Standortbestimmung zur

Umsetzung des

branchenspezifischen Sicherheitsstandards für die Gesundheitsversorgung im Krankenhaus

(B3S)

Präambel

Der Einsatz der Informationstechnik (IT) und damit die Digitalisierung haben an zentraler Bedeutung gewonnen bzw. werden weiter an Bedeutung gewinnen, und damit auch die Einhaltung regulatorischer Maßgaben durch die IT gestützten Prozesse.

Der Bundesverband der Krankenhausträger und er Bundesrepublik Deutschland hat u.a. vor diesem Hintergrund einen branchenspezifischen Sicherheitsstandard für die Gesundheitsversorgung im Krankenhaus erarbeitet, der gemäß Feststellungsbescheid vom 22.10.2019 zur Gewährleistung der Anforderungen nach § 8a Absatz 1 BSIG geeignet ist. In einem ersten Schritt sollen sich alle Krankenhäuser und Gesundheitseinrichtungen, die als KRITIS relevant eingestuft sind, nach diesem Standard auszurichten. Der Wunsch des Verbandes und der Politik ist, dass sich alle Krankenhäuser und Gesundheitseinrichtungen nach diesem Sicherheitsstandard ausrichten.

Ihr Nutzen

Individuelle Standortbestimmung unter bestmöglichen Voraussetzungen – niemand kennt Ihr Unternehmen so gut wie Sie.

Sie können das Tool als Dokumentationsnachweis nutzen, um gegenüber Dritten aufzuzeigen, dass Sie sich mit der Thematik auseinandergesetzt haben.

Beitrag zur Vermeidung (Entlastungsbeweis nach § 831 Abs. 1 S. 2 BGB) eines so genannten Organisationsverschuldens nach § 823 BGB Abs. 1 sowie zahlreicher gesetzlichen Maßgaben des AktG, GmbHG sowie KWG.

Sie können die in Ihrem Unternehmen vorhandene Dokumentation den entsprechenden Prüffeldern zuordnen und haben diese somit „griffbereit“ bzw. können diese Dritten gegenüber als erste Nachweise anführen.

Die bestehenden Organisationsabläufe lassen sich in ein Reifegradmodell einordnen woraus sich entsprechende Handlungsbedarfe ableiten lassen.

Die vorliegende Dokumentation wird durch ein Bewertungsschema in ihrer Aussagekraft visuell dargestellt, was die Ermittlung von Aufwänden und Handlungsbedarfe vereinfacht bzw. eine direkte Übernahme der Charts in die Berichte ermöglicht.

3-Stufen-Vorgehensmodell

Aufnahme und Bewertung

Der erste Schritt ist eine IST-Aufnahme, unter Berücksichtigung der bereits etablierten Prozesse und erbrachten Arbeitsergebnisse aus den Bereichen

- Aufbau- und Ablauforganisation
- Organisation der Informationssicherheit
- Meldepflichten nach §8b Abs. 4 BSI-Gesetz
- Betriebliches Kontinuitätsmanagement
- Asset Management
- Robuste/resiliente Architektur
- Physische Sicherheit
- Personelle und organisatorische Sicherheit
- Vorfallerkennung und -behandlung
- Überprüfungen im laufenden Betrieb
- Externe Informationsversorgung und Unterstützung
- Lieferanten, Dienstleister und Dritte
- Technische Informationssicherheit
- Datenschutz

Dies erfolgt unter zur Hilfenahme des Tools. Das nachfolgende Schaubild verdeutlicht dies anhand des Beispiels „Organisation der IS“ und zeigt den jeweiligen Erfüllungsgrad der Anforderungen, die jeweils zugeordneten Kontrollen, den Grad der Bewertung der existierenden Dokumentation und Umsetzung sowie einen Aufwand in PT (Personentage) je Arbeitspaket zur möglicherweise notwendigen Anpassung an die bisherige Umsetzung und Dokumentation.

