken *„konsolidieren"* sollen, die beispielsweise an den unterschiedlichen Standorten eines Spitals auftreten können. Erfahrungsgemäß lohnt es sich, auf eine solche Konsolidierung zu verzichten und die bewerteten Risiken nach den Standorten gegliedert zu bewirtschaften: Denn nur so erhält das Überwachungsorgan jene Sicht auf die gesamte Risikolandschaft, welche ihm konsequentes und schlüssiges Handeln im Gesamtkontext erlaubt. Keine Probleme bestehen jedoch, falls ein Spital eine Konzernstruktur (mit Beteiligungen an Tochtergesellschaften) aufweist (oder selbst Teil einer übergeordneten Beteiligungsstruktur ist). Diesfalls verlangt die internationale best practice, dass die in jeder Gesellschaft zu führenden (und zu pflegenden) Risikomanagement-Systeme aufeinander abgestimmt sind. Die Organe einer Tochtergesellschaft können sich also nicht haftungsmindernd darauf berufen, ihre Risiken seien bereits im Risikomanagement-System der Muttergesellschaft enthalten.

Das Überwachungsorgan hat zudem ein besonderes Augenmerk auf die stete Aktualisierung des Risikomanagements zu richten, auf die sog. *„best available information"* (**Bild 10**). Woher diese Informationen stammen, ist dabei sekundär – viel wichtiger ist, dass die zugänglichen und gesammelten Informationen systematisch ausgewertet und auf ihre Relevanz für das jeweilige Spital hin überprüft werden.

Vor diesem Hintergrund sei die Frage gestellt, was mit Verantwortlichen geschieht, die den hohen Sorgfaltspflichten an die Ausgestaltung, Implementierung und Überwachung des integralen Risikomanagement-Systems nicht nachkommen. Auch diese Frage lässt sich klar beantworten, wie diverse Beispiele in jüngster Vergangenheit aus der produzierenden Industrie gezeigt haben: Die Verantwortlichen setzen sich persönlich sowohl strafrechtlich als auch zivilrechtlich hohen Risiken aus, die in extremis zur Zerstörung der Karriere und der persönlichen Reputation bis hin zum finanziellen Ruin führen können.

Unter allen Prämissen setzt die Konzeption des integralen Risikomanagements (als System und als Prozess) voraus, dass die Verantwortlichen *aktiv und sorgfältig handeln*, dies in voller Übereinstimmung mit der gelebten internationalen best practice, wie sie in diesem Artikel beschrieben wird. Das vorausgesetzte *„aktive Tun"* gilt folglich bei allen Elementen des integralen Risikomanagements, somit insbesondere auch bei der Risikobewältigung.

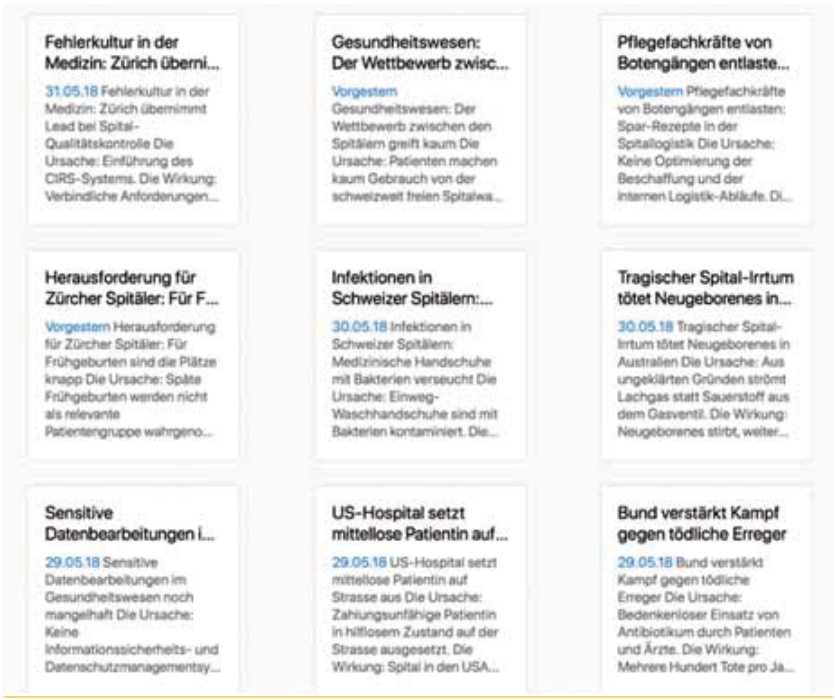

Bild 10: RISKMONITOR® als Beispiel für „best available information"

Was bedeutet *„Risikobewältigung"* heute?

Die Risikobewältigung ist (wie die Risikobeurteilung) Teil des Risikomanagement-Prozesses. Bei der Risikobewältigung werden sämtliche beurteilten Risiken mit Handlungsbedarf mittels konkreter Maßnahmen (Bezeichnung der verantwortlichen Person mit Zeitplan und Budget) aus dem nicht-konformen IST-Zustand in den konformen SOLL-Zustand überführt. Ein besonderes Augenmerk ist dabei auf all jene Risiken zu richten, bei denen es zu Verletzten und/oder Toten kommen kann. Hier besteht *immer* akuter Handlungsbedarf.

