Standortbestimmung zur

Umsetzung der

bankenaufsichtliche

Anforderung an die IT

(BAIT)

Präambel

Der Einsatz der Informationstechnik (IT) in den Instituten hat eine zentrale Bedeutung und wird weiter an Bedeutung gewinnen und damit auch im Zusammenhang mit der Einhaltung regulatorischer Maßgaben.

Das Rundschreiben der BaFin 02/2017 in der Fassung vom 23.02.2017 gibt auf der Grundlage des § 25a Abs. 1 des Kreditwesengesetzes (KWG) einen flexiblen und praxisnahen Rahmen für die Ausgestaltung der IT der Institute, insbesondere für das Management der IT-Ressourcen und für das IT-Risikomanagement vor. Es konkretisiert ferner bereichsübergreifend die Anforderungen des § 25a Abs. 3 KWG (Risikomanagement auf Gruppenebene) sowie des § 25b KWG (Auslagerung). Die Aktuelle Version des Rundschreibens finden Sie hier.

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.

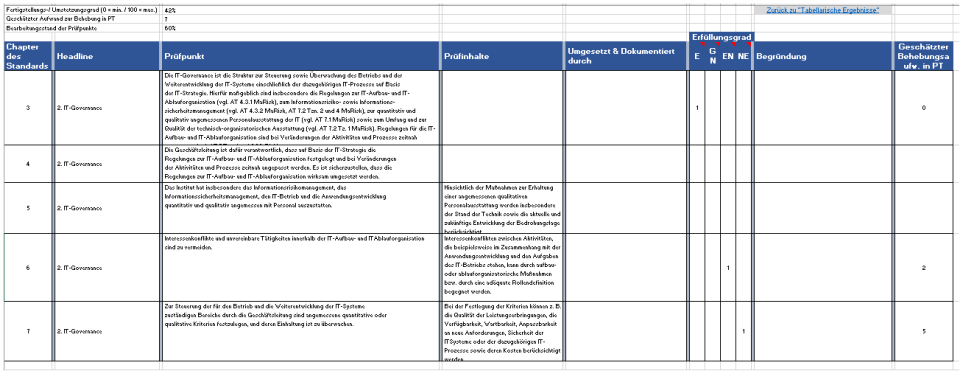
3-Stufen-Vorgehensmodell

Aufnahme und Bewertung

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

- IT-Strategie
- IT-Governance
- Informationsrisikomanagement
- Informationssicherheitsmanagement
- Benutzerberechtigungsmanagement
- IT-Projekte, Anwendungsentwicklung (inkl. durch Endbenutzer in den Fachbereichen)
- IT-Betrieb (inkl. Datensicherung)
- Auslagerungen und sonstiger Fremdbezug von IT-Dienstleistungen
- Kritische Infrastrukturen

Dies erfolgt unter zur Hilfenahme der Excel-Matrix. . Das nachfolgende Schaubild verdeutlicht dies anhand des Beispiels „IT-Governance“ 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 je Arbeitspaket zur möglicherweise notwendigen Anpassung an die bisherige Umsetzung und Dokumentation.



