CWS
CYBERWERKSUITE

ISMS-Kennzahlenkatalog

Achtundvierzig Messgrößen für ein ISO/IEC-27001-Managementsystem — je die führende Formel und das, was die Zahl tatsächlich aussagt.

Kein Dashboard und kein Reifegradmodell. Die Formeln selbst, die vier Fallstricke, die sie zum Lügen bringen, und die Regeln, die ein Verhältnis ehrlich halten, wenn ein Prüfer es nachrechnet.

CyberWerkSuite · ISO/IEC 27001:2022, Kapitel 9.1 · Annex B der ISO/IEC 27004:2016 ist informativ — er enthält Messbeispiele, keine verpflichtenden Kennzahlen. Jede Formulierung hier ist unsere eigene; wir geben den Annex nicht wieder.

48	36	12	DE / EN
Messgrößen	Gegenstände in Annex B	Ergänzt für 2022 und 2024	Beide Ausgaben

CyberWerkSuite

cyberwerksuite.com

Dr. Sait Yalazay

CISO · DPO · Author | CISM · CIPP · AAISM · LA 27001, 27701, 22301, 42001

Architect of Automated Compliance Systems for NIS2, GDPR, ISMS, BCM, DORA, Cloud Security (C5), Tisax & AI Act

Leitung, Ressourcen, Audit und Verbesserung

Jede Messgröße in einer Zeile: die Formel, was die Zahl aussagt, und ob sie Leistung, Wirksamkeit oder beides misst - die Zuordnung stammt von uns und ist aus Kapitel 7.2 und 7.3 begründet. B-Nummern zitieren das Konstrukt in Annex B der ISO/IEC 27004:2016; CWS-Nummern sind unsere eigenen. „Plus n weitere“ heißt: das Konstrukt trägt weitere abgeleitete Verhältnisse - abgedruckt ist das führende. Zielwerte fehlen bewusst, die Begründung folgt nach der Liste. Diese Gruppe: wie das Managementsystem selbst ausgestattet, gesteuert, auditiert und korrigiert wird.

ART DER MESSGRÖSSE	DIE FORMEL, IN EINER ZEILE	WAS DIE ZAHL AUSSAGT
B.2 LEISTUNG	**Zugewiesene Mittel geteilt durch genutzte Mittel, je Budgetposten, über eine Budgetperiode**	Ob die für Sicherheit budgetierten Mittel tatsächlich genutzt wurden und wo nicht
B.3 LEISTUNG	**In der Periode überprüfte Richtlinien geteilt durch geltende Richtlinien, in Prozent**	Ob Richtlinien im geplanten Intervall oder nach wesentlicher Änderung überprüft werden
B.4 LEISTUNG	**Durchgeführte Managementbewertungen geteilt durch geplante · plus 1 weitere**	Ob die oberste Leitung an den ihr obliegenden Managementbewertungen teilnimmt
B.5 WIRKSAMKEIT	**Anzahl hoher und mittlerer Risiken oberhalb des Akzeptanz-Schwellenwerts · plus 1 weitere**	Wie viel Risiko oberhalb des akzeptierten Niveaus liegt und ob es bearbeitet wird
B.6 LEISTUNG	**Durchgeführte Audits geteilt durch geplante Audits, in Prozent**	Ob das geplante Auditprogramm umgesetzt wurde
B.7 LEISTUNG	**Maßnahmen, die Zeit, Kosten und Qualität einhalten, geteilt durch in der Periode fällige Maßnahmen**	Ob Verbesserungsmaßnahmen termin-, kosten- und anforderungsgerecht abschließen
B.8 WIRKSAMKEIT	**Summe der Kosten aller Sicherheitsvorfälle der Periode, dann der Mittelwert je Vorfall und Kategorie**	Was fehlende Sicherheit kostet, Periode für Periode
B.9 LEISTUNG UND WIRKSAMKEIT	**Sicherheitsvorfälle mit ausgelöster Verbesserungsmaßnahme geteilt durch alle Sicherheitsvorfälle**	Ob Sicherheitsvorfälle etwas verändern oder nur geschlossen werden
B.10 LEISTUNG	**Nicht umgesetzte Maßnahmen geteilt durch bis dato geplante Maßnahmen · plus 2 weitere**	Ob Korrekturmaßnahmen wie geplant abschließen und ob Verzug begründet ist

Menschen und Zugang

Schulungsabdeckung und -aktualität, wie Menschen sich im Test verhalten, und wer noch Rechte hat, die er nicht haben sollte.