Fertigstellungsgrad (0 = min. / 100 = max : 65,00
Gesättter Aufwand zur Behebung in PT : %
Vervollständigt : 100%

Zurück zu "Tabellarische Ergebnisse"

Chapter des Standards	Headline	A.6.1 Interne Organisation Ziel: Festlegung eines Frameworks für die Leitung, mit dem die Implementierung der Informationssicherheit in der Organisation eingeleitet und kontrolliert werden kann.	Umgesetzt & Dokumentiert durch	Erfüllungsgrad E	GN	EN	NE	Begründung	Geschätzter Behebungsaufw. in PT
A 6.1.1	Aufgaben und Zuständigkeiten im Bereich der Informationssicherhei	Alle Zuständigkeiten im Bereich der Informationssicherheit müssen festgelegt und zugeordnet werden.			1				1
A 6.1.2	Kontakt zu Behörden	Es sind angemessene Kontakte zu relevanten Behörden zu pflegen.			1				2
A 6.1.3	Kontakt mit Interessen-	Es sind angemessene Kontakte zu Interessenvertretungen oder sonstigen sicherheitsorientierten Expertenforen und Fachverbänden zu pflegen.			1				3
A 6.1.4	Informationssicherheit im	Die Informationssicherheit muss ungeachtet der Art des Projekts auch im Projektmanagement berücksichtigt werden.			1				4
A 6.1.5	Aufgabentrennung	Miteinander in Konflikt stehende Aufgaben und Zuständigkeitsbereiche müssen getrennt werden, um das Risiko unautorisierter oder versehentlicher Änderung oder missbräuchlicher Anwendung der Werte der Organisation zu verringern.				1			5

Aufbereitung der Ergebnisse

Die in Bezug auf die einzelnen Anforderungen erhobenen Daten sind durch das schematische Vorgehen bei der Erhebung mit einem Auswertungsalgorithmus versehen, welcher einen ganzheitlichen oder aber einen in Teilabschnitten untergliederten Überblick über den jeweiligen Status Quo gibt, so dieser genutzt wurde.