Fortgeschrittenheit Umsetzungsgrad (0 = min. / 100 = max.)	42%											Zurück zu "Tabellarische Ergebnisse"
Geschätzter Aufwand zur Behebung in PT	1											
Bearbeitungsgrad der Prüfpunkte	66%											
									Erfüllungsgrad			
Chapter des Standards	Headline	Prüfpunkt	Prüfinhalte	Umgesetzt & Dokumentiert durch					E	G	EN	NE	Begründung	Geschätzter Behebungsaufw. in PT
3	2. IT-Governance	Die IT-Governance ist die Struktur zur Steuerung sowie Überwachung des Betriebs und der Weiterentwicklung der IT-Systeme abschließend der dazugehörigen IT-Prozesse auf Basis der IT-Strategie. Hierfür maßgeblich sind insbesondere die Regelungen zur IT-Aufbau- und IT-Ablauforganisation (vgl. AT 4.3.1 MaRisk), zum Informationsrisiko- sowie Informations-sicherheitsmanagement (vgl. AT 4.3.2 MaRisk, AT 7.2 Tz. 2 und 4 MaRisk), zur qualitativ und quantitativ angemessenen Personalausstattung der IT (vgl. AT 7.1 MaRisk) sowie zum Umfang und zur Qualität der technisch-organisatorischen Ausstattung (vgl. AT 7.2 Tz. 1 MaRisk). Regelungen für die IT-Aufbau- und IT-Ablauforganisation sind bei Veränderungen der Aktivitäten und Prozesse anhand					1						0
4	2. IT-Governance	Die Geschäftsleitung ist dafür verantwortlich, dass auf Basis der IT-Strategie die Regelungen zur IT-Aufbau- und IT-Ablauforganisation festgelegt und bei Veränderungen der Aktivitäten und Prozesse zeitnah angepasst werden. Es ist sicherzustellen, dass die Regelungen zur IT-Aufbau- und IT-Ablauforganisation wirksam umgesetzt werden.										
5	2. IT-Governance	Das Institut hat insbesondere das Informationsrisikomanagement, das Informationssicherheitsmanagement, das IT-Betrieb und die Anwendungsentwicklung quantitativ und qualitativ segmentiert mit Personal auszustatten.	Hinsichtlich der Maßnahmen zur Erhaltung einer angemessenen qualitativen Personalausstattung wurden insbesondere der Stand der Technik sowie die aktuelle und zukünftige Entwicklung der Bedrohungslage berücksichtigt.									
6	2. IT-Governance	Interessenkonflikte und unvereinbare Tätigkeiten innerhalb der IT-Aufbau- und IT-Ablauforganisation sind zu vermeiden.	Interessenkonflikte zwischen Aktivitäten, die beispielsweise im Zusammenhang mit der Anwendungsentwicklung und den Aufgaben des IT-Betriebs stehen, kann durch aufbau- oder ablauforganisatorische Maßnahmen bzw. durch eine adäquate Rollendefinition begegnet werden.					1				2
7	2. IT-Governance	Zur Steuerung der für den Betrieb und die Weiterentwicklung der IT-Systeme zuständigen Bereiche durch die Geschäftsleitung sind angemessene quantitative oder qualitative Kriterien festzulegen, und deren Einhaltung ist zu überwachen.	Bei der Festlegung der Kriterien können z. B. die Gefährt der Leistungserbringungen, die Verfügbarkeit, Vertraulich, Angemessenheit in enes Anforderungen, Sicherheit der IT-Systeme oder der dazugehörigen IT-Prozesse sowie deren Kosten berücksichtigt werden.					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.

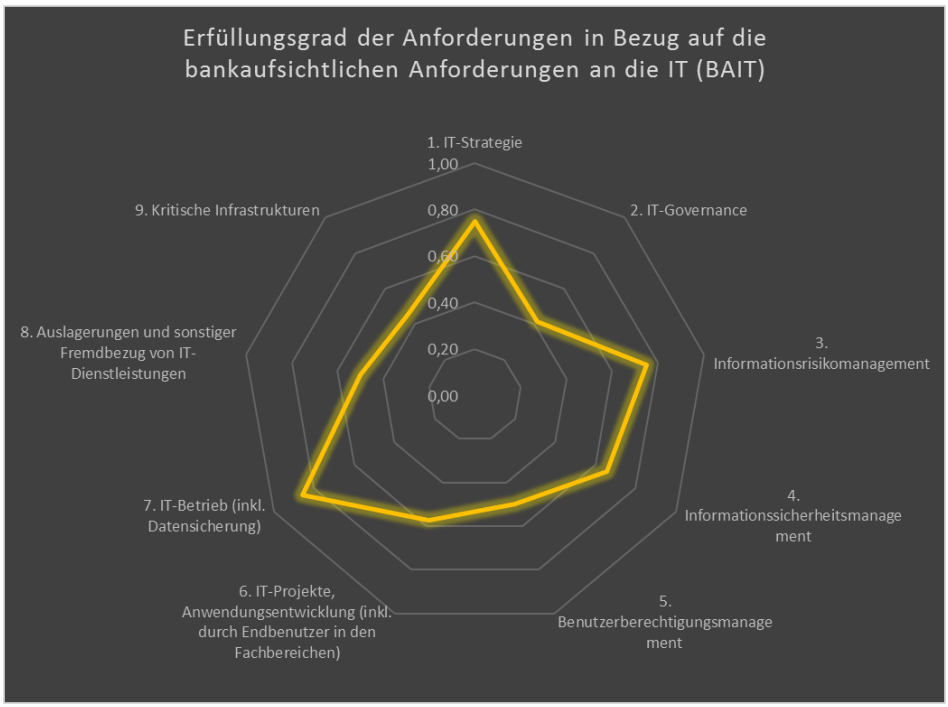
Bereich	Erfüllungsgrad 0 min. / 1 max.	Aufwand in PT je Arbeitspaket zur Anpassung der Prozesse, RL, AA, Dokumentation (geschätzt) im Sinne der bankaufsichtlichen Anforderungen an die IT (BAIT)	Bearbeitet 0%-100%	Reifegrade der Doku. (BSI)	Reifegrade der Orga (CMMI)
1. IT-Strategie	0,75	6 PT	100%	1	1
2. IT-Governance	0,42	7 PT	60%	2	2
3. Informationsrisikomanagement	0,75	21 PT	100%	3	3
4. Informationssicherheitsmanagement	0,66	40 PT	100%	4	4
5. Benutzerberechtigungsmanagement	0,50	20 PT	100%	5	5
6. IT-Projekte, Anwendungsentwicklung (inkl. durch Endbenutzer in den Fachbereichen)	0,57	36 PT	100%	1	1
7. IT-Betrieb (inkl. Datensicherung)	0,86	14 PT	100%	2	2
8. Auslagerungen und sonstiger Fremdbezug von IT-Dienstleistungen	0,50	12 PT	100%	3	3
9. Kritische Infrastrukturen	0,45	20 PT	100%	4	4