ART DER MESSGRÖSSE	DIE FORMEL, IN EINER ZEILE	WAS DIE ZAHL AUSSAGT
B.11 LEISTUNG	**Geschulte Beschäftigte in ISMS-Rollen geteilt durch die zu Schulenden · plus 1 weitere**	Wie viel Belegschaft eine Sensibilisierungsschulung hatte und wie aktuell diese ist
B.12 LEISTUNG	**Beschäftigte mit diesjähriger Sensibilisierungsschulung geteilt durch alle im Anwendungsbereich**	Erfüllung der Pflicht zur jährlichen Sensibilisierungsschulung
B.13 LEISTUNG	**Beschäftigte mit Unterschrift geteilt durch die bis dahin vorgesehenen, plus der Trend**	Ob Beschäftigte die Sensibilisierungsschulung abschlossen und die Nutzervereinbarung zeichneten
B.14 WIRKSAMKEIT	**Geprüfte mit bestandenem Wissenstest zu den Kampagnenthemen geteilt durch die Stichprobe**	Ob die Inhalte einer Sensibilisierungskampagne verstanden wurden
B.15 WIRKSAMKEIT	**Klicks geteilt durch Getestete, niedriger ist besser, dann gewichtete Summe der Raten · plus 2 weitere**	Ob Beschäftigte auf einen simulierten Social-Engineering-Versuch richtig reagieren
B.16 LEISTUNG	**Richtlinienkonforme Passwörter geteilt durch registrierte Passwörter, gegen den Vorwert**	Ob die genutzten Passwörter die Richtlinie erfüllen, per Prüfung festgestellt
B.17 LEISTUNG UND WIRKSAMKEIT	**Im Testbudget nicht geknackte Passwörter geteilt durch alle Passwörter, als Trend gelesen**	Wie viele Passwörter einem automatisierten Knackversuch standhalten
B.18 LEISTUNG	**Kritische Systeme mit periodischer Überprüfung der Zugriffsrechte geteilt durch alle kritischen Systeme**	Ob Zugriffsrechte auf kritischen Systemen systematisch überprüft werden

Gebäude, Lieferanten und unabhängige Überprüfung

Zutrittssteuerung und Instandhaltung, Sicherheitsanforderungen in Verträgen mit Dritten, und ob die geplanten Überprüfungen tatsächlich stattfinden.

ART DER MESSGRÖSSE	DIE FORMEL, IN EINER ZEILE	WAS DIE ZAHL AUSSAGT
B.19 LEISTUNG	**Ordinalskala des eingesetzten Zutrittsmechanismus, kumulative Stufen, kein Verhältnis**	Welcher Zutrittsmechanismus vorhanden ist und wie stark er ist
B.20 WIRKSAMKEIT	**Unbefugte Zutritte dieser Periode geteilt durch den Wert der Vorperiode, als Trend gelesen**	Ob physische Maßnahmen Unbefugte aus Gebäuden mit Systemen fernhalten
B.21 LEISTUNG	**Durchgeführte Ereignisse geteilt durch geplante Ereignisse, mit Abstand zwischen Soll- und Ist-Termin**	Ob geplante Wartung dann stattfindet, wann sie geplant war
B.31 LEISTUNG	**Mittlerer Anteil der abgedeckten geforderten Sicherheitsanforderungen je Vereinbarung**	Inwieweit geforderte Sicherheitsanforderungen in Verträgen mit Dritten stehen
B.32 LEISTUNG	**Abgedeckte geteilt durch geforderte Sicherheitsanforderungen, je Vereinbarung gemittelt, plus Trend**	Ob Vereinbarungen zu personenbezogenen Daten die geforderten Anforderungen tragen
B.36 LEISTUNG	**Durchgeführte unabhängige Überprüfungen geteilt durch geplante unabhängige Überprüfungen**	Ob die geplanten unabhängigen Überprüfungen der Sicherheit wirklich stattfinden
B.37 LEISTUNG	**Systeme mit gültigem Bewertungs- oder Penetrationstest-Datum geteilt durch alle Systeme im Bestand**	Wie viel des Bestands wirklich im Anwendungsbereich von Bewertung oder Penetrationstest liegt

Betrieb: Änderungen, Schadsoftware, Verfügbarkeit

Die größte Gruppe, auf zwei Seiten verteilt. Hier liegen in den meisten Organisationen bereits Daten vor - und werden falsch gelesen.