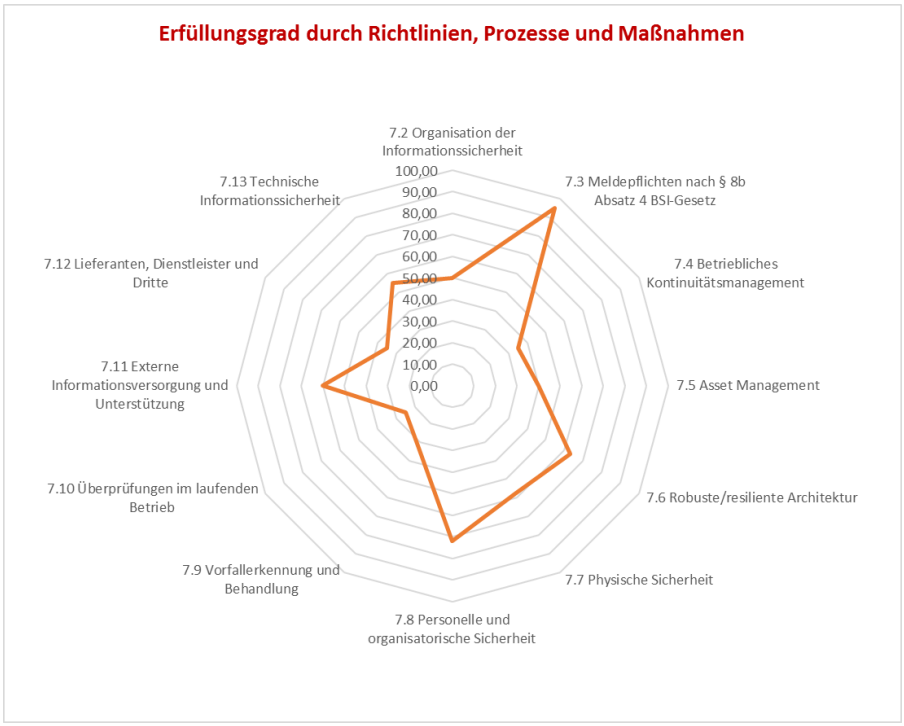
Tabellarische Darstellung der Bewertungsergebnisse 12 Control Section, 32 Control Objectives, 198 Controls	51,66	2 PT 12 PT 32 PT 379,00	Durchschnitt je Control Durchschnitt je Objective Durchschnitt je Section Insgesamt
Bereich	**Erfüllungsgrad 0 min. / 100 max.**	**Aufwand zur Behebung (geschätzt)**	**Bearbeitet 0%-100%**
7.2 Organisation der Informationssicherheit	50,00	20 PT	100%
7.2.1 Geschäftsführung / Leitung	25,00	8 PT	100%
7.2.2 Beauftragter für Informationssicherheit (ISB, CISO)	75,00	7 PT	100%
7.2.3 Prozess- /Anwendungsverantwortlicher	50,00	5 PT	100%
7.3 Meldepflichten nach § 8b Absatz 4 BSI-Gesetz	95,00	5 PT	75%
7.3 Meldepflichten nach § 8b Absatz 4 BSI-Gesetz	95,00	5 PT	75%
7.4 Betriebliches Kontinuitätsmanagement	35,00	50 PT	75%
7.4 Betriebliches Kontinuitätsmanagement	35,00	50 PT	75%
7.5 Asset Management	40,00	15 PT	75%
7.5 Asset Management	40,00	15 PT	75%
7.6 Robuste/resiliente Architektur	63,00	20 PT	75%
7.6 Robuste/resiliente Architektur	63,00	20 PT	75%
7.7 Physische Sicherheit	58,00	5 PT	100%
7.7 Physische Sicherheit	58,00	5 PT	100%
7.8 Personelle und organisatorische Sicherheit	72,00	10 PT	100%
7.8 Personelle und organisatorische Sicherheit	72,00	10 PT	100%
7.9 Vorfallerkennung und Behandlung	32,00	13 PT	50%
7.9 Vorfallerkennung und Behandlung	32,00	13 PT	50%
7.10 Überprüfungen im laufenden Betrieb	25,00	15 PT	75%
7.10 Überprüfungen im laufenden Betrieb	25,00	15 PT	75%
7.11 Externe Informationsversorgung und Unterstützung	60,00	25 PT	100%
7.11 Externe Informationsversorgung und Unterstützung	60,00	25 PT	100%
7.12 Lieferanten, Dienstleister und Dritte	35,00	50 PT	25%
7.12 Lieferanten, Dienstleister und Dritte	35,00	50 PT	25%
7.13 Technische Informationssicherheit	54,89	151 PT	75%
7.13.1 Netz- und Systemmanagement (Netztrennung und Segmentierung)	25,00	5 PT	25%
7.13.2 Absicherung Fernzugriffe	25,00	10 PT	50%
7.13.3 Härtung und sichere Basiskonfiguration der Systeme und Anwendungen	25,00	5 PT	75%
7.13.4 Schutz vor Schadsoftware	50,00	7 PT	25%
7.13.5 Intrusion Detection / Prevention	75,00	6 PT	75%
7.13.6 Identitäts- und Rechtemanagement	53,00	10 PT	100%
7.13.7 Sichere Authentisierung	52,00	5 PT	100%
7.13.8 Kryptographische Absicherung (data in rest, data in motion)	41,00	3 PT	75%
7.13.9 Mobile Sicherheit, Sicherheit Mobiler Zugang und Telearbeit (ggf. „bring your own device“ BY	63,00	4 PT	75%
7.13.10 Vernetzung von Medizingeräten	75,00	6 PT	75%
7.13.11 Datensicherung, Datenwiederherstellung und Archivierung	75,00	8 PT	75%
7.13.12 Ordnungsgemäße Systemadministration	55,00	5 PT	75%
7.13.13 Patch- und Änderungsmanagement	65,00	5 PT	75%
7.13.14 Beschaffungsprozesse	40,00	10 PT	75%
7.13.15 Protokollierung	52,00	15 PT	75%
7.13.16 Umgang mit Datenträgern, Austausch von Datenträgern	58,00	20 PT	75%
7.13.17 Sicheres Löschen und Entsorgung von Datenträgern	56,00	5 PT	100%
7.13.18 Softwaretests und Freigaben	84,00	7 PT	100%
7.13.19 Datenschutz	74,00	15 PT	100%

Vorgefertigte grafische Auswertungen unterstützen die weitere Analyse sowie die Verwendung der unternehmensindividuellen und themenbereichsbezogenen Ergebnisverwendung und -beschreibung.

