VORLAGE ZU ABSCHNITT 4.1 DES BANDES 5B

Die Kette des Zertifikats

Sechs Fragen in einer Viertelstunde: ob Stelle, Akkreditierung und Zertifikat nachprüfbar sind, bevor ein Angebot gelesen oder ein Papier aufgehängt wird.

Kategorie: Checkliste. Bezug im Buch: Abschnitt 4.1 (Das Prinzip, Prüffolge der sechs Fragen, Operative Synthese); Norm: Klauseln 4.1, 4.2, 5.1, 7.5, 8.1, 9.2 und 9.3 der ISO/IEC 27001:2022 mit Änderung 1:2024; Regeln der Zertifizierung nach ISO/IEC 17021-1 und ISO/IEC 27006-1:2024. Rechtsstand des Bandes: 28. September 2026.

Haus / Standort		**Ausgefüllt von**	
Zertifizierungsstelle		**Zertifikatsnummer**	
Land (DE / AT / CH)		**Stichtag**	

So nutzen Sie diese Vorlage

1. Prüfen Sie die Stelle, bevor Sie das Angebot lesen, nicht danach. Ein Angebot einer nicht akkreditierten Stelle ist ein Angebot für eine andere Leistung und gehört nicht in denselben Vergleich.
2. Gehen Sie die Prüffragen 1 bis 6 in ihrer Reihenfolge durch: sechs Fragen, sechs Antworten, alle nachprüfbar, alle vor dem ersten Euro. Ein fehlender Eintrag ist ein Anlass zur Nachfrage beim Aussteller und bei der Akkreditierungsstelle, noch kein Urteil.
3. Lesen Sie danach, was Ihre Auftraggeber anerkennen (Frage 8): Prüfen Sie nicht nur, was Sie kaufen.

Spalte «Im Buch»: verlangt = von Norm, Regelwerk oder Recht verlangt, wie der Band es nennt (Quelle in Klammern); Methode = Vorgehen dieses Bandes, keine Anforderung.

1 Anwendung in Schritten

Nr.	Schritt	Grund (aus dem Band)	Im Buch
1	Das eigene Zertifikat hervorholen und die ausstellende Stelle im Verzeichnis der nationalen Akkreditierungsstelle suchen.	Eine Viertelstunde, heute. Das Papier selbst stellt die Frage nach der Aufsicht über die Stelle nie.	Methode dieses Bandes
2	Den Geltungsbereich der Akkreditierung lesen und die Zertifikatsnummer in der öffentlichen Datenbank abfragen; bei fehlendem Treffer beim Aussteller nachfragen.	Nicht jede Stelle und nicht jedes Akkreditierungssystem nutzt die Datenbank; ein fehlender Eintrag ist kein Beweis.	Methode dieses Bandes
3	Den Geltungsbereich des eigenen Systems gegen die Anforderungen der wichtigsten Auftraggeber halten; wo er zu eng ist, die Erweiterung mit der Stelle besprechen.	Im Lübecker Gegenfall war nur der Serverraum zertifiziert; die Kette sagt nicht, ob das Richtige geprüft wurde.	Methode dieses Bandes
4	Die Bedingungen der drei größten Firmenkunden lesen: Was erkennen sie als Nachweis an?	Große Auftraggeber nennen die Anerkennung durch eine nationale Akkreditierungsstelle ausdrücklich in ihren Bedingungen.	Methode dieses Bandes
5	Ablaufdatum des Zertifikats und Laufzeit der Akkreditierung im Dokumentenverzeichnis führen, mit jährlicher Wiedervorlage.	Akkreditierungen können auch während der Laufzeit eines Zertifikats ausgesetzt oder zurückgezogen werden.	Methode dieses Bandes (Anker Klausel 7.5)

