

# logbuch



## THEMEN:

- 01 ISO IEC 80001-1: ein neuer Standard für die Vernetzung von medizinischen Geräten?
- 02 Business Continuity Management – Einstieg leicht gemacht mit dem CRISAM® BCM Catalog
- 03 CRISAM® ISMS (IT-Riskmanagement) Katalog-Version V16
- 04 Die Kärntner Landesregierung nutzt CRISAM® - Ein Pilotprojekt mit Überzeugungskraft
- 05 Veranstaltungsnachlese

## 01

## ISO IEC 80001-1: ein neuer Standard für die Vernetzung von medizinischen Geräten?

Sehr geehrte  
Geschäftsfreunde!

Zu Beginn dieses Newsletters erzählt Ihnen Manfred Stallinger, wie Sie CRISAM® bei der Vernetzung von medizinischen Geräten in Richtung der ISO IEC 80001-1 unterstützen kann.

Danach stellt Ihnen Wolfgang Mahr kurz den CRISAM® BCM Catalog vor und Markus Müller präsentiert Ihnen die Neuerungen im CRISAM® ISMS Catalog V16.

Christina Haas berichtet danach über das erfolgreiche Pilotprojekt bei der Kärntner Landesregierung und abschließend geben wir Ihnen einen kurzen Überblick über einige Veranstaltungen, die vor kurzem stattgefunden haben.

Im Namen des CRISAM® Teams wünsche ich Ihnen viel Freude bei der Lektüre und eine schöne, erholsame Urlaubszeit!

Ihre  
Mag.ª Anita Wenigwieser  
calpana business consulting  
gmbh

**Die Komplexität im klinischen Alltag hat in den letzten Jahren durch eine stetig steigende Durchdringung von IT-Anwendungen in Medizinprodukten und die steigenden Anforderungen an Interoperabilität und Flexibilität dramatisch zugenommen. Insbesondere das Zusammenwirken mehrerer, auch von verschiedenen Herstellern stammenden Medizinprodukten stellt die Klinik-Betreiber vor große Herausforderungen. Besonders in kritischen Bereichen, beispielsweise im Operationssaal spielt die Vernetzung und Integration der einzelnen Geräte eine immer wichtigere Rolle. Eine Isolation der Medizintechnik-IT-Netzwerke von den IT-Netzwerken im allgemeinen Klinikumfeld ist aufgrund der geforderten Interoperabilität mit dem Nichtmedizingeräte-Umfeld nicht mehr denkbar. Exakt an dieser Stelle setzt die Normfamilie, beginnend mit der ISO IEC 80001-1 („Risk Management for IT-Networks incorporating Medical Devices“) an. Für Klinik-Betreiber, die Medizinprodukte für eine klar umrissene Zweckbestimmung in ein allgemeines Klinik-IT-Netzwerk integrieren und vernetzen wollen, werden Vorgaben definiert, die einem Stand der Technik für diese Integration entsprechen. Dieser Stand der Technik wirkt somit auf das Inverkehrbringen und Betreiben von Medizinprodukten (MP) im Sinne des Medizinproduktegesetzes (MPG) zurück.**



DI Dr. Dr. Manfred Stallinger, MBA  
Geschäftsführer  
calpana business consulting gmbh

Die Vernetzung von medizinischen Geräten spielt in Gesundheitsbetrieben (Krankenhäuser, Kliniken, Ärztezentren etc.) eine zentrale Rolle, ohne der ein effizienter Klinikbetrieb nicht aufrechterhalten werden kann. Besonders in Zeiten von Gesundheitsreformen und Sparpaketen muss in Verbesserung der Prozesse und Abläufe sowie in weitere Automatisierung investiert werden, um einen Qualitätsverlust in der medizinischen Versorgung verhindern zu können.