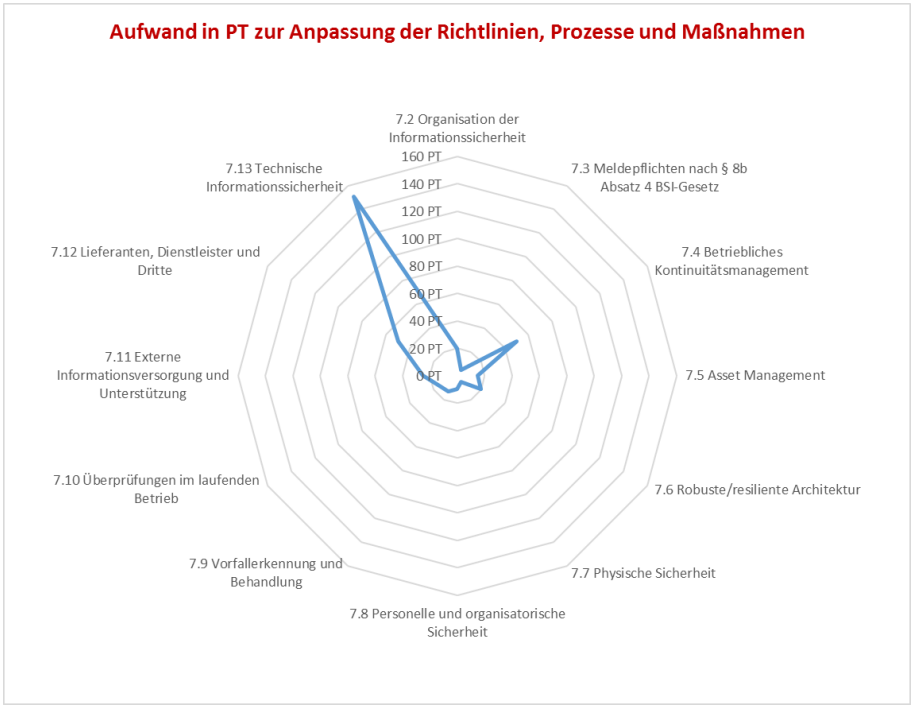
Diese sind editierbar und lassen sich den unternehmens- bzw. abteilungsindividuellen Maßgaben durch Sie anpassen.

Die nachfolgenden Darstellungen sind als beispielhaft zu verstehen und können durch die Excel eigenen Tools entsprechend angepasst werden.

Die nachfolgende Grafik gibt eine prozentuale Aussage über den Erfüllungsgrad der regulatorischen Anforderungen wieder.



Die folgende Grafik gibt Auskunft darüber, wie viel PT (Personentage) für die Bewirtschaftung der im Rahmen der Standortbestimmung identifizierten Felder geschätzt aufgebracht werden müsste, um diese Lücken in den jeweiligen Bereichen auf eine angestrebte prozentuale Abdeckung zu heben.

