Standortbestimmung zur

Umsetzung der

ISO/IEC 27001

Information technology – Security techniques –

Information security management systems – Requirements

(ISO/IEC 27001)

Präambel

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

Die internationale Norm ISO/IEC 27001 Information technology – Security techniques – Information security management systems – Requirements spezifiziert die Anforderungen für die Einrichtung, Umsetzung, Aufrechterhaltung und fortlaufende Verbesserung eines implementierten, gelebten und dokumentierten Informationssicherheits-Managementsystems unter Berücksichtigung des Kontexts Ihrer unternehmensindividuellen Organisationsstrukturen.

Dieser ISO Standard ist für eine Zertifizierung zugelassen, wodurch Ihr Unternehmen die Umsetzung nicht nur zum Selbstzweck in Bezug auf die Beurteilung und Behandlung von Informationssicherheitsrisiken nutzen, sondern die Ergebnisse auch in Ausschreibungen bzw. zu Marketingzwecken verwenden kann.

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.

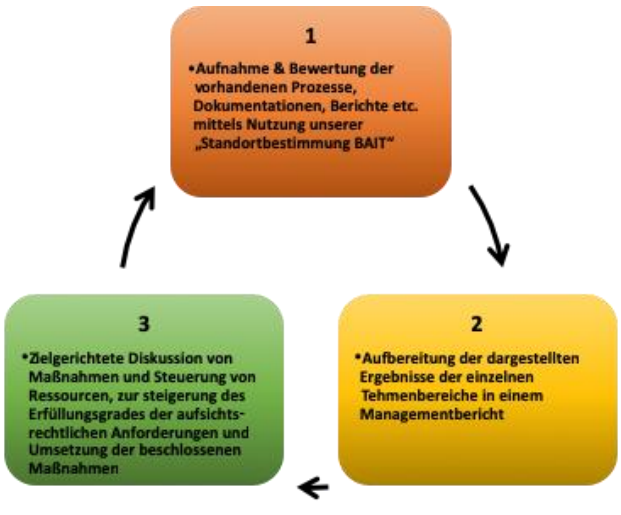
Beitrag zur Vermeidung (Entlastungsbeweis nach § 831 Abs. 1 S. 2 BGB) eines so genannten Organisationsverschuldens nach § 823 BGB Abs. 1 sowie zahlreicher gesetzlichen Maßgaben des AktG, GmbHG sowie KWG.

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
- Sicherheitsleitlinien
- Organisation der IS
- Sicherheit des Personals
- Wertemanagement
- Zugriffskontrolle
- Kryptographie
- Schutz vor physischem Zugang und Umwelteinflüssen
- Betriebssicherheit
- Sicherheit in der Kommunikation
- Anschaffung, Entwicklung und Instandhaltung von Systemen
- Lieferantenbeziehungen
- Management von Informationssicherheitsvorfällen
- Informationssicherheitsaspekte des Business Continuity Management
- Richtlinienkonformität

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 je Arbeitspaket zur möglicherweise notwendigen Anpassung an die bisherige Umsetzung und Dokumentation.

Fertigstellungsgrad (0 = min. / 100 = max : 65,00
Gesätzter 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 Beheburgsaufw. 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	Informationssicherhei t 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.

