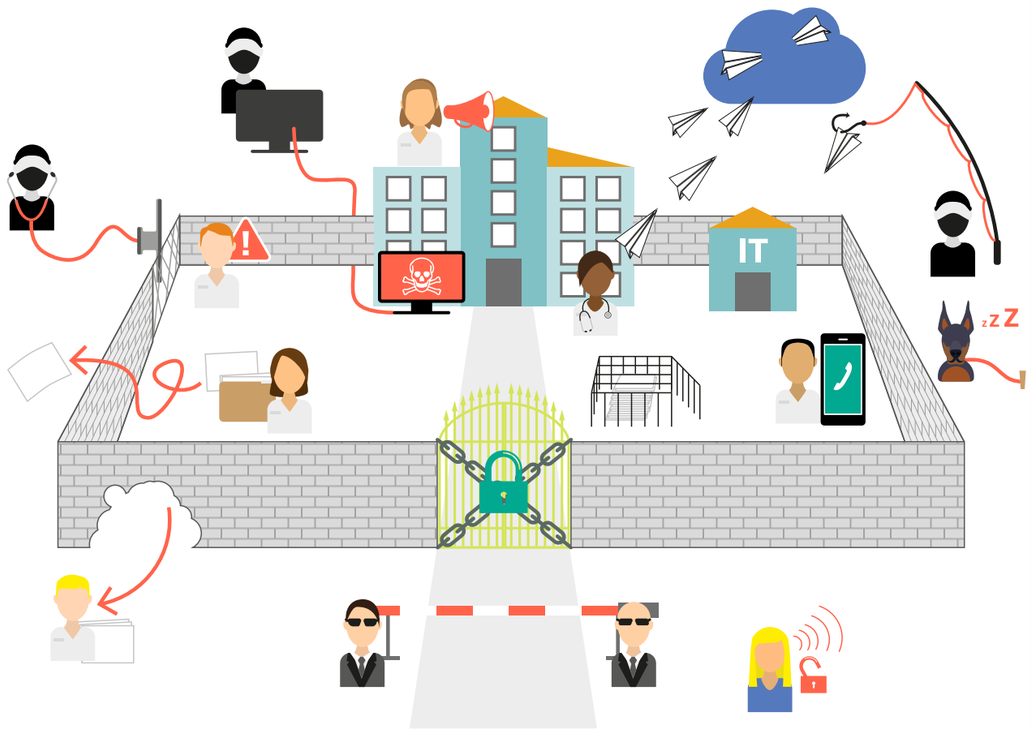
Rödl & Partner

KRITIS 2023

EFFIZIENTE VORBEREITUNG AUF DIE NÄCHSTE RUNDE

Lassen Sie uns gemeinsam dafür sorgen,
dass digitale Lösungen für die
Krankenversorgung verfügbar bleiben ...



... und man nicht durch Lücken in der Sicherheit
in analoge Notfalllösungen verfällt.

Mind the Gap

Sehr geehrte Damen und Herren,

auch wenn „MIND THE GAP“ sich ursprünglich eigentlich als Warnhinweis beim Einstieg in U-Bahnen in London versteht, so ist dies mit der deutschen Übersetzung „Achten Sie auf die Lücke“ genauso gut als Warnmeldung für Betreiber kritischer Infrastrukturen geeignet.

Lücke, Bedrohung, Schwachstellen: All diese Begriffe haben im Bereich der Informationssicherheit eine große Bedeutung, denn das Ausnutzen ebendieser kann für den KRITIS-Betreiber sehr schmerzlich werden.

Dabei sind Lücken in der Umsetzung des Stands der Technik hinsichtlich Informationssicherheit im Sinne der KRITIS-Verordnung zunächst einmal Mängel, welche je nach Schweregrad bedeutend über geringfügig sein können.

Besonders schlimm ist eine Sicherheitslücke aber, wenn sie ein System betrifft, welches zur Absicherung dient. Man liest immer wieder von bestehenden Schwachstellen in IT-Systemen, die durch ein geregeltes Patchmanagement behoben werden müssen.

Wie ist mit organisatorischen Lücken umzugehen? Mit technischen Schutzmaßnahmen kann man sich nur bis zu einem bestimmten Grad absichern, am Ende kommt es auf jede einzelne Mitarbeiterin oder jeden Mitarbeiter an. Auch wenn das Haupttor stark abgesichert sein mag, so gibt es daneben häufig unterschiedlichste Wege dieses zu umgehen, um Informationen zu erhalten.