ART DER MESSGRÖSSE	DIE FORMEL, IN EINER ZEILE	WAS DIE ZAHL AUSSAGT
B.22 LEISTUNG	**Neuinstallationen mit Änderungs- und Härtungsnachweis geteilt durch Installationen der Periode**	Ob neue Systeme über das Änderungsmanagement und die Härtungsvorgabe eingeführt werden
B.23 WIRKSAMKEIT	**Sicherheitsvorfälle durch Schadsoftware geteilt durch abgewehrte Angriffe - Quote, kein Anteil**	Wie gut der Schutzverbund Schadcode stoppt, gemessen an dem, was durchkam
B.24 LEISTUNG	**Systeme mit veralteten Signaturen geteilt durch alle Systeme**	Wie viele Systeme veraltete Schadsoftware-Signaturen tragen
B.25 WIRKSAMKEIT	**Tatsächliche Ende-zu-Ende-Verfügbarkeit geteilt durch maximale Verfügbarkeit, ohne vereinbarte Ausfälle**	Ob jeder Dienst die zugesagte Verfügbarkeit erbringt
B.26 LEISTUNG	**Anzahl der Grenz-Firewallregeln ohne Treffer im Stichprobenzeitraum, Anzahl kein Verhältnis**	Wie viel des Grenz-Regelwerks toter Ballast ist

Betrieb: Protokolle, Konfiguration, Schwachstellen, Vorfälle

Die Nachweisspur, die Konfigurationsvorgabe dahinter, und ob Sicherheitsvorfälle bearbeitet werden und etwas verändern.

ART DER MESSGRÖSSE	DIE FORMEL, IN EINER ZEILE	WAS DIE ZAHL AUSSAGT
B.27 LEISTUNG	**Fristgerecht überprüfte Protokolldateien geteilt durch alle Protokolldateien im Anwendungsbereich**	Ob die zu überprüfenden kritischen Protokolldateien tatsächlich überprüft werden
B.28 LEISTUNG	**Korrekt konfigurierte Geräte geteilt durch alle Geräte, je Gerätetyp, sobald alles definiert ist**	Ob Geräte so konfiguriert bleiben, wie es die Richtlinie vorgibt
B.29 LEISTUNG	**Seit dem letzten Major-Release getestete kritische Systeme geteilt durch alle kritischen Systeme**	Ob kritische Systeme seit ihrem letzten Major-Release getestet wurden
B.30 WIRKSAMKEIT	**Schwerewert je offener Schwachstelle multipliziert mit betroffenen Systemen, dann aggregiert**	Wie viel ungepatchte Angriffsfläche der Bestand trägt
B.33 WIRKSAMKEIT	**Anzahl der Sicherheitsvorfälle über dem Lösungszielwert ihrer Kategorie, gegen den Schwellenwert**	Ob Sicherheitsvorfälle in der Zielzeit ihrer Kategorie gelöst werden
B.34 WIRKSAMKEIT	**Mittel der letzten zwei Perioden geteilt durch das Mittel der letzten sechs, gesamt und je Kategorie**	Wohin sich das Vorfallsaufkommen entwickelt, gesamt und je Kategorie
B.35 LEISTUNG	**Vom Reaktionsteam formal bearbeitete Ereignisse geteilt durch gemeldete Ereignisse der Periode**	Ob Sicherheitsereignisse überhaupt gemeldet und dann formal bearbeitet werden

CyberWerkSuite-Erweiterung, erste Hälfte

Zwölf Konstrukte für Gegenstände, für die es 2016 kein Messbeispiel gab: die elf Maßnahmen der ISO/IEC 27002:2022 und die Klimarelevanz-Feststellung, die 2024 mit Änderung 1 in die ISO/IEC 27001:2022 kam. Keines wird als ISO-Beispiel dargestellt.