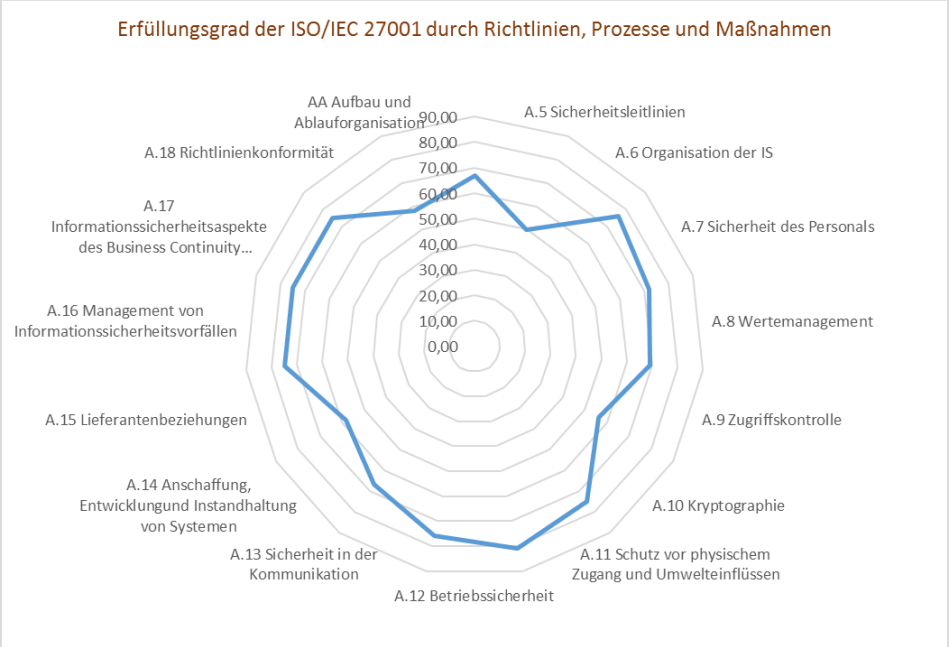
Bereich	Erfüllungsgrad 0 min. / 100 max.	Aufwand zur Behebung (geschätzt)	Bearbeitet 0%-100%
AA Aufbau und Ablauforganisation	67,44	98 PT	88%
AA 4 - Organisation	75,00	12 PT	75%
AA 5 - Führung	58,33	13 PT	100%
AA 6 - Planung	45,00	22 PT	71%
AA 7 - Unterstützung	68,75	32 PT	100%
AA 8 - Einsatz	75,00	9 PT	100%
AA 9 - Leistungsauswertung	75,00	7 PT	67%
AA 10 - Verbesserung	75,00	3 PT	100%
A.5 Sicherheitsleitlinien	50,00	13 PT	100%
A.5.1 Vorgaben der Leitung zur Informationssicherheit	50,00	13 PT	100%
A.6 Organisation der IS	76,25	8 PT	100%
A.6.1 Interne Organisation	65,00	6 PT	100%
A.6.2 Mobilgeräte und Telearbeit	87,50	2 PT	100%
A.7 Sicherheit des Personals	72,22	21 PT	100%
A.7.1 Vor der Einstell	75,00	10 PT	
A.13 Sicherheit in der Kommunikation	66,67	24 PT	
A.13.1 Netzwerksicherheitsmanagement	58,33	12 PT	100%
A.13.2 Informationsübertragung	75,00	12 PT	100%
A.14 Anschaffung, Entwicklung und Instandhaltung von Systemen	58,33	26 PT	81%
A.14.1 Sicherheitsanforderungen für Informationssysteme	75,00	9 PT	100%
A.14.2 Sicherheit in Entwicklungs- und Unterstützungsprozessen	75,00	12 PT	44%
A.14.3 Prüfdaten	25,00	5 PT	100%
A.15 Lieferantenbeziehungen	75,00	10 PT	42%
A.15.1 Sicherheit in Lieferantenbeziehungen	75,00	5 PT	33%
A.15.2 Management der Dienstleistungserbringung durch Lieferanten	75,00	5 PT	50%
A.16 Management von Informationssicherheitsvorfällen	75,00	36 PT	300%
A.16.1 Management von Informationssicherheitsvorfällen und Verbesserungen	75,00	36 PT	300%
A.17 Informationssicherheitsaspekte des Business Continuity Management	75,00	13 PT	75%
A.17.1 Kontinuität der Informationssicherheit	75,00	10 PT	50%
A.17.2 Redundanzen	75,00	3 PT	100%
A.18 Richtlinienkonformität	58,33	40 PT	100%
A.18.1 Informationssicherheitsprüfungen	41,67	15 PT	100%
A.18.2 Einhaltung gesetzlicher und vertraglicher Anforderungen	75,00	25 PT	100%

Vorgefertigte grafische Auswertungen unterstützen die weitere Analyse sowie die Verwendung der unternehmensindividuell 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.