Wir wollen Sie nicht nur bei der Erbringung der Nachweispflicht gegenüber dem BSI unterstützen, sondern auch dabei helfen, die gefährlichen Lücken zu schließen. Wir sind selbst als Beauftragte zur Informationssicherheit bei kritischen Infrastrukturen bestellt und kennen die Probleme somit aus eigener Erfahrung.

Als Prüfer im Rahmen des Nachweisverfahrens ist es uns deshalb besonders wichtig, zielgerichtete und umsetzbare Vorschläge zu unterbreiten, die Ihnen in Ihrem Alltag helfen.

Nachdem das BSI einen Wechsel des Prüfungsleiters nach zwei Prüfungen vorschreibt und dieser auch nicht mehr Teil des Prüfungsteams sein darf, wollen wir diese Chance des bei Ihnen ggf. anstehenden Prüferwechsels nutzen und Ihnen unsere Experten aus dem Team Assurance & IT aus dem Bereich Gesundheitswirtschaft bei Rödl & Partner vorstellen.

Ihr Jürgen Schwestka

Vorbereitung auf die Prüfung

Nachdem in den Jahren 2019 und 2021 für die meisten Betreiber kritischer Infrastrukturen im Bereich des Gesundheitswesen die ersten Nachweisverfahren gemäß § 8a BSIG stattfanden, steht im Jahr 2023 die dritte Runde an. Es wurden somit schon einige Erfahrungen gesammelt, manche gut, manche vielleicht weniger befriedigend. Das BSI sieht nach zwei nachfolgenden durch ein Prüfteam durchgeführten Prüfungen einen Prüferwechsel vor. Wir möchten die Gelenheit nutzen uns Ihnen als Partner auf Augenhöhe für Ihr kommendes Nachweisverfahren vorzustellen und Ihnen Impulse für die Vorbereitungen mitzugeben.

Bei den durchgeführten Prüfungen dürften einige Mängel gefunden und Maßnahmen zur Abstellung der Mängel erarbeitet worden sein, sind vom BSI doch einige konkrete Anforderungen erhoben worden, die in den meisten Krankenhäusern und Kliniken noch nicht ausreichend strukturiert umgesetzt waren. Die Umsetzung der Anforderungen ist je nach Ausgangssituation häufig mit aufwendigen IT-Projekten verbunden, welche sehr viele IT-Ressourcen binden. Die Zeit für die Umsetzung schwindet zusätzlich, nachdem etwaige Förderbescheide erst mit mehreren Monaten Verzögerung bewilligt wurden.

Während des Tages- und Projektgeschäftes ist es dennoch wichtig, sich auf das nächste Nachweisverfahren gegenüber dem BSI vorzubereiten, denn erfahrungsgemäß steigen die Erwartungen beim BSI und somit auch bei den Prüfern. Nicht zuletzt ist auch die Gültigkeit des B3S nach zwei Jahren erloschen, sodass neue Anforderungen zu erwarten sind. Im Rahmen des Nachweisverfahrens im Jahre 2021 wurden durch das BSI bereits weitläufig im Nachgang der Nachweiserbringung weitere Informationen über den Fortschritt der Mängelbehebung eingefordert. Bei einem ausbleibenden Fortschritt drohen weitere aufwendige Nachforderungen seitens des BSI oder eine Sonderprüfung vor Ort. Dies gilt es durch eine gute Prüfungsvorbereitung und eine qualitativ hochwertige Prüfung samt Erstellung von Nachweisunterlagen bestmöglich zu vermeiden.

Unabhängig der von Ihnen geplanten Prüfungsgrundlage (B3S, ISO 27001, IT-Grundschutz, BSI-Prüfkatalog o.ä.) empfiehlt es sich im Vorfeld der Prüfung eine grundsätzliche Beschreibung der Umsetzung der KRITIS-Anforderungen zu erstellen bzw. diese zu aktualisieren. Eine solche Dokumentation hilft den Überblick zu behalten und ist somit für den ISMS-Verantwortlichen genauso nützlich wie für die Prüfung selbst. In der aktuellen Version 1.1 des B3S der Medizinischen Versorgung ist eine solche Beschreibung der Umsetzung mit Anforderung ANF-RM28 sogar explizit gefordert. In gleichem Maße gilt es, die bereits festgestellten Mängel aus vorherigen Audits zu berücksichtigen und den Umsetzungsstand zu überwachen.

