Konformitätsbericht zu Standard/Norm

ISO/IEC 27001:2022

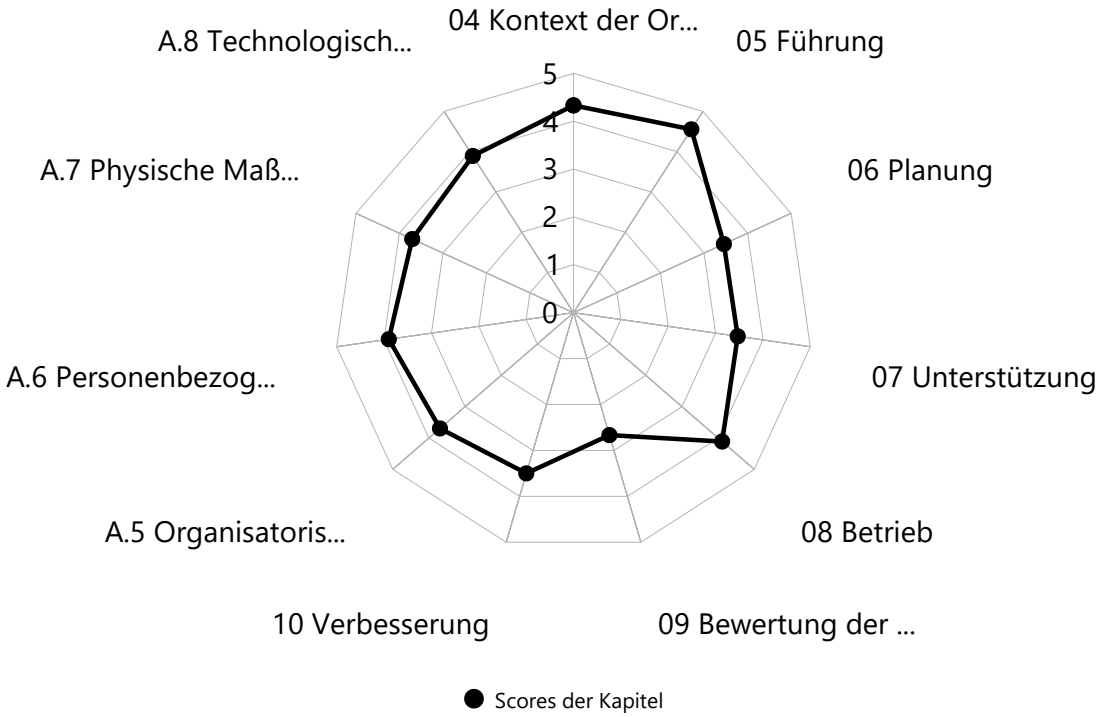
Managementsystem(e): Information Security
Target Score: Reifegrad 4: gemessen

Inhaltsverzeichnis

ISO/IEC 27001:2022

Informationssicherheit, Cybersicherheit und Datenschutz - Informationssicherheitsmanagementsysteme - Anforderungen (ISO/IEC 27001:2022); Deutsche Fassung EN ISO/IEC 27001:2023

Stand:	30.11.2024
Beschreibung:	Diese Norm ist für alle Organisationsarten anwendbar und legt die Anforderungen an Aufstellen, Umsetzen, Betrieb, Überwachung, Bewertung, Wartung und Verbesserung von dokumentierten Informationssicherheit-Managementsystemen in Bezug auf die allgemeinen Geschäftsrisiken einer Organisation fest. Sie legt außerdem die Anforderungen an die Einführung von Sicherheitskontrollen fest, die auf die Bedürfnisse einer Organisation oder Teilen davon zugeschnitten sind. Das Informationssicherheits-Managementsystem ist dafür entwickelt worden, die Auswahl ausreichender und angemessener Sicherheitskontrollen zu gewährleisten, die den Informationsbestand sichern und interessierten Partnern Vertrauenswürdigkeit vermitteln.