Labordaten müssen in das Krankenhausinformationssystem (KIS) übertragen werden, vom mobilen Visitenwagen abrufbar sein und zur Weiterverarbeitung in den entsprechenden Abteilungen zur Verfügung stehen. Dabei stellt sich jedoch die Frage: Ist das Gebilde an Medizinprodukten, IT-Anwendungen und IT-Netzwerken ein, in die Klinik-IT integrierter Verbund von Medizinprodukten (MP), oder handelt es sich dabei um ein Medizinprodukt als gesamte Einheit? Die Beantwortung dieser Frage hat weitreichende Konsequenzen, da Medizinprodukte mit dem Medizinproduktegesetz (MPG) einer sehr strengen gesetzlichen Regulierung unterliegen.

Exakt an dieser Stelle setzt der neue Standard ISO IEC 80001-1 an. Entsprechend der Norm kann die Frage folgendermaßen beantwortet werden: Wird der Verbund von Geräten von einem einzigen Medizinprodukte-Hersteller integriert und betrieben, so ist es als medizintechnisches System in der Verantwortung des MP-Herstellers zu sehen.

>> Lesen Sie weiter auf der nächsten Seite.



# logbuch

## 01

Ist es jedoch ein Verbund an Medizinprodukten unterschiedlicher Hersteller, integriert im IT-Netzwerk der Klinik, so ist es ein Verbund aus Medizinprodukten und die Auflagen der Norm treffen vollinhaltlich zu. Die Verantwortung für den ordnungsgemäßen Betrieb im Sinne des Medizinproduktegesetzes liegt beim Klinik-Betreiber.

Medizinprodukte müssen vermehrt in übergeordnete Klinik-IT-Netzwerke eingebunden werden, um Daten sowohl klinikweit, als auch für telemedizinische Anwendungen hausübergreifend bereitstellen zu können. Somit sind bereits heute nahezu alle IT-Netzwerke in Kliniken von diesem neuen „Stand der Technik“ der Norm erfasst.

Im Rahmen der Entwicklung der ISO IEC 80001-1 wurde dem Faktum Rechnung getragen, dass die Integration von Medizinprodukten in ein Klinik-IT-Netzwerk neue Risiken birgt. Häufige Änderungen, Erweiterungen, alle Gefahren von Viren bis Schadsoftware sind in nicht isolierten Klinik-IT-Netzwerken zu finden. Darüber hinaus wurde auch erkannt, dass klare Verantwortungsstrukturen zwischen dem medizinischen Klinikverantwortlichen, dem Medizinprodukte-Hersteller und dem IT-Netzwerk-Provider festgelegt werden müssen.

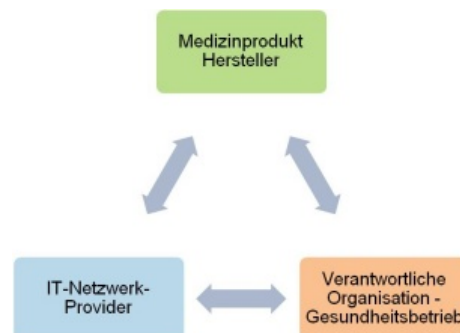


Abbildung 1: ISO 80001-1 Verantwortungsstruktur

So schreibt der neue „Stand der Technik“ dem Klinik-Betreiber für die Integration von medizinischen Geräten in das IT-Netzwerk, dem Medizinproduktegesetz für Hersteller von Medizinprodukten gleichgestellte Auflagen vor. Kern dieser Auflagen ist das Identifizieren und Bewerten möglicher Risiken beim Betrieb der Medizinprodukte im IT-Netzwerk, Bewerten der Effektivität von Vorkehrungen, Darstellen der Restrisiken in Bezug zu, vom Top-Management vorgegebenen Akzeptanzkriterien.

Die ISO IEC 80001-1 verlangt die Implementierung eines nachvollziehbaren und streng reglementierten Risikomanagement Prozesses. Auch hier ist es wichtig, eine klare und nachvollziehbare Methodik zugrunde zu legen. Nicht zuletzt verlangt die Norm eine Messbarkeit der Effektivität, einen klaren Wert für das verbleibende Restrisiko und einen SOLL-IST Vergleich zum, vom Top Management akzeptierten Risiko. Der „Medizinische-IT-Netzwerk Risikomanager“ ist als zentraler Manager aller Risiken, die sich aus der Integration von Medizinprodukten in ein IT-Netzwerk ergeben können, vom Top-Management einzusetzen. Er ist für die Abnahmen geplanter Netzwerkänderungen, der Feststellung des verbleibenden Restrisikos und die Freigabe der durchgeführten Änderungen vor dem Live-Betrieb verantwortlich und berichtet an das verantwortliche Management.

