Voraussetzungen der Stichprobe bei mehreren Standorten

Die Bedingungen, unter denen eine Gruppe ein Zertifikat für mehrere Standorte tragen darf, und das interne Auditprogramm, das die äußere Stichprobe verdienen muss.

Kategorie: Prüfliste. Bezug im Buch: Abschnitt 4.13 (Multi-Site-Zertifizierung für eine Hotelgruppe); Norm: Klauseln 4.3, 5.3, 8.1, 9.2 und 9.3 sowie Maßnahmen des Anhangs A (Fassung 2022) der ISO/IEC 27001:2022 mit Änderung 1:2024, in den eigenen Worten des Buches. Rechtsstand des Bandes: 28. September 2026.

Gruppe / Gesellschaft		**Ausgefüllt von**	
Zentralfunktion (Ort)		**Datum**	
Zertifizierungsstelle		**Zahl der Standorte im Anhang**	

So nutzen Sie diese Vorlage

1. Prüfen Sie zuerst die Zulässigkeit (Teil 1), dann die Bedingungen der Steuerung (Teil 2 und 3), zuletzt die Standorte (Teil 4). Fehlt eine der Voraussetzungen in Teil 1, ist die Stichprobenbildung nicht zulässig, und die Häuser brauchen eigene Verfahren.
2. Die Stichprobe der Stelle ist kein Rabatt, sondern ein Vertrauensvorschuss: Die Stelle prüft weniger, weil die Gruppe zusagt, alles selbst zu prüfen. Alles, was die Stelle wegen der Stichprobe nicht sieht, muss die Gruppe selbst sehen.
3. Die Rechnung dazu steht in der Excel-Datei zu diesem Abschnitt (Besuche im Zyklus, Kennzahl der nie besuchten Standorte). Dieses Blatt ist die Prüfliste dazu.

1 Die Voraussetzungen der Stichprobe

Frage	Antwort	Grund (aus dem Band)	Im Buch
Besteht eine rechtliche oder vertragliche Verbindung zwischen der Zentralfunktion und jedem Standort? ☐ ja ☐ nein		Bei mehreren Gesellschaften braucht die Zertifizierung auf einem Zertifikat eine vertragliche Verbindung, die der Zentralfunktion die nötigen Befugnisse gibt.	verlangt (Dokument der Akkreditierung über Multi-Site-Zertifizierung; 17021-1; 27006-1)
Besteht ein einziges Managementsystem, dem alle Standorte unterliegen, mit zentraler, gemeinsamer Managementbewertung? ☐ ja ☐ nein		Fehlt diese Voraussetzung, ist nicht die Stichprobe zu klein: Dann ist die Stichprobenbildung überhaupt nicht zulässig.	verlangt (wie oben; 9.3)
Hat die Zentralfunktion die Befugnis, das einheitliche Managementsystem festzulegen und aufrechtzuerhalten und an jedem Standort Korrekturmaßnahmen zu verlangen? ☐ ja ☐ nein		Eine Zentralfunktion ohne Befugnis erfüllt die Anforderung nicht, auch wenn sie die Zuständigkeit trägt.	verlangt (wie oben; 5.3)
Ist die Zentralfunktion nicht an Dritte ausgelagert? ☐ ja ☐ nein		Nach der Verifikationsnotiz des Abschnitts setzt die Stichprobenbildung insbesondere dies voraus.	verlangt (wie oben)
Unterliegen alle Standorte dem internen Auditprogramm der Organisation? ☐ ja ☐ nein		Das ist der Preis der äußeren Stichprobe und die Gegenleistung für die eingesparten Auditage (9.2).	verlangt (wie oben; 9.2)
Probe: Nennen Sie die letzte Änderung, die die Zentralfunktion an einem Standort gegen dessen Widerstand durchgesetzt hat.		Wer eine nennen kann, hat eine Zentralfunktion; wer keine nennen kann, hat entweder außergewöhnlich einige Häuser oder eine Stabsstelle.	Methode dieses Bandes

Die Zentralfunktion wird in jedem Verfahren auditiert (Erstzertifizierung, jedes Überwachungsaudit, jede Rezertifizierung); sie ist nie Stichprobe. Bedingungen, Fassung und Einzelheiten der Dokumente, auch einer möglichen Reduzierung in der Rezertifizierung, sind vor Anwendung zu prüfen.