Tabellarische Auflistung der Kapitelstruktur

Gliederung	Bezeichnung	∅Score
04	**Kontext der Organisation**	**4,3**
4.1	Verstehen der Organisation und ihres Kontextes	3,7
4.2	Verstehen der Erfordernisse und Erwartungen interessierter Parteien	3,7
4.3	Festlegen des Anwendungsbereichs des Informationssicherheitsmanagementsystems	5,0
4.4	Informationssicherheitsmanagementsystem	5,0
05	**Führung**	**4,6**
5.1	Führung und Verpflichtung	5,0
5.2	Politik	5,0
5.3	Rollen, Verantwortlichkeiten und Befugnisse in der Organisation	3,7
06	**Planung**	**3,5**
6.1	Maßnahmen zum Umgang mit Risiken und Chancen	3,9
6.1.1	Allgemeines	4,0
6.1.2	Informationssicherheitsrisikobeurteilung	4,3
6.1.3	Informationssicherheitsrisikobehandlung	3,4
6.2	Informationssicherheitsziele und Planung zu deren Erreichung	3,0
6.3	Planning of changes	-
07	**Unterstützung**	**3,5**
7.1	Ressourcen	3,7
7.2	Kompetenz	5,0
7.3	Bewusstsein	2,0
7.4	Kommunikation	3,0
7.5	Dokumentierte Information	3,7
7.5.1	Allgemeines	3,7
7.5.2	Erstellen und Aktualisieren	3,7
7.5.3	Lenkung dokumentierter Information	3,7
08	**Betrieb**	**4,1**
8.1	Betriebliche Planung und Steuerung	4,3
8.2	Informationssicherheitsrisikobeurteilung	4,3
8.3	Informationssicherheitsrisikobehandlung	3,7
09	**Bewertung der Leistung**	**2,7**
9.1	Überwachung, Messung, Analyse und Bewertung	4,0
9.2	Internes Audit	5,0
9.2.1	Allgemeines	5,0
9.2.2	Internes Auditprogramm	5,0
9.3	Managementbewertung	4,0
9.3.1	Allgemeines	4,0
9.3.2	Inputs der Managementbewertung	4,0

Gliederung	Bezeichnung	∅Score
9.3.3	Ergebnisse der Managementbewertung	4,0
10	**Verbesserung**	**3,5**
10.1	Fortlaufende Verbesserung	3,0
10.2	Nichtkonformität und Korrekturmaßnahmen	4,0
A.5	**Organisatorische Maßnahmen**	**3,7**
A.5.1	Informationssicherheitsrichtlinien	5,0
A.5.2	Informationssicherheitsrollen und -verantwortlichkeiten	4,0
A.5.3	Aufgabentrennung	3,7
A.5.4	Verantwortlichkeiten der Leitung	3,0
A.5.5	Kontakt mit Behörden	3,0
A.5.6	Kontakt mit speziellen Interessensgruppen	3,7
A.5.7	Bedrohungsintelligenz	5,0
A.5.8	Informationssicherheit im Projektmanagement	5,0
A.5.9	Inventar der Informationen und anderen damit verbundenen Werten	4,0
A.5.10	Zulässiger Gebrauch von Informationen und anderen damit verbundenen Werten	4,0
A.5.11	Rückgabe von Werten	4,0
A.5.12	Klassifizierung von Information	4,0
A.5.13	Kennzeichnung von Information	3,7
A.5.14	Informationsübertragung	4,0
A.5.15	Zugangssteuerung	4,2
A.5.16	Identitätsmanagement	4,2
A.5.17	Informationen zur Authentifizierung	3,5
A.5.18	Zugangsrechte	3,9
A.5.19	Informationssicherheit in Lieferantenbeziehungen	3,7
A.5.20	Behandlung von Informationssicherheit in Lieferantenvereinbarungen	4,0
A.5.21	Umgang mit der Informationssicherheit in der IKT-Lieferkette	3,0
A.5.22	Überwachung, Überprüfung und Änderungsmanagement von Lieferantendienstleistungen	2,3
A.5.23	Informationssicherheit für die Nutzung von Cloud-Diensten	1,0
A.5.24	Planung und Vorbereitung der Handhabung von Informationssicherheitsvorfällen	2,7
A.5.25	Beurteilung und Entscheidung über Informationssicherheitsereignisse	3,0
A.5.26	Reaktion auf Informationssicherheitsvorfälle	3,5
A.5.27	Erkenntnisse aus Informationssicherheitsvorfällen	2,5
A.5.28	Sammeln von Beweismaterial	3,0
A.5.29	Informationssicherheit bei Störungen	4,0
A.5.30	IKT-Bereitschaft für Business Continuity	2,0