2 Prüffragen in der Reihenfolge des Abschnitts

Nr.	Frage	Befund	Grund (aus dem Band)	Im Buch
1	Steht die Stelle im Verzeichnis der nationalen Akkreditierungsstelle eines Landes, mit Nummer und Geltungsbereich?	☐ ja ☐ nein ☐ offen	Ein Zertifikat darf jede Gesellschaft ausstellen; entscheidend ist, wer die ausstellende Stelle überwacht.	Methode dieses Bandes (Prüffolge 1); je Mitgliedstaat nur eine Stelle: Verordnung (EG) Nr. 765/2008, Art. 4
2	Umfasst der Geltungsbereich ihrer Akkreditierung die Informationssicherheit?	☐ ja ☐ nein ☐ offen	Eine Akkreditierung gilt für bestimmte Normen und Programme; eine Stelle kann für Qualitätsmanagement akkreditiert sein und nicht für Informationssicherheit.	Methode dieses Bandes (Prüffolge 2)
3	Weist er, soweit das Akkreditierungssystem Wirtschaftszweige ausweist, das Beherbergungsgewerbe aus; und kann die Stelle andernfalls die Kompetenz ihres Teams für Hotels belegen?	☐ ja ☐ nein ☐ offen	Die fehlende Nennung ist für sich kein Mangel des Zertifikats, wohl aber ein Anlass, nach Branchenerfahrung und Kompetenz des Teams zu fragen.	Methode dieses Bandes (Prüffolge 3)
4	Gehört die Akkreditierungsstelle für das betreffende Programm den internationalen Vereinbarungen an (Mitgliederliste)?	☐ ja ☐ nein ☐ offen	Über diese Vereinbarung werden Akkreditierungen zwischen Ländern anerkannt. Die Organisation auf dem Siegel kann ein privates Unternehmen sein, das ihr nicht angehört. Seit dem 1. Januar 2026 nimmt Global ACI die Aufgaben von IAF und ILAC wahr; bereits ausgestellte Zertifikate werden dadurch nicht ungültig.	Methode dieses Bandes (Prüffolge 4)
5	Lässt das Angebot erkennen, wie die Auditzeit nach ISO/IEC 27006-1 berechnet wurde?	☐ ja ☐ nein ☐ offen	Die Zahl der angebotenen Auditage ist eine aufschlussreiche Kennzahl, sofern das Angebot die Berechnungsgrundlage erkennen lässt.	verlangt: Auditzeit nach ISO/IEC 27006-1:2024, Anhang C; die Frage: Methode dieses Bandes

Nr.	Frage	Befund	Grund (aus dem Band)	Im Buch
6	Ist die Stelle von jeder Beratung getrennt, die dasselbe System betroffen hat, auch über verbundene Unternehmen?	☐ ja ☐ nein ☐ offen	Wer ein Managementsystem schreibt und wer es prüft, dürfen nicht dieselbe Gesellschaft sein; sonst prüft am Ende jemand seine eigene Arbeit. Es gilt eine Sperrfrist für Stellen, die dasselbe System zuvor beraten haben.	verlangt (Regeln für Zertifizierungsstellen, ISO/IEC 17021-1)
7	Lässt sich die Zertifikatsnummer in der öffentlichen Datenbank abfragen?	☐ ja ☐ nein ☐ offen	Soweit die Stelle das Zertifikat dort eingestellt hat; ein fehlender Eintrag ist Anlass zur Nachfrage beim Aussteller, kein Beweis.	Methode dieses Bandes
8	Nennen die Bedingungen Ihrer Auftraggeber die Anerkennung durch eine nationale Akkreditierungsstelle?	☐ ja ☐ nein ☐ offen	Wer diese Bedingungen vor der Beauftragung liest, kauft einmal richtig. In Vergabeunterlagen kann ein nicht akkreditiertes Zertifikat zum Ausschluss des Angebots führen.	Methode dieses Bandes; Anforderung des Auftraggebers: Klauseln 4.1 und 4.2 (interessierte Partei)
9	Deckt der Geltungsbereich des zertifizierten Systems (zweite Zeile des Zertifikats) ab, was der Auftraggeber geprüft sehen will?	☐ ja ☐ nein ☐ offen	Die Kette beantwortet, ob die Prüfung etwas wert war, nicht ob das Richtige geprüft wurde. Ein begrenzter Geltungsbereich ist zulässig, wenn er genau benannt ist.	Methode dieses Bandes