Geltungsbereich

In Anbetracht des dynamischen Umfelds der Gesundheitsbranche ist für die nächste KRITIS-Prüfung insbesondere zu prüfen, ob der festgelegte Geltungsbereich weiterhin zutreffend ist oder ggf. Gebäude, Bereiche, Stationen und Anwendungen hinzugekommen oder weggefallen sind. Der Geltungsbereich stellt die Grundlage für die Umsetzung von Maßnahmen und somit auch der Prüfung dar und ist im Zuge der Nachweiserbringung in Form eines Dokuments zu beschreiben und grafisch darzustellen (Anlage PD.A). Auskunftsgemäß gab es hier seitens des BSI besonders viele Nachfragen.

Zentrale Fragestellungen für die optimale Prüfungsvorbereitung:

Wie kann der Prozess der Nachweiserbringung an das BSI effizient gestaltet werden?

Sind Fortschritte bei der Umsetzung von Maßnahmen erkennbar?

Welcher Prüfer ist der Richtige und woran ist das festzumachen?

Welche Anforderungen sollte man als KRITIS-Betreiber stellen und wie überprüft man bereits vorher die Qualität der Prüfung?

Das BSI stellt generelle Anforderungen an die prüfenden Stellen, die es auch nachzuweisen gilt:

- Grundsätzliche Kompetenz über das IT-Sicherheitsgesetz und die Nachweiserbringung, die vom BSI „zusätzliche Prüfverfahrenskompetenz für §8a BSIG“ genannt wird
- Expertise in den Bereichen Audit/Prüfung, IT-Sicherheit und der entsprechenden Branche
- Während die Audit- und IT-Sicherheitserfahrung geringe Hürden darstellen und sich durch anerkannte Zertifizierungen wie CISA, IT-Sicherheitsbeauftragte, ISO 27001 Auditor u.v.m. leicht nachweisen lassen können, ist eine Branchenerfahrung meist schwerer nachweisbar und am Markt nicht ausreichend verfügbar

Tipps für den Nachweis der Branchenerfahrung:

- Lassen Sie sich Referenzkunden nennen
- Fragen Sie nach Empfehlungsschreiben von Kunden der entsprechenden Branche mit vergleichbaren Aufgabenstellungen
- Lassen Sie sich das Prüfungsvorgehen im Vorfeld ausführlich erläutern, um sicherzustellen, dass die Erwartungen und die Zeitplanung mit den eigenen Vorstellungen konform gehen, so schaffen Sie eine konstruktive und für alle Parteien angenehme Prüfungssituation

Rödl & Partner als prüfende Stelle

Was macht uns als prüfende Stelle und Prüfer aus? Als Wirtschaftsprüfungsgesellschaft haben wir einen sehr hohen Qualitätsanspruch an unsere prüferische Tätigkeit, ebenso wie Sie an Ihre Informationssicherheit als Betreiber kritischer Infrastruktur im Umgang mit hochsensiblen und schützenswerten Informationen. Aus diesem Grund setzen wir ausschließlich hochqualifizierte Mitarbeiter ein. Für die Prüfung der Umsetzung der Anforderungen des BSI kommen Spezialisten aus unserem Team Assurance & IT im Geschäftsbereich Gesundheits- und Sozialwirtschaft zum Einsatz.

Als Team Assurance & IT in der Gesundheits- und Sozialwirtschaft sind uns die KRITIS-Prüfungen quasi auf den Leib geschneidert, da jedes Teammitglied und somit jeder Kopf des Prüfungsteams alle vom BSI geforderten Kompetenzen mitbringt, statt diese siloartig auf mehrere Köpfe zu verteilen. Dies ermöglicht uns einen noch tieferen Austausch der typischen Problem- und Fragestellungen im Bereich Informationssicherheit der Gesundheitswirtschaft untereinander, von dem unsere Mandanten profitieren.