2 Die Hebel der Zentralfunktion

Methode dieses Bandes: Die Zentralfunktion braucht mehr als Zuständigkeit, sie braucht Hebel. Vier genügen in der Praxis; wer sie hat, kann steuern, wer sie nicht hat, sammelt Berichte. Wo ein Standort verpachtet ist, müssen sie im Pachtvertrag stehen (Geltung der Gruppenverfahren, Duldung interner Audits, Meldepflichten, Mitwirkung bei Korrekturmaßnahmen); sonst ist der Standort im Anhang aufgeführt, aber nicht steuerbar (8.1).

Hebel	Vorhanden?	Beleg (Vertrag, Verfahren, Datum)
Vergabe von Systemzugängen	☐ ja ☐ nein	
Festlegung des Standards	☐ ja ☐ nein	
Mitspracherecht bei örtlichen Beschaffungen mit Systembezug	☐ ja ☐ nein	
Eskalationsweg zur Geschäftsführung mit Frist	☐ ja ☐ nein	

3 Das interne Auditprogramm: alle Standorte

Frage	Antwort	Grund (aus dem Band)	Im Buch
Stehen alle Standorte im internen Auditprogramm, nicht eine Auswahl, nicht die erreichbaren, nicht die mit Auffälligkeiten?		Multi-Site bedeutet nach außen Stichprobe und nach innen Vollständigkeit.	verlangt (9.2); Methode dieses Bandes

Frage	Antwort	Grund (aus dem Band)	Im Buch
Richtet sich der interne Audittermin jedes Saisonbetriebs nach dessen Öffnungszeit, nicht nach dem Kalender der Zentralfunktion?		Ein Berghotel wird im Februar oder im August auditiert, nicht im November. Wer das umdreht, produziert Vertagungen.	Methode dieses Bandes
Gilt für Vertagungen die Staffel: einmal vertagt, im selben Zyklus nachgeholt; zweimal vertagt, Chefsache; dreimal vertagt, eine Feststellung im eigenen System?		Vertagung ist zulässig, darf aber nicht folgenlos bleiben.	Methode dieses Bandes
Wird die Zahl der Standorte, die im laufenden Zyklus weder intern noch extern besucht wurden, in der Managementbewertung genannt?		Eine Bewertung, die das verschweigt, verschweigt die wichtigste Zahl der Gruppe. Sie ist am Ende des Zyklus null.	verlangt (9.3); Kennzahl: Methode
Hat jeder Standort, der einem Gruppenverfahren nicht folgen kann, eine dokumentierte Abweichung (was, warum, Risiko, Ersatzmaßnahme, Überprüfung)?		«Wir machen das oben anders» ist keine Abweichung, sondern ein zweites System im Entstehen.	Methode dieses Bandes

4 Die Standorte

Standort	Öffnungszeit (Monate)	Internes Audit (Monat)	Besuche extern im Zyklus	Vertagungen	Sonderweg / dokumentierte Abweichung

Methode dieses Bandes. Die Auswahlkriterien der Stelle, nach dem Band: ein Teil zufällig, der Rest nach Kriterien, zu denen Ergebnisse interner Audits, Beschwerden, Abweichungen, Unterschiede in Größe und Komplexität sowie Veränderungen seit dem letzten Audit gehören; über den Zyklus soll eine möglichst große Bandbreite abgedeckt werden. Ein Standort, der sich von allen anderen unterscheidet, ist ein Pflichtbesuch. Die Bitte an die Gruppe: Verlangen Sie, dass ein nie besuchter Standort gezogen wird; die Vorgaben lassen das ausdrücklich zu.

Veränderung im Bestand	Gemeldet am	Standort in die Stichprobe einbezogen
Standort hinzugekommen: _____		☐ gezielt besucht
Standort weggefallen: _____		

Methode dieses Bandes: Kommt ein Standort hinzu oder fällt einer weg, ist das der Zertifizierungsstelle zu melden; der neue Standort wird in die Stichprobe einbezogen und regelmäßig zunächst gezielt besucht. Wer in einem Zyklus zwei Häuser übernimmt und dies erst bei der Rezertifizierung erwähnt, hat den Anhang des eigenen Zertifikats unrichtig gemacht.