3 Häufige Fehler

Nr.	Häufiger Fehler	Was der Abschnitt dazu sagt	Bei uns
1	Zertifikat und Anerkennung verwechselt	Das Wort «Zertifikat» ist nicht geschützt, die Ausstellung ist in keinem der drei Länder erlaubnispflichtig. Was zählt, ist die Aufsicht über die ausstellende Stelle.	☐ trifft zu ☐ nicht zu
2	Das Siegel	Es ist größer als der Name der Stelle und wirkt wie die Autorität. Wer es nachschlägt, findet oft private Gesellschaften, die Akkreditierungen gegen Gebühr vergeben und von niemandem überwacht werden.	☐ trifft zu ☐ nicht zu
3	Das Komplettpaket	Beratung und Zertifizierung aus einer Hand: Das Ergebnis steht vor dem ersten Auditag fest. Dieselbe Adresse auf Beratungsvertrag und Zertifikat ist genug gesehen.	☐ trifft zu ☐ nicht zu
4	Der Preis als Vorteil	Vierzehntausend Euro für Beratung und Zertifizierung mit zwei Auditagen lagen erheblich unter den Kosten allein der Zertifizierung bei einer akkreditierten Stelle. Wer zwei Tage anbietet, muss erklären können, wie er sie berechnet hat.	☐ trifft zu ☐ nicht zu
5	Die Geschwindigkeit	Sechs Wochen bis zum fertigen System. Keine Norm nennt eine Mindestdauer; entscheidend ist, was bis zur Prüfung gelaufen ist: Aufzeichnungen, internes Audit (9.2), Managementbewertung (9.3). Ein System ohne Geschichte ist eine Behauptung.	☐ trifft zu ☐ nicht zu
6	Die Gegenseite nie geprüft	Das Zertifikat wurde achtzehn Monate in Ausschreibungen verwendet, ohne zu prüfen, ob die Empfänger es anerkennen.	☐ trifft zu ☐ nicht zu
7	Das gute Gewissen	Zugriffsrechte ehemaliger Mitarbeitender nicht entzogen, Sicherungen nie zurückgespielt, Vertrag ohne Regelung über Unterauftragnehmer. Ein Zertifikat bescheinigt nicht, dass ein Haus sicher ist; ein nicht tragendes beendet die Aufmerksamkeit.	☐ trifft zu ☐ nicht zu

4 Die Rechnung hinter der Auditzeit (Beispiel aus Abschnitt 4.1)

Rechenschritt	Ihr Haus	Beispiel aus Abschnitt 4.1
Ausgangspunkt: Zahl der Personen unter der Kontrolle der Organisation für den Anwendungsbereich, gleich ob angestellt oder nicht		rund hundertzwanzig Beschäftigte
Begründete Anpassungen, etwa für Komplexität, Auslagerung und Standorte		mehrere Verarbeitungen mit Gastdaten; ausgelagerter IT-Betrieb
Auditzeit nach der Berechnung der Stelle (ISO/IEC 27006-1:2024, Anhang C), beide Stufen zusammen, in Auditortagen		Größenordnung sechs bis acht Auditortage; im Fall des Abschnitts umfasste das Angebot sechseinhalb Auditage in zwei Stufen
Umrechnung: Zahl der Auditoren × Tage im Haus = Auditortage; die Kalendertage sind die Tage im Haus		zwei Auditoren, drei Tage im Haus: sechs Auditortage, drei Kalendertage

Die Zeitvorgaben der Akkreditierungsregeln für Qualitäts-, Umwelt- und Arbeitsschutzmanagementsysteme sind für die Informationssicherheit nicht die Grundlage. Die Modellannahme ist weder eine Mindestzahl noch ein Maßstab, an dem sich ein Angebot für unzulässig erklären ließe; die verbindliche Zahl steht in der Berechnung der Stelle. Liegt ein Angebot weit darunter, etwa bei zwei Tagen, müsste es diese Berechnung offenlegen. Rechtsstand des Bandes: 28. September 2026.

Was diese Vorlage nicht ist

Diese Vorlage ist kein Rechtsrat und ersetzt weder die ISO/IEC 27001 noch die Regeln der Zertifizierung (ISO/IEC 17021-1, ISO/IEC 27006-1) noch das Recht, das für Ihr Haus gilt. Sie beurteilt nicht, ob ein bestimmtes Zertifikat oder eine bestimmte Stelle anerkannt wird; das entscheiden Akkreditierungsstelle und Auftraggeber. Ein ausgefülltes Blatt ist kein Nachweis, sondern der Anlass, ihn zu holen. Die Rechnung in Abschnitt 4 ist ein Rechenbeispiel und kein Angebot; maßgeblich bleibt die Berechnung der Zertifizierungsstelle nach ISO/IEC 27006-1. Rechtsstand des Bandes: 28. September 2026.