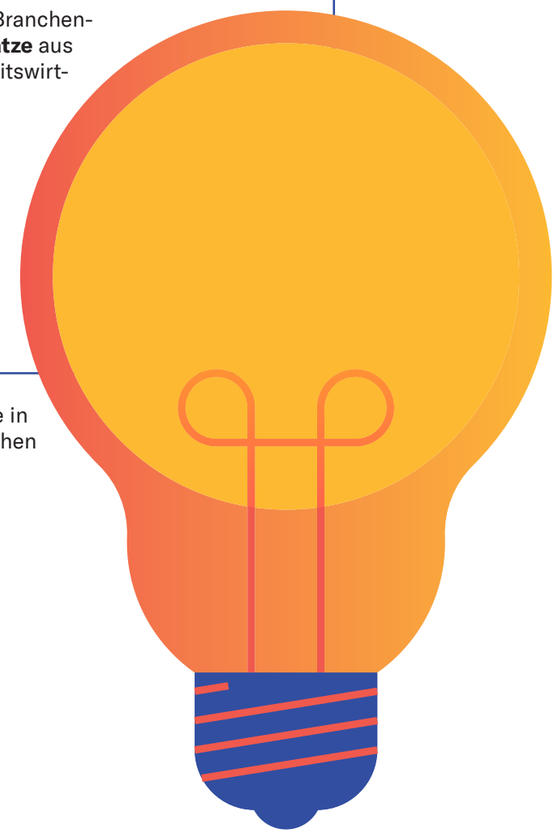
Wir sehen uns als den agilen Kümmerer, der sich vollumfänglich und zentral koordinierend um die Belange des Mandanten kümmert. Aus diesem Selbstverständnis heraus ist es uns besonders wichtig, dass unsere Mandanten bereits vor einer möglichen Beauftragung wissen, mit wem sie es zu tun haben und den zentralen Ansprechpartner, also den Prüfungsleiter sowie das Prüfungsteam bereits kennen. Bei der Auswahl der Prüfungsteams setzen wir zudem auf personelle Kontinuität. Diese Maßnahmen stellen eine effiziente Prüfung und Kommunikation sicher und geben unseren Mandanten die Sicherheit, ein passendes und hochqualifiziertes Team auf Augenhöhe an ihrer Seite zu haben.

Wie sieht unser Prüfungsvorgehen aus? Als zertifizierte IT-Auditoren (z.B. CISA, TÜV IT-Security-Auditor, ISO 27001 Lead Auditor, IDW IT-Auditor, DIIR Interner Revisor etc.) sind uns unterschiedliche Best Practice Prüfungsmethoden und -vorgehen bekannt. Dabei legen wir stets sehr viel Wert auf ein methodisches und gut vorbereitetes Vorgehen. Dies beinhaltet eine detaillierte Prüfungsplanung mit entsprechender Vor-Ort Prüfung und vordefinierten Fristen für die Bereitstellung der Nachweisformulare und des Prüfungsberichts.

Ihr Mehrwert durch die Prüfung mit unseren IT-Sicherheitsexperten für die Gesundheitswirtschaft