Für Klinik-Betreiber wird es an dieser Stelle, nicht zuletzt aus wirtschaftlichen Gründen erforderlich sein, eine klar definierte Abgrenzung zum IT-Netzwerk Provider des allgemeinen

>> Lesen Sie weiter auf der nächsten Seite.



# logbuch

## 01

Klinik IT-Netzwerkes zu finden. Gelingt diese Abgrenzung nicht, so hat der Provider des Klinik-IT-Netzwerkes auch die sehr aufwendigen Auflagen aus dem Medizinproduktegesetz zu erfüllen.

Eine durchgehende Umsetzung dieser Normvorgaben in Gesundheitsbetrieben, die als „Stand der Technik“ zu gesetzlichen Auflagen werden, erfordert eine entsprechende Implementierungsdauer. Wir empfehlen daher mit der Umsetzung bereits frühzeitig zu beginnen. Ein erster und wichtiger Schritt in Richtung der ISO IEC 80001-1 ist die Einführung eines nachvollziehbaren Risikomanagement Prozesses im IT-Netzwerk. Im Rahmen der kontinuierlichen Verbesserung sollte dieser Prozess weiterführend auf die einzubindenden Medizinprodukte ausgeweitet und somit ein erster Meilenstein in Richtung Umsetzung der Norm erreicht werden.

Der Weg zur ISO IEC 80001-1 Compliance sollte in einem abgegrenzten Pilotprojekt methoden- und toolgestützt begonnen werden. CRISAM® bietet Ihnen bereits jetzt eine umfassende Unterstützung für einen ISO IEC 80001-1 konformen Risikomanagement Prozess. Die Unterstützung generischer Medizinprodukte im CRISAM® Explorer wird aktuell geplant und soll demnächst als Katalog mit den entsprechenden Report-Packs und Compliance-Berichten bereitgestellt werden.

Calpana begleitet Sie mit CRISAM® sehr gerne auf dem Weg zu einem effizienten Risikomanagement Prozess und ISO IEC 80001-1 Compliance.

## 02

### Business Continuity Management – Einstieg leicht gemacht mit dem CRISAM® BCM Catalog



Wolfgang Mahr  
governance & continuity gmbh

**Der CRISAM® BCM Catalog bietet eine effiziente Methode, ein Business Continuity Management (BCM) Projekt aufzusetzen und dieses weiter zu entwickeln. BCM ist ein kontinuierlicher Prozess, der zwar als Projekt initiiert wird, dann aber das Unternehmen im Rahmen der Corporate Governance begleitet, um den vollen Nutzen zu erzielen.**

Der Katalog enthält alle Bausteine und Kontrollziele zur Bewertung eines Business-Continuity-Management-Systems (BCMS). Ein weiterer Nutzen des Katalogs ist die Fortschrittskontrolle: der Reifegrad der Implementierung kann zu jedem Zeitpunkt in Reports kommuniziert werden.

Der BCM Katalog wird vom CRISAM® Entwicklungspartner governance & continuity gmbh herausgegeben und weiterentwickelt. Ein White Paper zum Thema „Business Continuity für KMUs“ ist als Download von <http://continuuuity.ch/downloads.php> verfügbar. Die dort beschriebenen Ansätze gelten ebenfalls für Grossunternehmen.

#### Business Continuity Management

- ist ein ganzheitlicher Management-Prozess, der potenzielle Bedrohungen für eine Organisation identifiziert.
- Dieser Prozess identifiziert schwerwiegende Auswirkungen dieser Bedrohungen auf die Geschäftstätigkeit.
- Es bietet einen Rahmen für den Aufbau der organisatorischen Widerstandsfähigkeit (Resilienz).
- Der Prozess ist Basis für wirksame Massnahmen, die den Interessen der wichtigsten Stakeholders, der Reputation, Marke und der wertschöpfenden Aktivitäten dienen.