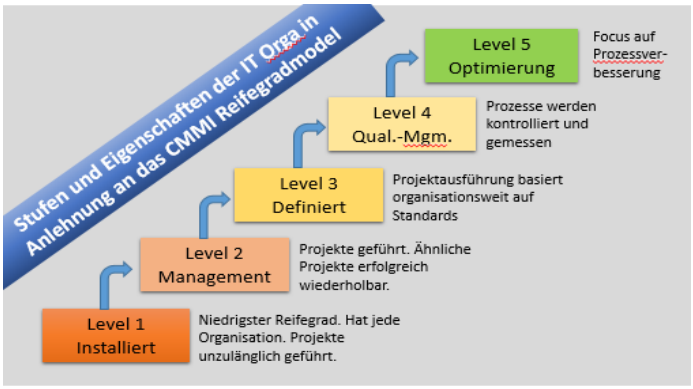


Reifegrad der Organisation

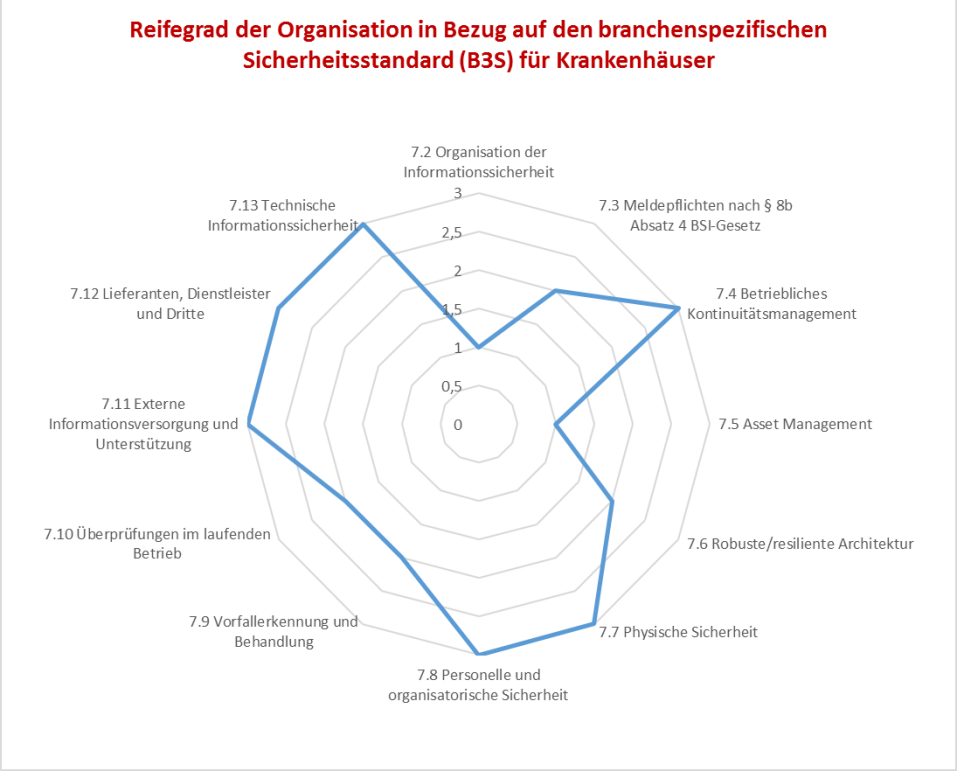
Der individuelle Reifegrad der Organisation kann anhand des bekannten und vorgegebenen CMMI Modells gemessen werden.

Ein Vergleich entsprechender Bewertungen über einen längeren Zeitraum kann eine, durch entsprechende Maßnahmen beeinflusste, Veränderung in der Organisation aufzeigen.

Die nachfolgend dargestellte Legende stellt die Stufen des Reifegradmodells dar.



Auf diese Weise lassen sich die Organisationsabläufe und damit die Organisationsbereiche einstufen und grafisch darstellen, wie die nachfolgende Grafik beispielhaft aufzeigt.