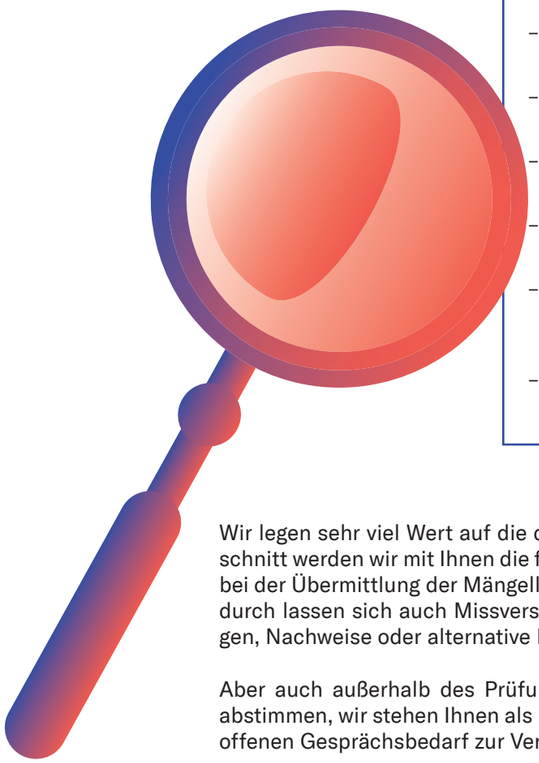
- ✓ In unserer Rolle als Prüfer, Implementierungsberater aber auch **externer Informationssicherheitsbeauftragter** haben wir Einblick in unterschiedlichste Einrichtungen der Gesundheitswirtschaft
- ✓ Wir sind Ihr Begleiter mit kritischer Grundhaltung für die **Identifikation der richtigen Maßnahmen** zur Schaffung von Informationssicherheit in Ihrem Betrieb
- ✓ Unsere Empfehlungen im Rahmen der **Prüfungsfeststellung** besprechen wir mit Ihnen auf Augenhöhe und es ist uns wichtig, dass Sie sich darin wiedererkennen
- ✓ Mit **objektivem Blick** stellen wir Ihre Maßnahmen auf den Prüfstand, berücksichtigen dabei bereits initiierte sowie geplante Maßnahmen
- ✓ Wir geben Ihnen **Impulse** für die Umsetzung bei festgestellten Lücken in Prozessen und technischer Ausgestaltung
- ✓ Profitieren Sie von unserer **Branchenexpertise**
- ✓ Mit der Bündelung aus IT-Sicherheits- und Branchenwissen können wir Ihnen **erfolgreiche Ansätze** aus vergleichbaren Einrichtungen der Gesundheitswirtschaft liefern
- ✓ Wir können beurteilen, welche Maßnahmen nicht nur angemessen sondern gleichzeitig auch **pragmatisch** umsetzbar sind
- ✓ Wir berücksichtigen bei den Maßnahmenempfehlungen die **wichtigen Bedarfe** für den Krankenhausbetrieb

Haben Sie noch Fragen? Gerne überzeugen wir Sie in einem persönlichen Gespräch von unserem Vorgehen und unserer Expertise.



Prüfungsablauf mit Rödl & Partner

Für die Durchführung einer Prüfung gemäß § 8a BSIG legen wir ein geordnetes Projektmanagement zugrunde. Ausgehend von dem geplanten Projektende planen wir die einzelnen Schritte und Meilensteine rückwärts, damit sichergestellt wird, dass alle Fristen eingehalten werden. Hierfür planen wir folgende Rahmenbedingungen:



- Frühzeitiger Auftakttermin für die Prüfung, idealerweise mindestens 3-4 Monate vor der Prüfung
- Prüfungsphase 1 mit Dokumentenprüfung und Prüfung des Geltungsbereichs ca. 1 Monat vor der eigentlichen Prüfung
- Prüfungsphase 2 als Vor-Ort-Prüfung mit Interviews und Ortsbegehungen
- Enge Abstimmung der Mängelliste und 1-2 Wochen Zeit für Sie zur Planung der Maßnahmen (Umsetzungsplan)
- Die einzureichenden Unterlagen stehen 1-3 Arbeitstage nach Erhalt des Umsetzungsplans auf Basis der Mängelliste zur Verfügung.
- Der Bericht zur Prüfung ist spätestens 14 Tage nach Übermittlung der einzureichenden Unterlagen fertiggestellt.

Wir legen sehr viel Wert auf die direkte Kommunikation. Nach jedem Prüfungsabschnitt werden wir mit Ihnen die festgestellten Ergebnisse besprechen, so dass Sie bei der Übermittlung der Mängelliste keine bösen Überraschungen erwarten. Hierdurch lassen sich auch Missverständnisse verhindern oder ggf. fehlende Unterlagen, Nachweise oder alternative Kontrollen nachreichen.

Aber auch außerhalb des Prüfungszeitraums können Sie sich jederzeit mit uns abstimmen, wir stehen Ihnen als persönlicher Ansprechpartner für alle Fragen und offenen Gesprächsbedarf zur Verfügung.