ART DER MESSGRÖSSE	DIE FORMEL, IN EINER ZEILE	WAS DIE ZAHL AUSSAGT
CWS.1 LEISTUNG UND WIRKSAMKEIT	**Angebundene Quellen geteilt durch Quellen im Quellenregister · plus 1 weitere**	Ob benannte Quellen wirklich angebunden sind und ob Bedrohungsinformationen etwas ändern
CWS.2 LEISTUNG	**Erkannte Cloud-Dienste mit gültigem Inventareintrag geteilt durch alle erkannten · plus 4 weitere**	Ob jeder Cloud-Dienst bekannt und abgedeckt ist und Abgänge sauber abgeschaltet wurden
CWS.3 WIRKSAMKEIT	**Im Wiederherstellungsziel wiederhergestellte kritische Dienste geteilt durch getestete · plus 3 weitere**	Ob kritische Dienste wirklich in ihren Wiederherstellungszielen wiederherstellbar sind
CWS.4 LEISTUNG UND WIRKSAMKEIT	**Kritische Bereiche mit laufend überwachter Detektion geteilt durch kritische Bereiche · plus 1 weitere**	Ob Räume mit Systemen überwacht werden und ob jemand auf den Alarm reagiert
CWS.5 LEISTUNG	**Werteklassen mit Konfigurationsvorgabe geteilt durch Werteklassen im Anwendungsbereich · plus 2 weitere**	Ob die Konfigurationsvorgabe das Installierte abdeckt und wie schnell Abweichungen behoben werden
CWS.6 LEISTUNG	**Sensible Datenarten mit dokumentiertem Entsorgungsverfahren geteilt durch alle · plus 1 weitere**	Ob jede sensible Datenart ein Entsorgungsverfahren hat und ob Daten gelöscht werden

CyberWerkSuite-Erweiterung, zweite Hälfte

Maskierung, Datenabfluss, Überwachung, Filterung, sichere Entwicklung und die Klimarelevanz-Feststellung.

ART DER MESSGRÖSSE	DIE FORMEL, IN EINER ZEILE	WAS DIE ZAHL AUSSAGT
CWS.7 LEISTUNG	**Vor Bereitstellung maskierte/pseudonymisierte Nichtproduktivdaten geteilt durch die im Anwendungsbereich**	Ob Produktivdaten nur maskiert in Test- und Analyseumgebungen gelangen
CWS.8 LEISTUNG	**Werte mit aktiven, justierten Abflussmaßnahmen geteilt durch Werte im Anwendungsbereich · plus 1 weitere**	Ob Werte mit sensiblen Daten abgedeckt sind und ob die Alarme lesenswert sind
CWS.9 WIRKSAMKEIT	**In der Zielzeit triagierte Alarme geteilt durch Alarme, je Schweregrad · plus 2 weitere**	Ob Ereignisse zentral auflaufen, zeitgerecht triagiert und Schwellenwerte justiert sind
CWS.10 LEISTUNG	**Werte mit erzwungener Webfilterung geteilt durch Werte im Anwendungsbereich · plus 2 weitere**	Ob Endgeräte und Netze die Webfilterung wirklich nutzen und wer sie umgeht
CWS.11 LEISTUNG	**Vorhandene Prozessbausteine geteilt durch die in Ihrer Richtlinie definierten · plus 3 weitere**	Ob ein Prozess sicherer Entwicklung besteht, Entwickler geschult und Code geprüft werden
CWS.12 LEISTUNG	**Binär ja oder nein: in der Kontextanalyse erfasst, plus Monate seit der letzten Überprüfung**	Ob die Klimarelevanz bestimmt und erfasst und Anforderungen dazu aufgenommen wurden

CWS
CYBERWERKSUITE

ISMSSuite

ein Werkzeug von **CyberWerkSuite** · die ISO/IEC-27001-Ausgabe von NIS2**Suite**

DIE ISO/IEC-27001:2022-AUSGABE DER CYBERWERKSUITE-PLATTFORM

Die Liste, die Sie gerade gelesen haben - im Betrieb.

Eine Liste von Formeln ist nur dann ein Anfang, wenn etwas sie rechnet. Hier laufen diese achtundvierzig: jede mit dem Zielwert, den Sie setzen, ihrer Häufigkeit, ihrem Verantwortlichen und ihrer Nachweisquelle - und die Ergebnisse laufen in die Managementbewertung statt in eine Tabelle, für die sich niemand zuständig fühlt.

Maßnahmenbewertung

Über 300 bewertbare Maßnahmen, abgebildet auf die 93 des Anhangs A — einmal bewertet, mit dem Attributschema von 2022, berechnetem Schweregrad der Lücken und Reifegrad, und der Begründung hinter jeder Bewertung.