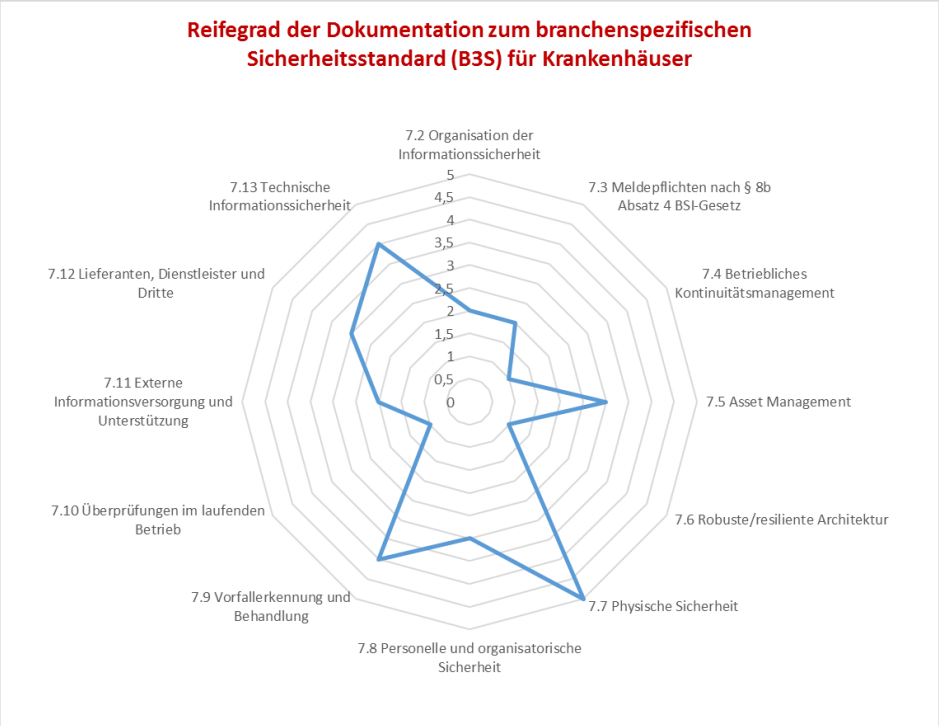
Reifegrad der Dokumentation

Der Reifegrad der Dokumentation im Unternehmen wird in 6 Stufen unterteilt. Dadurch kann ein sehr feiner Grad der Aufwandsmessung erfolgen.

Reifegrad der jeweiligen Dokumentation

Reifegrad	Bezeichnung	Beschreibung
0	Nicht vorhanden	Es liegt keine Dokumentation oder Richtlinie vor
1	Grundlagen vorhanden	Es liegen Grundlagen vor, jedoch nicht vollständig.
2	Veraltet	Es liegen veraltete Dokumentationen oder Richtlinien vor, die u.U. unvollständig sind.
3	Unvollständig/Entwurf	Es liegen in unvollständige Dokumentationen oder Richtlinien im Entwurfsstatus vor.
4	Unvollständig	Es liegen noch geringfügig unvollständige Dokumentationen oder Richtlinien vor.
5	Vollständig und aktuell	Es liegen vollständige Dokumentationen oder Richtlinien vor.

Eine Auswertung in Bezug auf die vorhandene Dokumentation kann wie folgt ausgestaltet werden. Eine Anpassung der Auswertungsdarstellung ist über die Excel eigenen Tools möglich.