Profitieren Sie in Ihrer Prüfungssituation von:

- ✓ Einem agilen Kümmerer, der alle Belange vollumfänglich und zentral koordiniert betreut
- ✓ Einer vorherigen Vorstellung des Prüfungsleiters und des kontinuierlichen Prüfungsteams – auch über mehrere KRITIS-Themen hinweg
- ✓ Dem Vorliegen aller notwendigen Qualifikationen, Zusatzausbildungen und Zertifizierungen
- ✓ Einer detaillierten Prüfungsplanung mit entsprechender Vor-Ort-Prüfung und vordefinierten Fristen für die Bereitstellung aller notwendigen Unterlagen und des Prüfungsberichtes
- ✓ Einer bewährten zweistufigen Prüfung analog der ISO 27001 Zertifizierung Stufe 1: Sichtung der zentralen Dokumente der Prüfung(en) des/der Vorjahr(e), Betrachtung der Basis und Umsetzung der Maßnahmen Stufe 2: Vor-Ort-Prüfung mit Ihrem Ansprechpartner und mindestens einem weiteren Prüfer
- ✓ Einer qualitativ hochwertigen und gleichzeitig effizienten Prüfung
- ✓ Möglichst vergleichbaren Ergebnissen, gleichbleibenden Begrifflichkeiten und Mängelkategorien
- ✓ Einer risikoorientierten, pragmatischen Herangehensweise
- ✓ Enge Orientierung an den Vorgaben des BSI

Durch die Vielzahl durchgeführter KRITIS-Audits haben wir mit jeglichen Prüfungsgrundlagen bereits gute Erfahrungen machen können. Dies beinhaltet insbesondere die vorhandenen B3S in der Gesundheitsbranche, die Orientierungshilfe zu Nachweisen vom BSI sowie BSI-Grundschutz und ISO 27001. Weiterhin ist der veröffentlichte Anforderungskatalog „Konkretisierung der Anforderungen an die gemäß §8a BSIG Absatz 1 BSIG umzusetzenden Maßnahmen“ vom BSI in Zusammenarbeit mit dem Institut der Wirtschaftsprüfer (IDW) als Prüfungsgrundlage grundsätzlich in Betracht zu ziehen. Darauf aufbauend hat das IDW in Zusammenarbeit mit dem BSI eine Prüfungshilfe (IDW PH 860.2) mit konkreten Prüfungshandlungen veröffentlicht. Als Wirtschaftsprüfungsgesellschaft profitieren wir von dieser engen Vernetzung mit dem BSI und begrüßen dieses einfache und nachvollziehbare Konzept zur Nachweiserbringung für Sie als Betreiber kritischer Infrastruktur.

Unsere Experten im Überblick

Nichts ist so beständig wie der Wandel. Dies gilt insbesondere für die Entwicklungen in der Informationsverarbeitung. Unsere Kolleginnen und Kollegen durchlaufen regelmäßig Schulungen, um sich mit den aktuellen Themen und Fragestellungen auseinanderzusetzen.

Um die für eine Prüfung gemäß § 8a BSIG erforderlichen Kompetenzen nachweisen zu können, haben all unsere Kolleginnen und Kollegen persönliche Zertifizierungen erworben. Wir sind sehr stolz auf unsere fachlich hohe Expertise in Verbindung mit unserem Fingerspitzengefühl für Prüfungssituationen. Gerne weisen wir Ihnen und dem BSI unsere Kompetenzen nach.

Die folgende Aufzählung zeigt die im Team vorhandenen Zertifizierungen.

- Certified Information Security Officer (CISO DGI®)
- Certified Information Systems Auditor [CISA]
- CISIS12 Information Security Officer
- Datenschutzauditor DSA-TÜV
- Interner Revisor DIIR
- IT-Compliance Manager (TÜV)
- IT-Security-Manager (TÜV)
- PECB Certified ISO/IEC 27001 Lead Auditor
- CISIS12 (Information Security Berater)
- Compliance Officer (TÜV)
- Datenschutz-beauftragter DSB-TÜV
- IT-Auditor IDW
- IT-Security-Beauf-tragter (TÜV)
- IT-Security-Auditor (TÜV)
- Prüfer für Interne Revisionssysteme DIIR
- Prüfer nach §8a BSIG

Rödl & Partner – Experten für die Gesundheits- und Sozialwirtschaft

Die Erfolgsgeschichte von Rödl & Partner begann 1977 als Ein-Mann-Unternehmen in Nürnberg. Gründer Dr. Bernd Rödl gehörte zu den ersten Rechtsanwälten in Bayern, die sich als Steuerberater und Wirtschaftsprüfer qualifizierten. Von Anfang an setzte Rödl & Partner so auf eine fachübergreifende, multidisziplinäre Beratung.