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

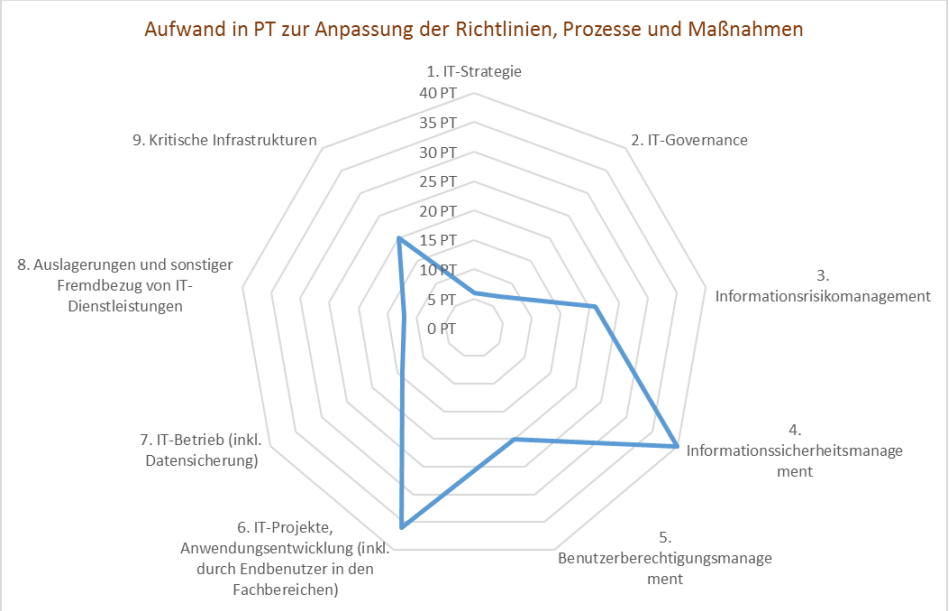
Diese sind editierbar und lassen sich den unternehmens- bzw. abteilungsindividuellen Maßgaben durch Sie anpassen.

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

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



Die untenstehende 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.

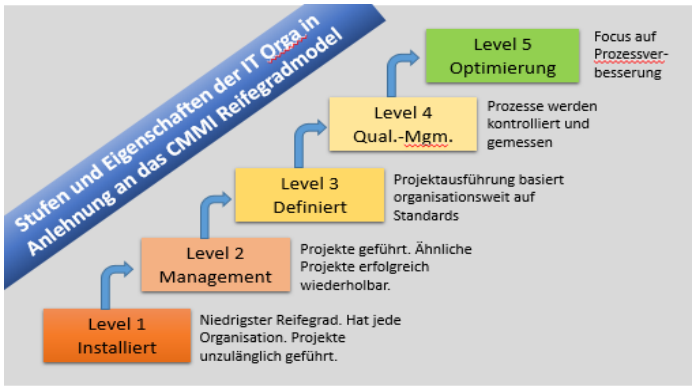


Reifegrad der Organisation

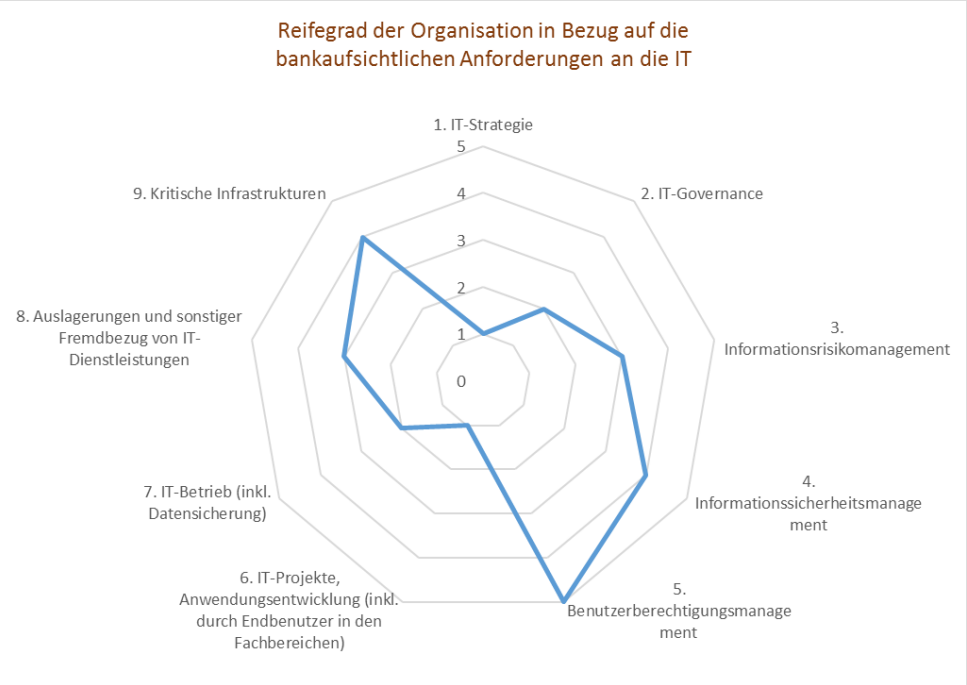
Der individuelle Reifegrad der Organisation kann anhand des bekannten und vorgegebenen CMMI Modells gemessen werden.