Anwendbarkeitserklärung

Ein lebendes SoA, das mit der Bewertung und dem Risikobehandlungsplan synchron bleibt — das Dokument, nach dem der Prüfer zuerst fragt.

Richtlinien-Generator

Prüffähige Richtlinien auf Deutsch und Englisch, aus Ihren eigenen Antworten erzeugt, auf Klauselebene, als PDF und Word exportierbar.

Risiko-Engine

Risiken aus echten Lücken abgeleitet, in einer konfigurierbaren Matrix bewertet, mit Behandlungsentscheidung, Verantwortlichem und Frist bis zum Abschluss.

Messung nach Kapitel 9.1

Diese achtundvierzig Messgrößen eingebaut, jede mit dem Zielwert, den Sie setzen, ihrer Häufigkeit, ihrem Verantwortlichen und ihrem Nachweis — die Ergebnisse fließen in die Managementbewertung, nicht in eine Folie.

Paket für die Managementbewertung

Die Eingaben nach Kapitel 9.3 zusammengestellt: Leistungstrends, Nichtkonformitäten, Auditergebnisse und Zielerreichung, vorstandsreif mit einem Klick.

Internes Audit

Auditprogramm, Feststellungsregister und Korrekturmaßnahmen — der Kreis, der den Nachweis das ganze Jahr aktuell hält.

Mehrere Normen

Ein Maßnahmenkatalog, mehrere Pflichten: ISO/IEC 27001:2022, NIS2 und die Durchführungsverordnung aus derselben Nachweisbasis bewertet.

300+	93	48	DE / EN
Bewertete Maßnahmen	Maßnahmen in Anhang A	Messgrößen	Zweisprachig

Die ISO-27001-Ausgabe auf cyberwerksuite.com

Bewertung · SoA · Richtlinien · Messung · Managementbewertung
Auch als 40-stündiges CISE-Programm verfügbar

MADE IN GERMANY

Gründlich, verlässlich — und bereit, lange bevor der Prüfer fragt.

CyberWerkSuite

cyberwerksuite.com

„Wir haben Kennzahlen“ ist nicht „wir messen“

In fast jedem Audit kommt der Moment, in dem die Kennzahlenfolie auf den Tisch kommt. Zehn Prozentzahlen, acht davon grün. Dann kippt eine Frage das Ganze.

Über welchen Zeitraum, und was steht im Nenner?

Die Frage, die die meisten Kennzahlenpräsentationen beendet

- Die Antwort ist selten eine Zahl. Meistens ist es ein Satz, der mit „das zieht sich das System automatisch“ beginnt.
- Und er endet mit der Feststellung, dass zwei Auswertungen desselben Quartals unterschiedlich ausfallen.

Nicht falsch — sondern nicht entscheidbar

WARUM DAS SCHWERER WIEGT ALS GENAUIGKEIT

Eine Kennzahl, die nicht nachgerechnet werden kann, ist keine schlechte Kennzahl, sie ist keine. Ein Prüfer kann sie nicht bestätigen, und die Geschäftsleitung kann auf ihrer Grundlage nichts beschließen. Kapitel 9.1 verlangt, dass gemessen wird; es sagt nicht, was. Die Liste, die Sie gerade gelesen haben, ist das, was wir messen - und warum.

Eine Messgröße ist entschieden, wenn Zeitfenster, Zähleinheit und Akzeptanzregel aufgeschrieben sind - in dieser Form, vor der ersten Erhebung.

Das Zeitfenster und die Zähleinheit

Zwei der vier Fallstricke betreffen die Rechnung. Sie wirken kleinlich - bis eine Zahl zum ersten Mal aus dem falschen Grund wandert.

Das Zeitfenster

FALLSTRICK 1

„Anteil der Systeme mit aktuellem Patchstand“ ist keine Messgröße, solange nicht feststeht, **wann** gezählt wird: Stichtag, Monatsdurchschnitt oder rollierende dreißig Tage. Dieselbe Umgebung liefert drei verschiedene Prozentwerte. Alle drei sind richtig. Keiner ist mit den anderen vergleichbar, und niemand merkt es.

Die Zähleinheit

FALLSTRICK 2

Zähler und Nenner müssen dieselbe Einheit zählen, abgeglichen über dieselbe Kennung. Anbieter A liefert neun Cloud-Dienste unter einem aktuellen Vertrag, Anbieter B einen unter einem veralteten. **Anbieterbasiert** beträgt die Aktualität 1/2 = 50 %. **Dienstbasiert** beträgt sie 9/10 = 90 %. Beide sind legitim. Keine ist eine Fassung der anderen — und wer sie vertauscht, berichtet eine Verbesserung, die es nicht gab.