5 Anwendung in Schritten

Reihenfolge nach dem Band

1. **Zulässigkeit und Bedingungen der Stichprobe prüfen** (Teil 1). Fehlt eine Voraussetzung, sind eigene Verfahren nötig.
2. **Auswahl der Standorte:** zufällig und nach Risiko, mit begründeten Ersetzungen; vorher fragen, welche Standorte in den zurückliegenden Zyklen nie an der Reihe waren, und einen nie besuchten Standort setzen lassen.
3. **Auditzeit:** Sie folgt für ein Informationssicherheits-Managementsystem den Regeln der ISO/IEC 27006-1 und nicht einer allgemeinen Formel, auch nicht der Quadratwurzel der Standortzahl. Maßgeblich ist die Berechnung der Zertifizierungsstelle.
4. **Innen:** Alle Standorte ins interne Auditprogramm, Saisonbetriebe nach Öffnungszeit, Staffel für Vertagungen, für jeden Sonderweg eine dokumentierte Abweichung, die vier Hebel prüfen und wo nötig vertraglich herstellen.
5. **Überwachen:** Zahl der Standorte ohne Besuch im laufenden Zyklus (am Ende null); Zahl der dokumentierten Abweichungen je Standort, die zeigt, wo das System der Wirklichkeit nachgegeben hat.

6 Häufige Fehler

Stichprobe nach Zufall und Bequemlichkeit statt nach Risiko.	Bei acht Standorten und zwei bis drei Besuchen je Verfahren kann ein Standort auch bei korrekter Auswahl über Jahre ungezogen bleiben; die Deckung dieser Lücke liegt in erster Linie bei der Gruppe.
Eine Zentralfunktion, die sammelt und verteilt, aber nichts durchsetzt.	Sie besteht dennoch jedes Audit, weil Verwaltung sich gut prüfen lässt.
Ein gemeinsames System, das keines ist: sieben Häuser nach denselben Verfahren, eines nach eigenen.	Dann ist die Stichprobenbildung nicht zulässig.
Ein internes Auditprogramm, das dreimal vertagt wurde.	Eine dreimal verschobene Prüfung ist eine Lücke mit Aktenzeichen.
Ein Ausnahmeweg, der nie als Abweichung erfasst wurde.	Lösungen, die funktionieren, werden nicht berichtet; Sonderwege bleiben unsichtbar, bis sie schiefgehen.
Saisonpersonal, das die Zentralfunktion nicht kennt.	Sie kann weder Zugänge verwalten noch Schulungen nachweisen noch beim Ausscheiden etwas entziehen. Anmeldung, Unterweisung, Verschwiegenheitsverpflichtung und Entzug gehören an den Saisonkalender gebunden.
Berichterstattung wird mit Überwachung verwechselt.	Die Monatszahlen stammten aus derselben Tabelle wie der Sonderweg und bestätigten ihn, statt ihn aufzudecken.

Rahmen laut Buch (Rechtsstand des Bandes: 28. September 2026.): Betreiben mehrere Gesellschaften die Häuser, ist jede für die Daten ihrer Gäste verantwortlich, die zentrale Reservierung ist insoweit Auftragsverarbeiterin, bei gemeinsamer Entscheidung über Zwecke und Mittel kommt eine gemeinsame Verantwortlichkeit mit eigener Vereinbarung in Betracht. Datenschutz: Für die Übermittlung personenbezogener Daten über offene Netze ist Verschlüsselung Stand der Technik. Österreich (Melderecht): Anmeldung binnen vierundzwanzig Stunden, Gästeverzeichnis sieben Jahre, für jeden Beherbergungsbetrieb eigenständig.

Was diese Vorlage nicht ist

Diese Vorlage ist kein Rechtsrat und ersetzt weder die ISO/IEC 27001 noch das verbindliche Dokument der Akkreditierung über Multi-Site-Zertifizierung, ISO/IEC 17021-1 oder ISO/IEC 27006-1. Sie wählt keine Standorte aus und rechnet keine Auditzeit: Auswahl und Auditzeit bestimmt die Zertifizierungsstelle nach den im Apparat des Bandes genannten Regeln. Ein ausgefülltes Blatt ist kein Nachweis: Es wird erst einer, wenn jeder Standort tatsächlich besucht wurde, intern oder extern.