Mittlerweile hat Rödl & Partner weltweit 5.260 Mitarbeiterinnen und Mitarbeiter in 50 Ländern mit 107 eigenen Niederlassungen.

Vor fast 30 Jahren wurde der Unternehmensbereich PMC mit dem Fokus auf Non-Profit-Gesellschaften gegründet, da sich der Bereich deutlich von klassischen Industrieunternehmen unterscheidet. Dazu gehört auch die Betreuung der Gesundheits- und Sozialwirtschaft.

Alles aus einer Hand: Rechtsberatung, Steuerberatung, Unternehmens- und IT-Beratung, Wirtschaftsprüfung

Etwa 100 Kolleginnen und Kollegen beschäftigen sich ausschließlich mit den aktuellen Entwicklungen und Anforderungen innerhalb der Gesundheits- und Sozialwirtschaft.

Hierzu zählen wir insbesondere die folgenden Branchen, die wir gemeinsam mit allen Berufsgruppen bedienen. Dabei gibt es kein Kostenstellendenken – so werden Sie immer vom besten Experten für Ihre konkrete Fragestellung unterstützt. Unsere Kolleginnen und Kollegen haben langjährige Erfahrungen in dem Bereich.

Krankenhäuser

Labore

Pflegeheime

Forschungseinrichtungen

Hochschulen

Wir unterstützen Sie vollumfänglich und interdisziplinär:

Wirtschaftsprüfung:

- Gesetzliche und freiwillige Jahresabschlussprüfung
- Krankenhausspezifische Prüfungen nach KHEntgG
- Sonderprüfungen
- IT-Audits und Datenmigrationsprüfungen
- Digitalisierte Abschlussprüfung

Steuerberatung:

- Erstellung der laufenden Finanz- und Lohnbuchhaltung
- Jahresabschlusserstellung
- Tax Compliance Management Systeme

Rechtsberatung:

- Krankenhausrecht und Recht der Krankenhausfinanzierung
- Vertragsrecht
- Health-Care-Compliance
- Datenschutzrecht
- EU-Beihilferecht

Betriebswirtschaftliche Beratung:

- Plausibilisierung von Wirtschafts- und Liquiditätsplanungen
- Implementierung bzw. Ausbau der Kostenrechnung sowie eines adäquaten betriebswirtschaftlichen Controllings
- Erstellung von Mehrjahresplanungen

Assurance & IT:

- Prüfungen nach §8a BSIG („KRITIS“)
- Beratung zu §75c SGB V
- Tätigkeit als externer Informationssicherheitsbeauftragter
- Beratung bei der Implementierung von Informationssicherheits- und Risikomanagementsystemen auf Basis BSI-Grundschutz und ISO 2700x
- Durchführung von Audits und Revisionsprüfungen in den Bereichen IT-Security und Datenschutz
- Prüfung von Internen Kontrollsystemen
- Beratung zur Optimierung von IT-gestützten Geschäftsprozessen
- Unterstützung bei der Softwareauswahl
- Prüfung der Revisionssicherheit von elektronischen Archiven

Medizinökonomie:

- Erlössicherung durch Analyse der Struktur-, Prozess- und Ergebnisqualität
- Wir schließen die Brücke zwischen Medizin und Ökonomie und analysieren sowohl die klinischen als auch ökonomischen Stärken und Schwächen von Krankenhäusern.

Glauben Sie nicht uns...

ANregiomed

ANregiomed · Postfach 613 · 91511 Ansbach

Rödl & Partner GmbH
Äußere Sulzbacher Str. 100
90491 Nürnberg

DLZ INFORMATIONTECHNIK
Lars Forchheim
CIO
Telefon 0981/484-32749
Fax 0981/484-2765
E-Mail lars.forchheim@anregiomed.de

IHR ZEICHEN:	IHRE NACHRICHT VOM:	UNSER ZEICHEN:	DATUM
		lf	15.02.2022

Empfehlungsschreiben für die Rödl & Partner GmbH

Sehr geehrter Herr Schwestka,

im ersten Halbjahr 2021 haben Sie uns, ANregiomed gemeinsames Kommunalunternehmen, Anstalt des öffentlichen Rechts des Landkreises Ansbach und der Stadt Ansbach, bei der Erstellung des Prüfnachweises gemäß § 8a BSIG auf Basis des Branchenspezifischen Sicherheitsstandards „Medizinische Versorgung" als Prüfende Stelle unterstützt. Für die sehr gute gemeinsame Zusammenarbeit möchten wir Ihnen danken und mit diesem Empfehlungsschreiben unsere vollste Zufriedenheit ausdrücken.