Quelle: The Business Continuity Institute & Standard BS 25999



# logbuch

## 03

### CRISAM® ISMS (IT-Riskmanagement) Katalog-Version V16



Markus Müller  
Consultant  
calpana business consulting gmbh

Im jeweiligen CRISAM® Katalog vereint sich das gebündelte Fachwissen des Risikomanagements in Form von Fragen, Bewertungsleitfäden und Gewichtungen für interne und externe Auditoren. Nur durch die Anpassung des CRISAM® IT-Riskmanagement Systems mit den jeweils aktuellen Katalogen kann sichergestellt werden, dass sich das Rating selbst und die erstellten Maßnahmen zur Erreichung des Ratings vom aktuellen Stand der Technik ableiten. Im Folgenden ein Überblick über die letzten Neuerungen.

#### CRISAM® ISMS Katalog

Der ISMS Katalog (Information Security Management System) umfasst alle relevanten technischen, organisatorischen, strategischen und rechtlichen Fragen aus den führenden Standardwerken ISO 27000, ITIL, Cobit, SOX, BSI und ÖSHB. In der 16. Version dieses Katalogs, der bereits mehr als 150 Bausteine mit über 1.500 Kontrollzielen enthält, wurden wiederum viele Anpassungen an den aktuellen Stand der Technik sowie an aktuelle Standards und Normen durchgeführt. Der Katalog ist vollständig in den Sprachen Deutsch und Englisch verfügbar.

Zusätzlich zu den laufenden Qualitätsverbesserungen bei Fragen und Bewertungsleitfäden ist mit folgenden Neuerungen zu rechnen:

#### ITIL V3

Um dem Stand der Technik in Sachen Service Management gerecht zu werden, wurde ITIL V3 in den ISMS Katalog aufgenommen und kann nun ebenfalls mit CRISAM® modelliert und bewertet werden. Dies bedeutet aber nicht, dass ITIL V2 entfernt wurde. Es kann sowohl mit ITIL V2 als auch mit ITIL V3-Bausteinen gearbeitet werden.

#### BSI Grundschutz

Im Zuge der Qualitätssicherung werden die vorhandenen Kontrollziele immer wieder auf eine mögliche Compliance zu anderen Normen und Standards geprüft. Im aktuellen ISMS Katalog V16 wird es nun möglich sein, mit Hilfe des Compliance-Berichts Risikoanalysen hinsichtlich einer Compliance in Richtung BSI-Grundschutz durchzuführen.

#### COBIT-Quellen

Auch für COBIT wurden die Kontrollziele des ISMS Katalogs überarbeitet und mit den nötigen Quellverweisen hinterlegt, um mit dem CRISAM® Compliance-Bericht die Einhaltung der COBIT-Anforderungen übersichtlich darstellen zu können.





# logbuch

## 04

### Die Kärntner Landesregierung nutzt CRISAM® - Ein Pilotprojekt mit Überzeugungskraft



Ing. Mag.ª Christina Haas  
Consultant  
calpana business consulting gmbh

In der EDV Abteilung der Kärntner Landesregierung, unter der Leitung von Dipl.-Ing. Rudolf Köller, werden täglich IT-Services für rund 3.500 User angeboten. Dabei zählen neben dem Amt der Kärntner Landesregierung selbst, auch Bezirkshauptmannschaften, Agrarbezirksbehörden und Vereine der öffentlichen Verwaltung zum Kundenkreis. Bereits seit 2005 beschäftigt sich Harald Kiko (Leitung Netz und Unix) in der EDV-Abteilung der Kärntner Landesregierung mit dem Thema Informationsrisikomanagement. Seither führte er viele Kundenbefragungen sowie Risikoanalysen durch und verwaltete die Ergebnisse mithilfe eines selbst erstellten Excel-Sheets. Ein Tool zur Unterstützung dieser Aufgaben, welches auch mit dem bisher verfolgten eigenen Gedankenmodell stimmig sein sollte, war bis dato nicht gefunden.