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.



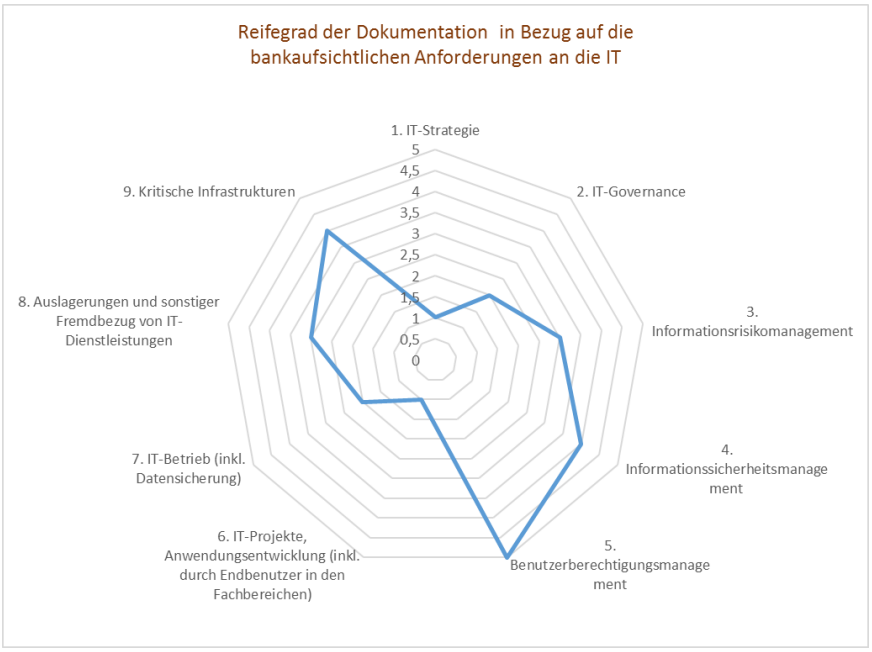
Reifegrad der Dokumentation

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.

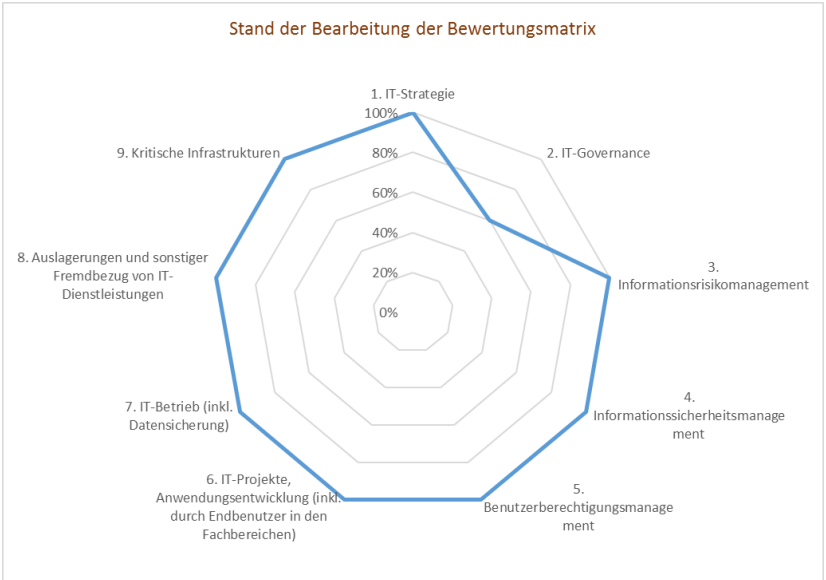


Bewertungs-matrix

Diese Auswertung gibt dem 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 Ansprech-partner

Das zur Verfügung gestellte 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.