Im Rahmen unserer Zusammenarbeit haben wir Sie als stets zuverlässige, kompetente und fachkundige Personen kennengelernt. Besonders hervorheben möchten wir die sehr angenehme und konstruktive Kommunikation im Projektverlauf sowie Ihre freundliche Art und Hilfsbereitschaft bei Unklarheiten und Fragestellungen.

Weiterhin empfanden wir Ihre kritische Grundhaltung bei gleichzeitig praxisorientierter Bewertung der Umsetzung unserer organisatorischen und technischen Maßnahmen zur Vermeidung von Störungen der Integrität, Vertraulichkeit, Verfügbarkeit und Authentizität sowie Behandlungseffektivität und Patientensicherheit in unserm Kontext als sehr angenehm und zielführend.

Wir halten Sie als Prüfende Stelle für die Erbringung der Nachweise gemäß § 8a BSIG für sehr qualifiziert und möchte Sie potenziellen Auftraggebern ohne jeden Vorbehalt als Dienstleister weiterempfehlen.

Mit freundlichen Grüßen
ANregiomed gKU
i. A.

CIO Dienstleistungszentrum Informationstechnik

... vertrauen Sie auf Bewertungen aus der Branche

Universitätsklinikum Erlangen

Medizinisches Zentrum für Informations- und Kommunikationstechnik
CIO: Prof. Dr. Hans-Ulrich Prokosch
Geschäftsführer: Martin Schneider
www.mik.uk-erlangen.de

Organisation und QM
Lorenz Feldberger
Telefon: 09131 85- 46367
Fax: 09131 85-36799
E-Mail: lorenz.feldberger@uk-erlangen.de
Krankenhausstraße 12, 91054 Erlangen

Öffentliche Verkehrsmittel:
Buslinie 290
Haltestelle Maximiliansplatz/Kliniken

Uni-Klinikum Erlangen Medizinisches IK-Zentrum 91012 Erlangen

Rödl & Partner GmbH
Äußere Sulzbacher Straße 100
90491 Nürnberg

17. Juli 2020

Empfehlungsschreiben für Rödl & Partner GmbH

Sehr geehrter Herr Schwestka,

im Juni 2019 haben Sie uns bei der Erstellung des Prüfnachweises nach §8a BSIG auf Basis des B3S „Medizinische Versorgung" als Prüfende Stelle unterstützt (Kritis-Prüfung). Sie haben die übertragene Aufgabe mit großer Sorgfalt und zu meiner vollsten Zufriedenheit erledigt. Dafür möchte ich mich nochmals bei Ihnen bedanken!

Ich habe Sie während unserer Zusammenarbeit als äußerst zuverlässige, kompetente und engagierte Person kennengelernt und dafür geschätzt. Besonders positiv fand ich die kritische Grundeinstellung bei gleichzeitig praxisnaher Abschätzung der Auswirkungen von möglichen Abweichungen und dem damit verbundenen Schweregrad der Mängel.

Aus diesen Gründen halte ich Sie für Projekte in dem Bereich der Prüfung nach §8a BSIG für sehr qualifiziert und möchte Sie potenziellen Auftraggebern ohne jede Vorbehalte als Dienstleister empfehlen.

Da Sie zudem im Auswahlverfahren das wirtschaftlichste Angebot abgegeben haben, freue ich mich auf die gemeinsame Kritis-Prüfung im kommenden Jahr.

Mit freundlichen Grüßen

Martin Schneider
Geschäftsführer

Ihr Ansprechpartner

JÜRGEN SCHWESTKA
IT-Security-Auditor (TÜV)
Certified Information Systems Auditor [CISA]
Zert. IT-Sicherheitsbeauftragter (ITSIBE/CISO)
IT-Auditor[IDW]
Prüfer nach § 8a BSIG
Partner

T +49 911 9193 3508
E juergen.schwestka@roedl.com

Rödl & Partner
Äußere Sulzbacher Straße 100
90491 Nürnberg

www.roedl.de/kritis