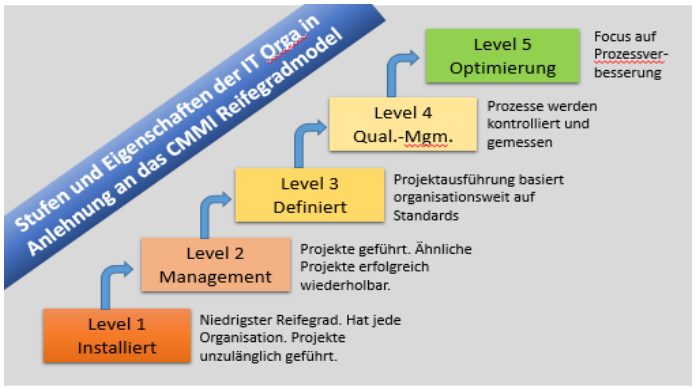
Die folgende Grafik gibt Auskunft darüber, wie viel PT (Personentage) für die Bewirtschaftung der im Rahmen der Standortbestimmung identifizierten Felder geschätzt aufgebracht werden müssten, um diese Lücken in den jeweiligen Bereichen auf eine angestrebte prozentuale Abdeckung zu heben.

Reifegrad der Organisation

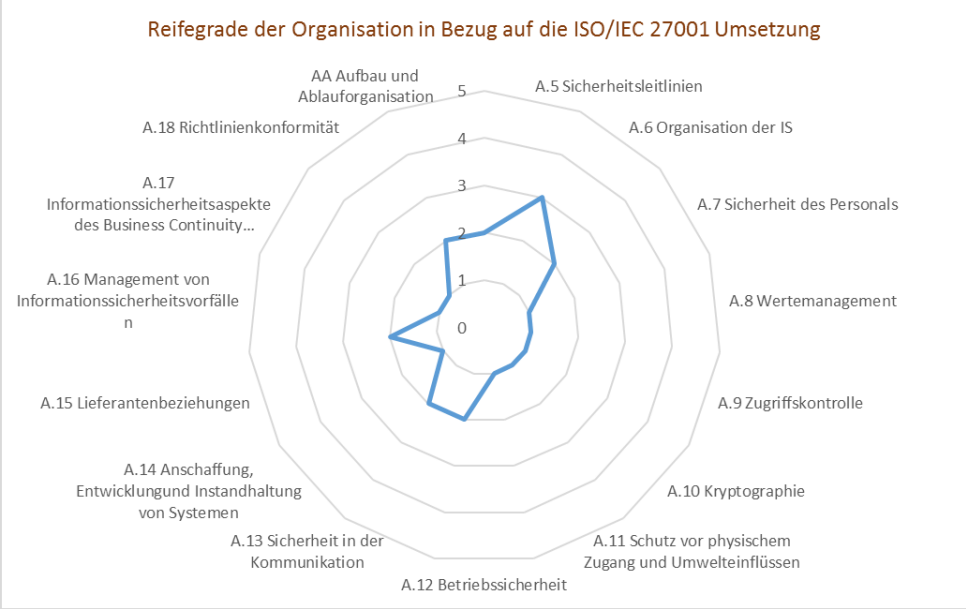
Der individuelle Reifegrad der Organisation kann anhand des bekannten und vorgegebenen CMMI Modells gemessen werden.

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.