Bei der Risikobewältigung steht somit das eigentliche *„Managen"* der Risiken im Zentrum. Dazu gehören (nebst der Erarbeitung von *präventiven* Risikobewältigungsmaßnahmen) insbesondere auch *reaktive* Risikobewältigungsmaßnahmen. Verwirklicht sich also ein Risiko

RN	Hackerangriff auf Server (mit Verschlüsselung)								1
Analyse		Verletzte		Tote		Klasse	H	F	R
Ursache: Hacker gelingt es, die Serverpasswörter zu knacken, er dringt in unser System ein.		MIN	MAX	MIN	MAX	Ist	5	2	3
Wirkung: Verschlüsselung sämtlicher Dateien; Wiederherstellung nur gegen Lösegeld.		0	0	0	0	Soll	3	1	2
Owner	Standort:	Upgrade: Nein.				Beurteilt am: 12.06.2017			
Audit Bestehende Massnahmen		Von		Bis		Status	Zuständig		

Bild 11: Beispiel für einen individuell konfigurierbaren Resilienzbericht aus NEXTREMIS®

und tritt es ein, müssen die vorbereiteten reaktiven Bewältigungsmaßnahmen ohne Weiteres, d. h. *„auf Knopfdruck"*, ausgelöst werden können.
Bei der Risikobewältigung steht somit die Ausarbeitung von Sofortmaßnahmen, von Notfall-, Krisen- und Kontinuitätsplänen im Fokus, welche bei Risikoeintritt ein Management in Echtzeit ermöglichen.
Um das Risikoprofil des Spitals zu reduzieren, sind im Risikomanagement-Prozess deshalb sämtliche Informationen aus der Risikobeurteilung in den Gesamtkontext zu stellen, mit konkreten Bewältigungsmaßnahmen zu unterlegen und zu priorisieren. Dabei hat das oberste Überwachungsorgan insbesondere zu kontrollieren, inwiefern die beschlossenen Risikobewältigungsmaßnahmen auch tatsächlich umgesetzt werden. Um Doppelspurigkeiten zu vermeiden, bedarf diese Fortschrittskontrolle in aller Regel der digitalen Synchronisation.

Die Erhöhung der Resilienz als messbarer Nutzen

Der messbare Nutzen des integralen Risikomanagements besteht darin, die Resilienz und damit die Widerstandsfähigkeit des Spitals zu erhöhen. Diese Entwicklung kann gut nachvollziehbar in einem sog. Resilienzbericht festgeschrieben und dokumentiert werden (**Bild 11**). Diese beweiskräftige Dokumentation ist nicht nur im Hinblick auf das Reporting an das oberste Überwachungsorgan im Spital wichtig: Sie ist insbesondere auch dann von rechtlichem Belang, falls ein Risiko tatsächlich eintritt. Denn aus haftungsrechtlicher Sicht ist es ratsam, die einzelnen Schritte in Bezug auf das integrale Risikomanagement-System sorgfältig zu dokumentieren, um in einem allfälligen Verantwortlichkeitsprozess nachweisen zu können, dass der Entscheidungsfindungsprozess im Rahmen des integralen Risikomanagement-Systems sorgfältig angegangen und die Überwachungspflicht umfassend wahrgenommen worden ist.

Die 10 Gebote des integralen Risikomanagements für Spitäler

Zusammenfassend lassen sich aus dem Vorstehenden die nachfolgenden *10 Gebote des integralen Risikomanagements für Spitäler* herleiten:

1. Integrales Risikomanagement ist für jedes Spital ein „must", daran führt kein Weg vorbei.
2. Setzen Sie die internationale „best practice" auch mittels „best available information" zeitnah um.
3. Richten Sie die Risikodefinition des Spitals auf dessen normativen Rahmen aus.
4. Bewerten Sie die Risiken des Spitals dreidimensional, dies unter Einbezug des Reputationsschadens.
5. Bleiben Sie nicht bei Einzelrisiken des Spitals stehen, sondern gehen Sie baldmöglichst zu Szenarien über. Bewerten Sie auch diese Szenarien dreidimensional.
6. Die Ausgestaltung, Implementierung und Überwachung des integralen Risikomanagements ist und bleibt Chefsache, Sie können diese nie gänzlich delegieren.
7. Nehmen Sie die Pflicht zum integralen Risikomanagement im wohlverstandenen Eigeninteresse sehr ernst. Und handeln Sie entsprechend.
8. Beziehen Sie die Mitarbeitenden in das integrale Risikomanagement des Spitals mit ein. Üben Sie mit ihnen insbesondere das Notfall-, Krisen- und Business Continuity Management praxisnah ein.
9. Erstellen Sie eine beweiskräftige Dokumentation zur Entwicklung des spitalweiten Risikomanagements über die Zeit. Und bewahren Sie diese nicht nur zur Geschichtsschreibung sorgfältig auf.
10. Messen Sie regelmäßig, wie sich die Resilienz des Spitals erhöht, und kommunizieren Sie diese aktiv.

Literatur

[1] Durrer, Mirjam; Die Pflicht des Verwaltungsrates zum integralen Risikomanagement in KMU. Dike 2017 (https://www.dike.ch/Mirjam-Durrer).

Dokumentation: M. Gruber, M. Durrer. Internationale best practice im integralen Risikomanagement von Spitälern. mt|medizintechnik 138 (2018), Nr. 4, S. 10, 11 Bilder, 1 Lit.-Ang.

Schlagwörter: Risikomanagementprozess, best practice, Risikokultur, Notfallmanagement

Autoren

Dr. iur. Marco Gruber

Fürsprecher, Gruber Partner AG, Aarau und Luzern,
E-Mail: marco.gruber@gruberpartner.ch,
Web: www.gruberpartner.ch

Dr. iur. Mirjam Durrer

Rechtsanwältin, Gruber Partner AG, Aarau und Luzern,
E-Mail: supportlu@gruberpartner.ch,
Web: www.gruberpartner.ch