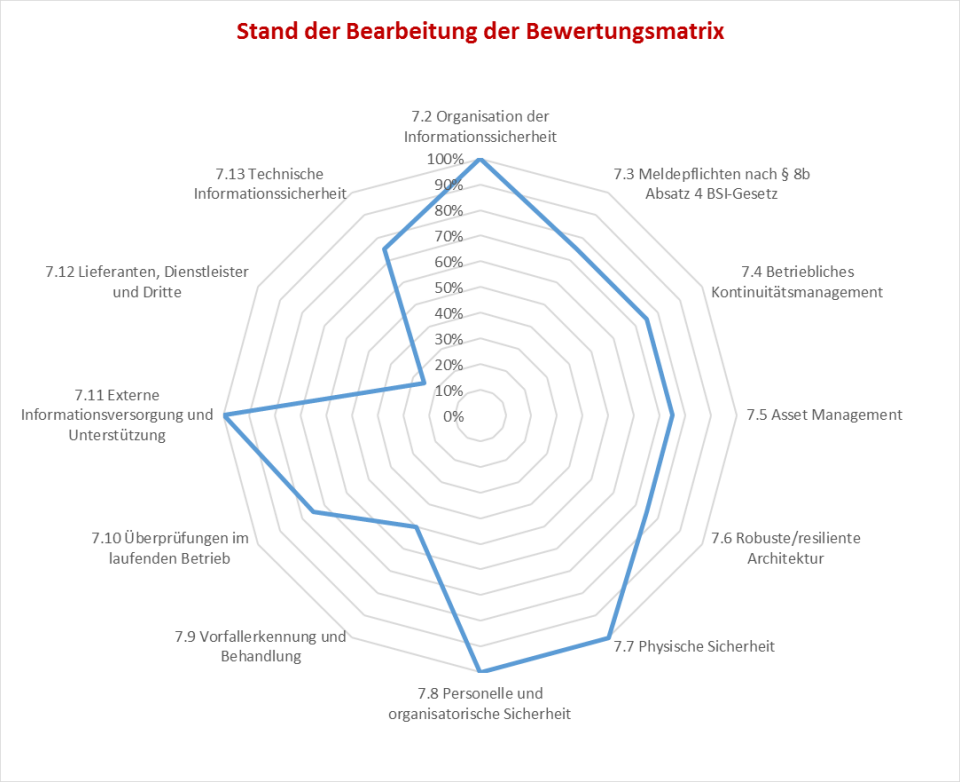


Bewertungsmatrix

Diese Auswertung gibt dem geneigten Leser darüber Auskunft, ob und in wie weit die Bearbeitung der Bewertungsmatrix insgesamt bzw. je Themenfeld fortgeschritten ist und damit wo noch Arbeiten durchzuführen sind.

Auf diese Weise muss die Bewertungsmatrix nicht „in einem Rutsch“ ausgefüllt werden, sondern ermöglicht es dem Anwender dies in Etappen bzw. nach seinem eigenen Tempo zu tun.

Eine Protokollierung wer bzw. wann an der Bewertungsmatrix gearbeitet hat erfolgt durch das Tool selber nicht. Wenn dies gewünscht ist, müssen hierzu externe Tools Anwendung finden.



Ihr Ansprechpartner

Das zur Verfügung zu stellende Tool (MS-Excel-Datei) ist von uns mit handelsüblichen Scannern auf Viren und andere Schadsoftware mit negativem Ergebnis geprüft worden und wird nach dem Zahlungseingang einer Schutzgebühr von 259,- EUR inkl. MwSt. zur Verfügung gestellt. Schicken Sie uns dafür gerne eine Anforderungs-eMail an

partners@compliance-net.com

und Sie erhalten eine Rechnung über die Schutzgebühr. Nach Zahlungseingang erhalten Sie eine eMail mit der Datei als Anhang oder einen Link zum Download der entsprechenden Datei.

Voraussetzung für die Nutzung ist eine aktuelle MS Excel-Version (z.B. mind. MS Excel 2016 oder MS Excel aus Office 365). Bei der Verwendung früherer MS Excel Versionen können Funktionseinbußen auftreten. Ihre IT Abteilung wird Ihnen gerne weiterhelfen.

Grundsätzlich ist das Tool aus unserer Sicht selbsterklärend und intuitiv zu handhaben. Sollten Sie dennoch Fragen haben oder der Auffassung sein, eine neutrale Stelle sollte die Befüllung der Bewertungsmatrix zur Standortbestimmung in Ihrer Organisation vornehmen, kontaktieren Sie uns selbstverständlich und gerne.

compliance-net GmbH

Robert-Bosch-Straße 32, 63303 Dreieich

Telefon: + 49 (0) 6103 376 96 0

eMail: partners@compliance-net.com

Hinweis:

Die compliance-net GmbH übernimmt für das Tool selbst und seine Anwendung keinerlei Haftung. Das Tool ist nach dem aktuellen Stand der Technik sowie nach bestem Wissen und Gewissen getestet worden. Dennoch können sich Fehler eingeschlichen haben. Der Nutzer verwendet das Tool deswegen eigenverantwortlich und auf eigene Gefahr. Zudem sind die Zellen und Datenblätter in der Datei nicht durch einen Schutz vor unsachgemäßer Veränderung geschützt. Somit sind die ausgewiesenen Ergebnisse immer durch den Bearbeitenden hinreichend genau zu prüfen. Das Tool verfügt über keinerlei eigene Sicherungsmechanismen und ist daher selbstständig entsprechenden Sicherungszyklen zuzuführen, um die Arbeitsergebnisse zu sichern. Das Tool basiert auf der neusten Version von Excel, daher sind ggf. Anpassungen durch Sie in Ihrem System vorzunehmen bevor Sie das Tool einsetzen können. Prüfen Sie dies bitte vor dem Erwerb und Einsatz des Tools. Für das Tool gibt es keinerlei Update Service. Sollten sich Verlautbarungen der grundlegenden Standards ändern, so sind diese selbstständig nach Erwerb des Tools durch den Erwerbenden einzupflegen.