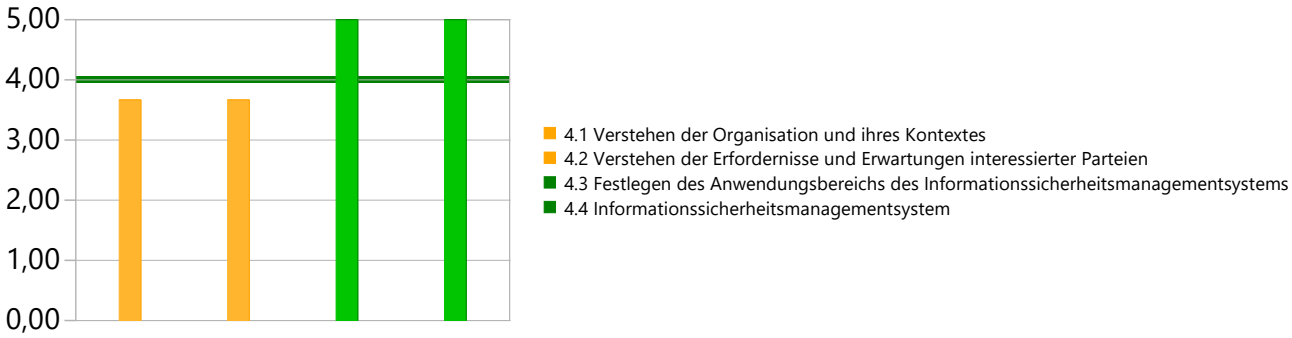
Gliederung	Bezeichnung	∅Score
A.5.31	Rechtliche, gesetzliche, regulatorische und vertragliche Anforderungen	5,0
A.5.32	Geistige Eigentumsrechte	5,0
A.5.33	Schutz von Aufzeichnungen	1,0
A.5.34	Datenschutz und Schutz personenbezogener Daten (pbD)	5,0
A.5.35	Unabhängige Überprüfung der Informationssicherheit	5,0
A.5.36	Einhaltung von Richtlinien, Vorschriften und Normen für die Informationssicherheit	5,0
A.5.37	Dokumentierte Betriebsabläufe	4,2
A.6	**Personenbezogene Maßnahmen**	**3,9**
A.6.1	Sicherheitsüberprüfung	5,0
A.6.2	Beschäftigungs- und Vertragsbedingungen	5,0
A.6.3	Informationssicherheitsbewusstsein, -ausbildung und -schulung	4,2
A.6.4	Maßregelungsprozess	3,7
A.6.5	Verantwortlichkeiten bei Beendigung oder Änderung der Beschäftigung	5,0
A.6.6	Vertraulichkeits- oder Geheimhaltungsvereinbarungen	3,0
A.6.7	Telearbeit	2,3
A.6.8	Meldung von Informationssicherheitsereignissen	3,0
A.7	**Physische Maßnahmen**	**3,7**
A.7.1	Physische Sicherheitsperimeter	1,7
A.7.2	Physischer Zutritt	3,0
A.7.3	Sichern von Büros, Räumen und Einrichtungen	2,3
A.7.4	Physische Sicherheitsüberwachung	2,0
A.7.5	Schutz vor physischen und umweltbedingten Bedrohungen	3,0
A.7.6	Arbeiten in Sicherheitsbereichen	2,3
A.7.7	Aufgeräumte Arbeitsumgebung und Bildschirmsperren	4,2
A.7.8	Platzierung und Schutz von Geräten und Betriebsmitteln	5,0
A.7.9	Sicherheit von Werten außerhalb der Räumlichkeiten	4,2
A.7.10	Speichermedien	4,7
A.7.11	Versorgungseinrichtungen	5,0
A.7.12	Sicherheit der Verkabelung	5,0
A.7.13	Instandhaltung von Geräten und Betriebsmitteln	5,0
A.7.14	Sichere Entsorgung oder Wiederverwendung von Geräten und Betriebsmitteln	4,4
A.8	**Technologische Maßnahmen**	**3,9**
A.8.1	Endpunktgeräte des Benutzers	4,4
A.8.2	Privilegierte Zugangsrechte	2,5
A.8.3	Informationszugangsbeschränkung	4,3
A.8.4	Zugriff auf den Quellcode	4,3
A.8.5	Sichere Authentifizierung	3,0