Dieselben Daten, zwei Urteile. Die Einheit wird schriftlich festgelegt, vor der ersten Erhebung, nicht nach dem ersten Ergebnis.

Die Null, die keine Null ist

Die anderen beiden Fallstricke betreffen die Bedeutung. Sie sind es, die unbeschadet bis in die Managementbewertung gelangen und dort den Schaden anrichten.

„0 %“ kann heißen	Was es tatsächlich ist	Wie es berichtet wird
Gemessen und tatsächlich null	**Ein Ergebnis**	0 %, mit Angabe der Grundgesamtheit
Die Grundgesamtheit gibt es hier nicht	**Nicht anwendbar**	not_applicable — weder 0 % noch 100 %, und nie grün
Es wurde nichts erhoben	**Nicht bewertet**	not_assessed — ein Eingeständnis, keine Bewertung
Grundgesamtheit vorhanden, kein Ereignis im Fenster	**Nicht ausgelöst**	not_triggered — die Maßnahme wurde nicht beansprucht

Leistung ist nicht Wirksamkeit

FALLSTRICK 4 — KAPITEL 7.2 GEGEN 7.3

„98 % der Mitarbeitenden haben die Schulung abgeschlossen“ ist Leistung. Ob sie im Phishing-Test anders handeln, ist Wirksamkeit. Beides ist legitim, und beides beantwortet verschiedene Fragen. Der Fehler ist nicht, die falsche zu messen — sondern nur die erste zu messen und das Sicherheit zu nennen. Jede Messgröße in der Liste ist als das eine, das andere oder beides gekennzeichnet.

Kopieren Sie keinen Schwellenwert

Ein Band, das in einem Dokument für jemand anderen steht, misst jemand anderen. Es ist der am häufigsten kopierte und am schlechtesten verteidigbare Teil jedes Messprogramms — deshalb gibt diese Liste Ihnen die Formeln und nicht die Bänder.

1

Erst messen, dann banden

Erheben Sie eine Ausgangsmessung, bevor Sie einen Schwellenwert setzen. Ein Band vor der ersten Messung ist ein Wunsch; ein Band nach dem ersten Ergebnis ist eine Verhandlung.

2

Banden Sie die Grundgesamtheit, um die es geht

Ein Band über einen gemischten Bestand verdeckt genau die Systeme, für die Sie die Messgröße gebaut haben. Banden Sie nach Kritikalitätsklasse und berichten Sie die Klassen getrennt.

3

Akzeptanzregel getrennt vom Zielwert halten

Der Zielwert sagt, wo Sie hinwollen. Die Akzeptanzregel sagt, was als bestanden gilt. Das sind nicht derselbe Satz, und ihre Verwechslung ist der Weg, auf dem aus einer Toleranz still ein Zielwert wird.

4

Den Schwellenwert am Rohwert prüfen

Gerundet wird nur für die Anzeige. Ein Ergebnis, das bei derselben gedruckten Zahl je nach Rundung besteht oder durchfällt, ist keine Messung, sondern eine Münze.

Ein Verhältnis ist nur so ehrlich wie seine Regeln

Ein Regelsatz, auf jede Messgröße der Liste angewandt, gemeinsam mit den Ergebnissen veröffentlicht. Ohne ihn ist jede Zahl strittig, und jeden Streit gewinnt der Ranghöhere.

Regel	Was sie in der Praxis bedeutet
Zeitfenster	**Die Periode wird angegeben. Jeder Posten wird einmal gezählt, über eine eindeutige Kennung.**
Teilmenge	**Bei Abdeckungs- und Erfolgsverhältnissen ist der Zähler eine Teilmenge der Nenner-Grundgesamtheit. Trends, Quoten und nicht normalisierte gewichtete Summen sind die Ausnahmen und dort gekennzeichnet, wo sie vorkommen.**
Leerer Nenner	**Gar keine Grundgesamtheit bedeutet not_applicable. Eine vorhandene Grundgesamtheit ohne Ereignis im Fenster bedeutet not_triggered. Nichts erhoben bedeutet not_assessed. Keines der drei ist 0 % oder 100 %, und keines ist grün.**
Rundung	**Der Schwellenwert wird am Rohwert geprüft; gerundet wird nur für die Anzeige.**
Ausnahmen	**Jede Ausnahme trägt Grund, Verantwortlichen und Ablaufdatum. Eine Ausnahme ohne Ablaufdatum ist eine Entscheidung, die niemand getroffen hat.**
Herkunft	**Trennen Sie, was die Norm festlegt, was Ihre Lesart davon ist und was Ihr eigener Schwellenwert ist. Drei verschiedene Dinge, drei verschiedene Kennzeichnungen.**