Ende 2010 präsentierte Dr. Stallinger der Kärntner Landesregierung das Tool CRISAM®. Die hinter der Software liegende Idee gefiel sofort und auch das Tool selbst vermittelte einen übersichtlichen und handhabbaren Eindruck. Man entschloss sich daher mit einem Prototyp-Projekt zu starten. Im Rahmen von 10 Projekttagen wurde die Strafabteilung der BH Villach bezüglich der, von ihr eingesetzten IT Services und deren Auswirkungen auf die Geschäftsabläufe bei nicht erfüllter Verfügbarkeits-, Vertraulichkeits- und Integritätsanforderungen betrachtet. Dazu modellierten Harald Kiko und Ing. Mag.ª Christina Haas in CRISAM® ein umfangreiches IT-Infrastrukturmodell zu den betrachteten IT-Services und befragten Applikations-, System- und Fachbereichsverantwortliche zu Sicherheitsaspekten der eingesetzten Systeme.

Die Abweichungen zwischen dem gesetzten Rating-Ziel und dem tatsächlichen Ist-Stand zeigte keine unerwarteten Überraschungen. Aber die Begeisterung war doch groß – endlich lag nachvollziehbar und gut pflegbar ein Ergebnis vor, dass sich einfach in handhabbare Maßnahmenpakete zur Problembeseitigung herunterbrechen lässt. Das Pilotprojekt war ein voller Erfolg und der Ausbau des Einsatzbereichs von CRISAM® in der Kärntner Landesregierung ist bereits für die Zukunft geplant.



„Die IT-Abteilung des Landes Kärnten ist seit 2005 nach ISO 27000 zertifiziert. Konsequentes Risikomanagement ist dabei ein unverzichtbares Kernelement. Mit CRISAM® realisieren wir eine valide und transparente Entscheidungsgrundlage, um die wirksamsten Maßnahmen zur Verbesserung der IT-Sicherheit des Landes Kärnten setzen zu können.“

Dipl.-Ing. Rudolf Köller, Leiter IT, Amt der Kärntner Landesregierung



# logbuch

## 05

### DIG Einkäufer-Forum 2011

DIG digital-information-gateway GmbH lud zum DIG Einkäufer-Forum am 10.05.2011 nach Steyregg, Nahe Linz. Beim DIG Einkäufer-Forum trafen sich über 100 Entscheidungsträger, Spezialisten und Anwender aus dem Bereich der elektronischen Beschaffung und partizipierten von Erfahrungen der Einkaufsexperten in den wichtigsten Unternehmen Österreichs. Dr. Manfred Stallingner war ebenfalls mit einem interessanten Vortrag zum Thema Risikomanagement im Einkauf vertreten.

### Information-Security-Symposium 2011

Die Zertifizierungsorganisationen CIS und Quality Austria luden am 11.05.2011 zum 7. Information-Security-Symposium in den Kursalon Wien. Der hochkarätige Branchen-Treff für jährlich mehr als 250 Teilnehmer bietet mit praxisnahen Vorträgen sowie etablierten Lösungsanbietern und Beratern Erfahrungsaustausch rund um Informationssicherheit nach ISO 27001, IT Service Management nach ISO 20000 und Integrierte Managementsysteme. Auch die calpana business consulting gmbh war wieder mit einem CRISAM® Info-Cube präsent.



Fotodienst, Anna Rauchenberger

### CRISAM® Frühlings-Academy 2011

Vom 25.05.2011 bis 26.05.2011 hat bei der calpana business consulting gmbh in Linz die CRISAM® Frühlings-Academy stattgefunden. Angeboten wurden 2 intensive Schulungstage zu den CRISAM® Themen: Modellierung, Service Level Management, Update 4.2, Notfallplanung, Key Performance Indicators, Kataloge und Reporting.

**Bitte gleich vormerken: im Herbst 2011 findet die nächste CRISAM® Academy statt!**