Gliederung	Bezeichnung	∅Score
A.8.6	Kapazitätssteuerung	2,3
A.8.7	Schutz gegen Schadsoftware	5,0
A.8.8	Handhabung von technischen Schwachstellen	5,0
A.8.9	Konfigurationsmanagement	3,0
A.8.10	Löschung von Informationen	5,0
A.8.11	Datenmaskierung	3,0
A.8.12	Verhinderung von Datenlecks	5,0
A.8.13	Sicherung von Information	3,8
A.8.14	Redundanz von informationsverarbeitenden Einrichtungen	4,3
A.8.15	Protokollierung	3,7
A.8.16	Überwachung von Aktivitäten	1,7
A.8.17	Uhrensynchronisation	3,0
A.8.18	Gebrauch von Hilfsprogrammen mit privilegierten Rechten	2,0
A.8.19	Installation von Software auf Systemen im Betrieb	4,6
A.8.20	Netzwerksicherheit	4,3
A.8.21	Sicherheit von Netzwerkdiensten	5,0
A.8.22	Trennung von Netzwerken	5,0
A.8.23	Webfilterung	3,0
A.8.24	Verwendung von Kryptographie	4,5
A.8.25	Lebenszyklus einer sicheren Entwicklung	5,0
A.8.26	Anforderungen an die Anwendungssicherheit	2,0
A.8.27	Sichere Systemarchitektur und technische Grundsätze	4,3
A.8.28	Sicheres Coding	4,0
A.8.29	Sicherheitsprüfung in Entwicklung und Abnahme	3,0
A.8.30	Ausgegliederte Entwicklung	-
A.8.31	Trennung von Entwicklungs-, Prüf- und Produktionsumgebungen	5,0
A.8.32	Änderungssteuerung	3,3
A.8.33	Prüfinformationen	5,0
A.8.34	Schutz der Informationssysteme während der Überwachungsprüfung	5,0

04 Kontext der Organisation

Der aktuelle Erfüllungsgrad für dieses Thema liegt bei: 4,3

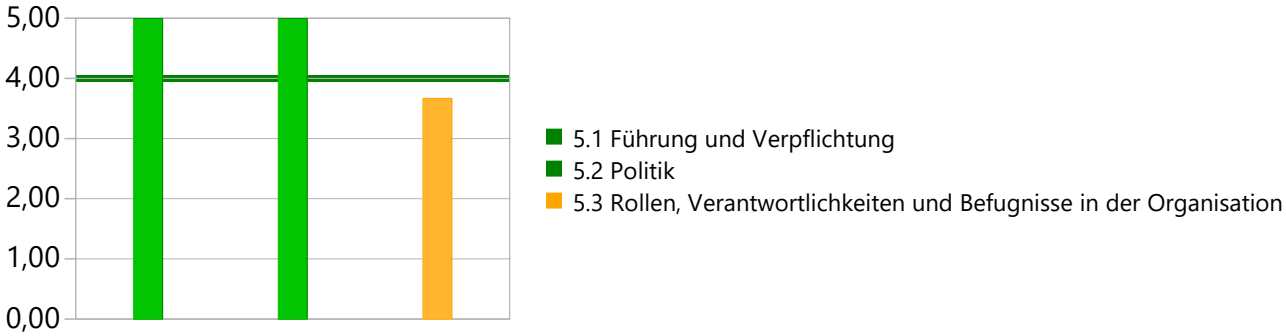
Dieses Resultat ergibt sich aus den Bewertungen der weiterführenden untergeordneten Themen wie folgt:



05 Führung

Der aktuelle Erfüllungsgrad für dieses Thema liegt bei: 4,6

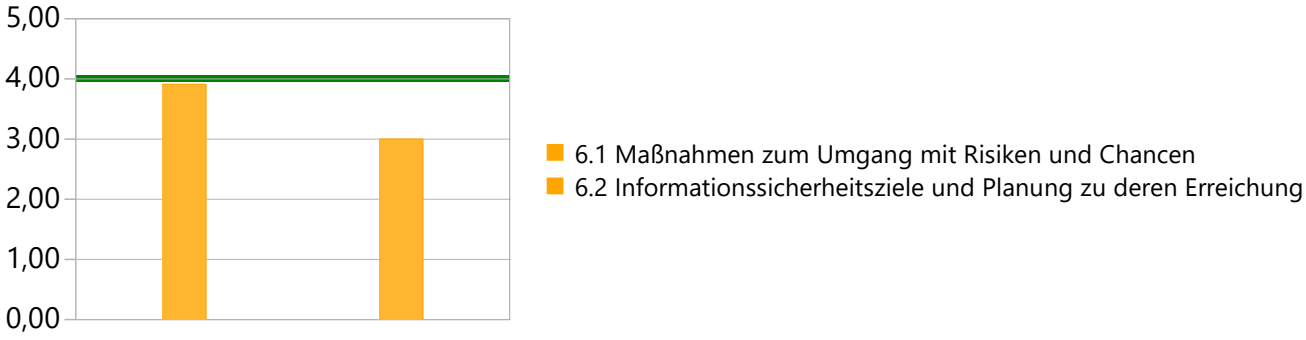
Dieses Resultat ergibt sich aus den Bewertungen der weiterführenden untergeordneten Themen wie folgt:



06 Planung

Der aktuelle Erfüllungsgrad für dieses Thema liegt bei: 3,5

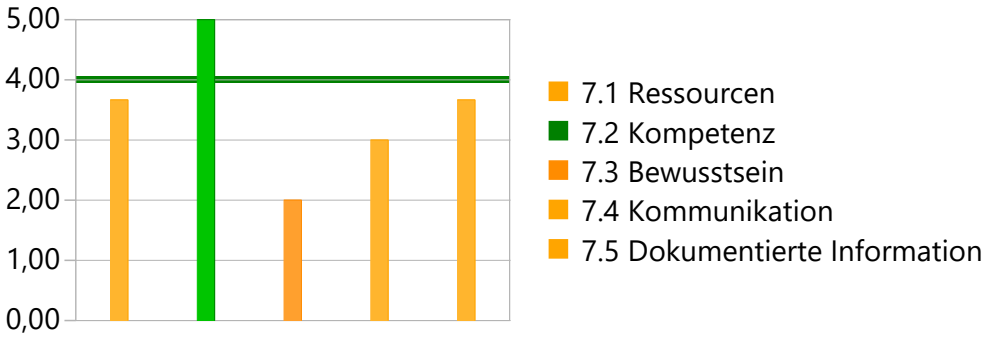
Dieses Resultat ergibt sich aus den Bewertungen der weiterführenden untergeordneten Themen wie folgt:



07 Unterstützung

Der aktuelle Erfüllungsgrad für dieses Thema liegt bei: 3,5

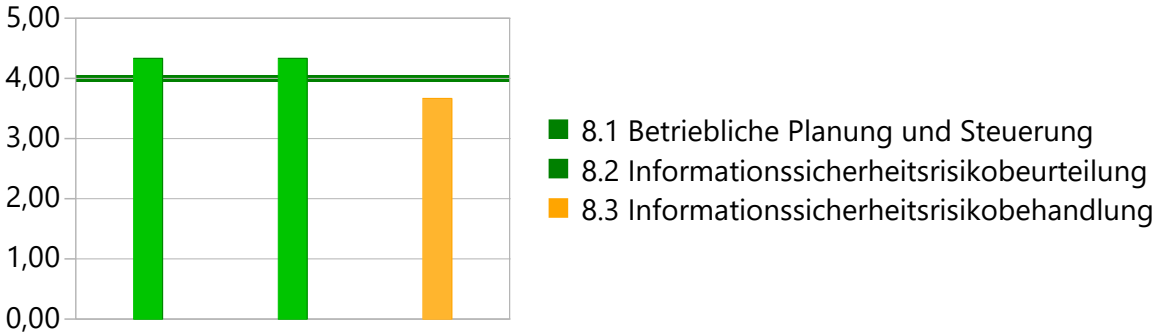
Dieses Resultat ergibt sich aus den Bewertungen der weiterführenden untergeordneten Themen wie folgt:



08 Betrieb

Der aktuelle Erfüllungsgrad für dieses Thema liegt bei: 4,1

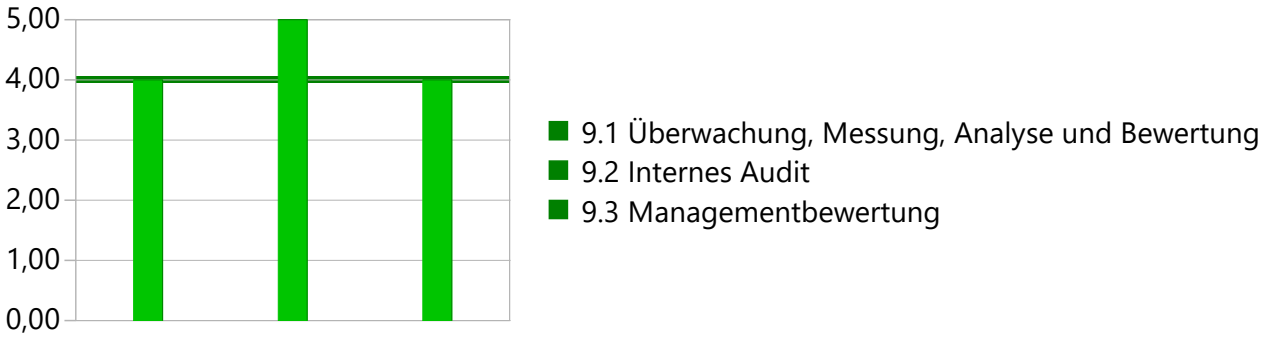
Dieses Resultat ergibt sich aus den Bewertungen der weiterführenden untergeordneten Themen wie folgt:



09 Bewertung der Leistung

Der aktuelle Erfüllungsgrad für dieses Thema liegt bei: 2,7

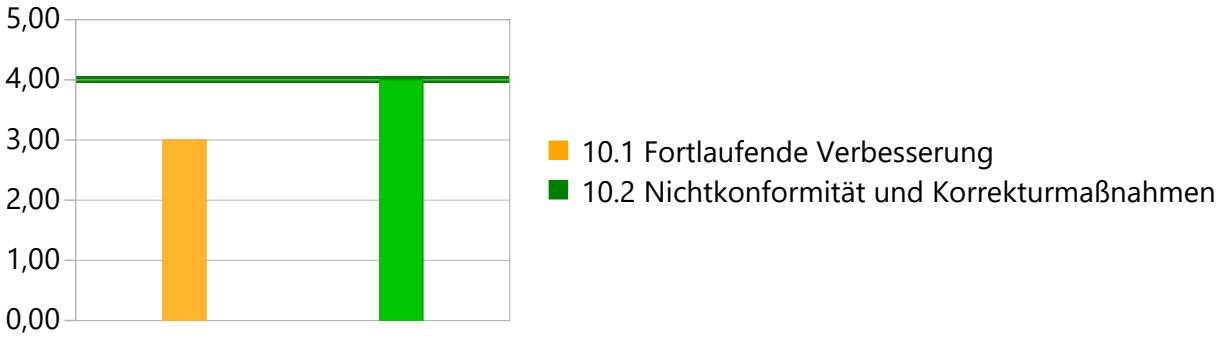
Dieses Resultat ergibt sich aus der Bewertung der Fragen die dem Hauptkapitel (Bewertung: 1.00) zugeordnet wurden und den Bewertungen der weiterführenden untergeordneten Themen. Die weiterführenden untergeordneten Themen wurden dabei wie folgt bewertet:



10 Verbesserung

Der aktuelle Erfüllungsgrad für dieses Thema liegt bei: 3,5

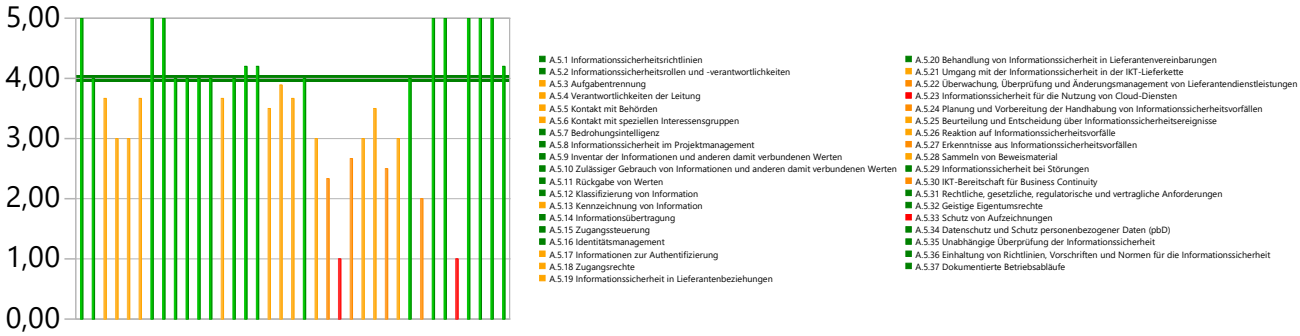
Dieses Resultat ergibt sich aus den Bewertungen der weiterführenden untergeordneten Themen wie folgt:



A.5 Organisatorische Maßnahmen

Der aktuelle Erfüllungsgrad für dieses Thema liegt bei: 3,7

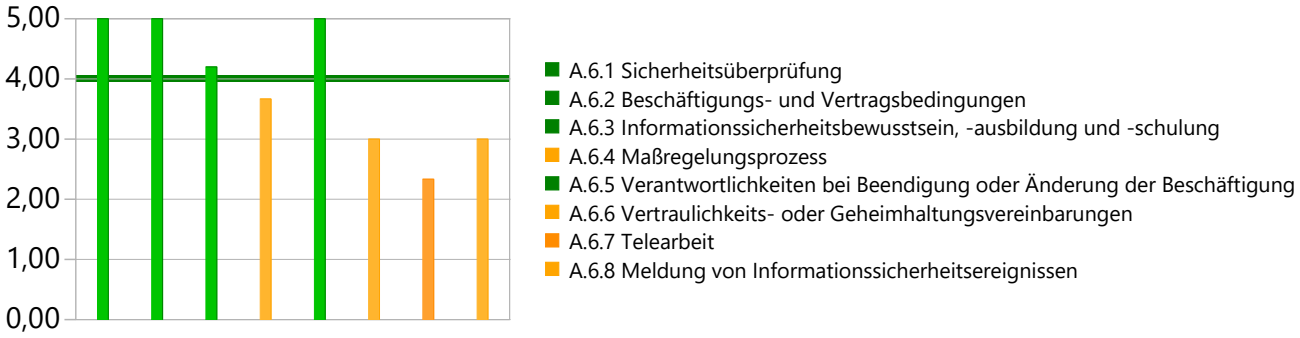
Dieses Resultat ergibt sich aus den Bewertungen der weiterführenden untergeordneten Themen wie folgt:



A.6 Personenbezogene Maßnahmen

Der aktuelle Erfüllungsgrad für dieses Thema liegt bei: 3,9

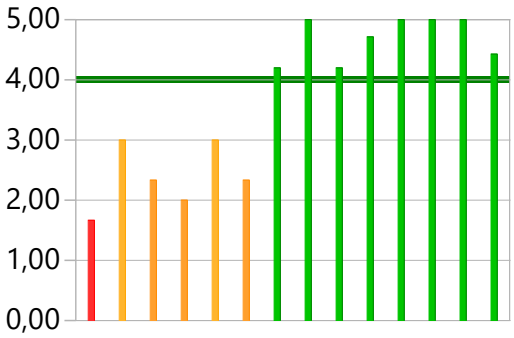
Dieses Resultat ergibt sich aus den Bewertungen der weiterführenden untergeordneten Themen wie folgt:



A.7 Physische Maßnahmen

Der aktuelle Erfüllungsgrad für dieses Thema liegt bei: 3,7

Dieses Resultat ergibt sich aus den Bewertungen der weiterführenden untergeordneten Themen wie folgt:

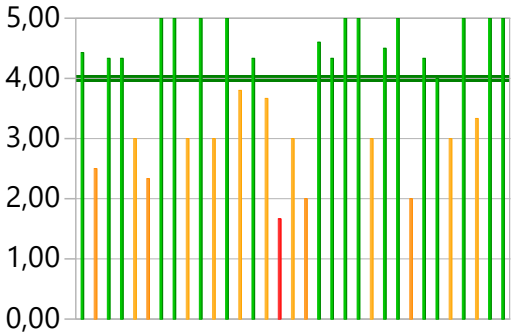


- A.7.1 Physische Sicherheitsperimeter
- A.7.2 Physischer Zutritt
- A.7.3 Sichern von Büros, Räumen und Einrichtungen
- A.7.4 Physische Sicherheitsüberwachung
- A.7.5 Schutz vor physischen und umweltbedingten Bedrohungen
- A.7.6 Arbeiten in Sicherheitsbereichen
- A.7.7 Aufgeräumte Arbeitsumgebung und Bildschirmsperren
- A.7.8 Platzierung und Schutz von Geräten und Betriebsmitteln
- A.7.9 Sicherheit von Werten außerhalb der Räumlichkeiten
- A.7.10 Speichermedien
- A.7.11 Versorgungseinrichtungen
- A.7.12 Sicherheit der Verkabelung
- A.7.13 Instandhaltung von Geräten und Betriebsmitteln
- A.7.14 Sichere Entsorgung oder Wiederverwendung von Geräten und Betriebsmitteln

A.8 Technologische Maßnahmen

Der aktuelle Erfüllungsgrad für dieses Thema liegt bei: 3,9

Dieses Resultat ergibt sich aus den Bewertungen der weiterführenden untergeordneten Themen wie folgt:



- A.8.1 Endpunktgeräte des Benutzers
- A.8.2 Privilegierte Zugangsrechte
- A.8.3 Informationszugangsbeschränkung
- A.8.4 Zugriff auf den Quellcode
- A.8.5 Sichere Authentifizierung
- A.8.6 Kapazitätssteuerung
- A.8.7 Schutz gegen Schadsoftware
- A.8.8 Handhabung von technischen Schwachstellen
- A.8.9 Konfigurationsmanagement
- A.8.10 Löschung von Informationen
- A.8.11 Datenmaskierung
- A.8.12 Verhinderung von Datenlecks
- A.8.13 Sicherung von Information
- A.8.14 Redundanz von informationsverarbeitenden Einrichtungen
- A.8.15 Protokollierung
- A.8.16 Überwachung von Aktivitäten
- A.8.17 Uhrensynchronisation
- A.8.18 Gebrauch von Hilfsprogrammen mit privilegierten Rechten
- A.8.19 Installation von Software auf Systemen im Betrieb
- A.8.20 Netzwerksicherheit
- A.8.21 Sicherheit von Netzwerkdiensten
- A.8.22 Trennung von Netzwerken
- A.8.23 Webfilterung
- A.8.24 Verwendung von Kryptographie
- A.8.25 Lebenszyklus einer sicheren Entwicklung
- A.8.26 Anforderungen an die Anwendungssicherheit
- A.8.27 Sichere Systemarchitektur und technische Grundsätze
- A.8.28 Sicheres Coding
- A.8.29 Sicherheitsprüfung in Entwicklung und Abnahme
- A.8.31 Trennung von Entwicklungs-, Prüf- und Produktionsumgebungen
- A.8.32 Änderungssteuerung
- A.8.33 Prüfinformationen
- A.8.34 Schutz der Informationssysteme während der Überwachungsprüfung

Anhang

Im Folgenden wird erläutert welche Arten von Fragen und Antworttypen in den Überprüfungen verwendet werden können und welche Bedeutung diese haben:

Score Fragen

Die Reifegradbewertung orientiert sich am Capability Maturity Model Integration (CMMI) Reifegradmodell der ISACA. Der Reifegrad beschreibt ein Entwicklungsniveau eines Prozesses. Die Reifegrade sind:

Reifegrad 1: initial
Diesen Reifegrad hat jedes Prozessgebiet automatisch.

Reifegrad 2: gemanagt
Die Projekte in diesem Prozessgebiet werden geführt. Ähnliche Projekte können dadurch erfolgreich wiederholt werden.

Reifegrad 3: definiert
Die Projekte in diesem Prozessgebiet werden nach einem angepassten Standardprozess durchgeführt und eine organisationsweite kontinuierliche Prozessverbesserung ist vorhanden.

Reifegrad 4: gemessen
Es wird eine statistische Prozesskontrolle durchgeführt.

Reifegrad 5: optimiert
Die Arbeit und die Arbeitsweise werden mit Hilfe der statistischen Prozesskontrolle verbessert.

Alternatives Bewertungsschema „Notensystem“

Wurde das Bewertungsschema „Notensystem“ ausgewählt, so sind die Antwortmöglichkeiten die folgenden: „Note 1: erfüllt“, „Note 2: teilweise erfüllt“, „Note 3: kaum erfüllt“ und „Note 4: nicht erfüllt“.

In jedem Fall berechnet HITGuard einen einheitlichen Score, unabhängig davon, welches Bewertungsschema in Überprüfungen angewendet wird.

Technikfragen

Die Bewertung von Technikfragen ist mit den Antwortmöglichkeiten „Ja“, „Nein“, „Teilweise“ möglich.

Weitere Antwortmöglichkeiten

Die Option "Entbehrlich" bedeutet, dass eine Frage im Kontext des Anwendungsbereichs nicht sinnvoll bzw. nicht relevant ist. „Nicht beantwortet“ bedeutet, dass die Frage im Zuge der Überprüfung nicht gestellt wurde.

Strukturfrage/Teilfrage

Die Beantwortung von Strukturfragen steuert die Anzeige bzw. Beantwortung von Teilfragen. Die Beantwortung der Teilfragen ist relevant für die Compliance Auswertungen. Dies bedeutet, dass Strukturfragen nicht in den Score eingerechnet werden. Sie erkennen Strukturfragen an der kursiven Darstellung; die dazugehörigen Teilfragen sind darunter eingerückt.