Was gilt, und wie wir zitieren

Jede Aussage über den Stand einer Norm trägt das Datum ihrer Prüfung, denn die Antwort ändert sich ohne Ankündigung.

ISO/IEC 27004:2016 ist die geltende Ausgabe

ZWEITE AUSGABE · KEINE ÄNDERUNG, KEINE BERICHTIGUNG VERÖFFENTLICHT

Geprüft am 13. September 2026. Eine dritte Ausgabe ist als ISO/IEC DIS 27004 in Arbeit und **nicht veröffentlicht**. Arbeiten Sie mit der Ausgabe von 2016 und bauen Sie Ihr Programm so, dass jede Messgröße eine Verweiszeile auf ISO/IEC 27002:2022 trägt — dann bedeutet eine neue Ausgabe, die Verweise zu prüfen, und nicht, das Programm neu zu bauen.

Annex B ist informativ

EINE FESTSTELLUNG ZUR KONFORMITÄT, KEIN URHEBERRECHTSARGUMENT

Er enthält Messbeispiele, keine verpflichtenden Kennzahlen. Verpflichtend ist Kapitel 9.1: dass gemessen wird — nicht, dass genau diese Größen gemessen werden. Jeder Satz der Form „ISO verlangt 36 Kennzahlen“ ist falsch, und im Audit kostet er Glaubwürdigkeit.

Wie wir zitieren

UNSERE EIGENE REDAKTIONELLE REGEL

Konstruktnummern und Klauselverweise sind Zitate. Jede Formel und jede Zeile der Auslegung in dieser Ausgabe ist CyberWerkSuite-Formulierung; den Text des Annex geben wir nicht wieder. Für die Norm selbst brauchen Sie ein eigenes Exemplar, von ISO, IEC, DIN Media oder Ihrem nationalen Normungsinstitut. Die zwölf CWS-Messgrößen sind unsere eigenen und als solche gekennzeichnet.

CWS
CYBERWERKSUITE

Messung

Von der Kennzahl zum Nachweis

Messung nach Kapitel 9.1, eingebaut in das System, das den Nachweis erzeugt — und vermittelt an die Menschen, die sie betreiben müssen.

SIE HABEN DIE LISTE. DIE ARBEIT KOMMT DANACH

Achtundvierzig Formeln sind der leichte Teil. Die Bänder zu setzen, die Zähleinheiten zu vereinbaren und die Zahlen im Raum zu verteidigen, ist die Arbeit.

✓ **Certified ISMS Expert (CISE)**	Vierzig Stunden ISO/IEC-27001:2022-Umsetzung an Ihrer eigenen Organisation — GAP-Analyse, Risikoarbeit nach ISO 27005, die 93 Maßnahmen, die Anwendbarkeitserklärung, dann Messung nach Kapitel 9.1 und internes Audit
✓ **Umsetzung und Auditbegleitung**	Wir führen die GAP-Analyse, schreiben die Dokumente und definieren die Messgrößen mit Ihnen — und sitzen am Tag des Audits neben Ihnen
✓ **ISMSSuite**	Über 300 bewertbare Maßnahmen auf den 93 des Anhangs A, ein lebendes SoA, erzeugte Richtlinien, eine Risiko-Engine — und diese Messgrößen in der Managementbewertung

Für Menschen, die Nachweise liefern müssen und nicht Meinungen

Sprechen Sie uns an · das Erstgespräch ist kostenfrei

cyberwerksuite.com/trainings

ODER SIE FÜHREN ES SELBST — SCHRITT FÜR SCHRITT

ISMSSuite

cyberwerksuite.com

Bewertung, SoA, Richtlinien, Risiko und **Messung nach Kapitel 9.1** in einem System.

Messen Sie, was Sie ändern wollen — und können Sie es zeigen.