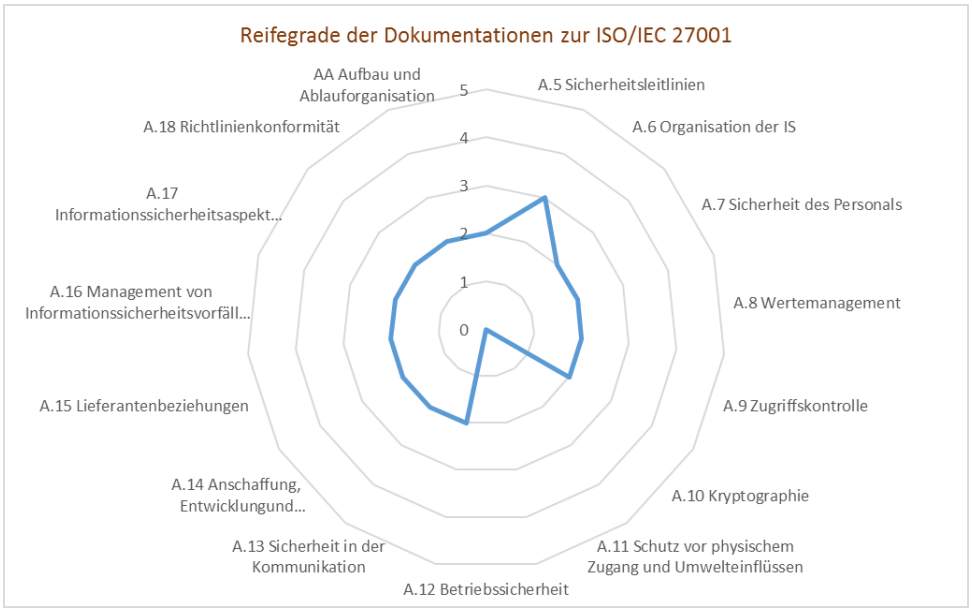
Reifegrad der Dokumentation

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 in Excel eigenen Tools möglich.

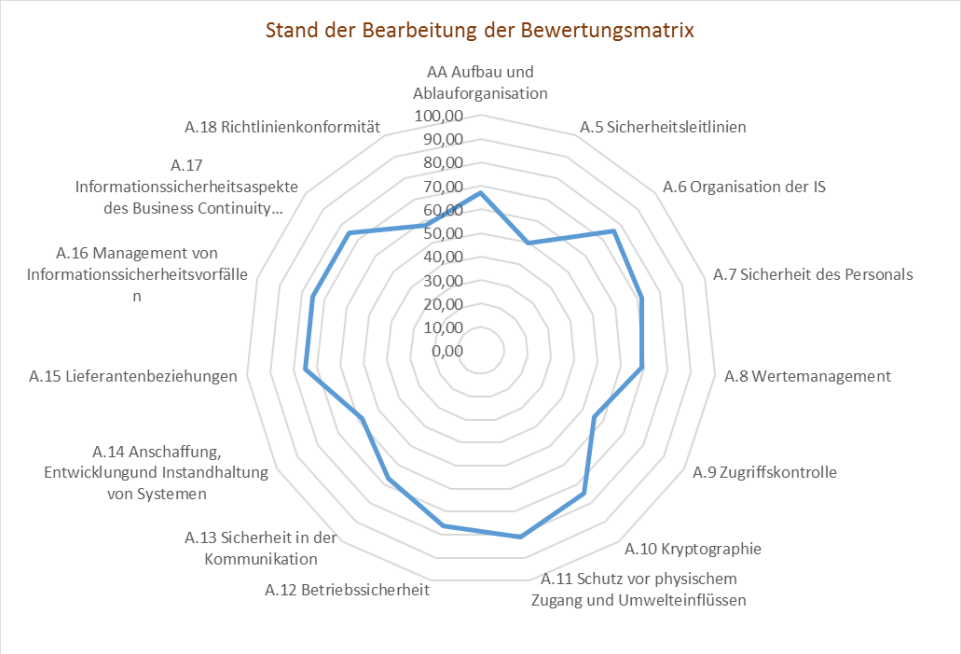


Bewertungsmatrix

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.