

Remote-Audits

1. Ziel und Zweck

Diese Anweisung enthält Regelungen zur Nutzung von Informations- und Kommunikationstechnologie (ICT) im Rahmen von Prüfungen, vor allem für Remote-Audits. Damit soll sichergestellt werden, dass bei Durchführung von Remote-Audits vergleichbare Ergebnisse wie bei Präsenzaudits erzielt werden.

Die Fassung berücksichtigt die Anforderungen des IAF MD 4:2022.

2. Geltungsbereich

Sofern bestimmte Dienstleistungen in Punkt 8 nicht explizit ausgenommen sind, gilt diese Anweisung für alle Prüfungen im Rahmen der ISO/IEC 17021, ISO/IEC 17065, ISO 14065 sowie für Prüfungen nach EfbV, sofern in diesen Prüfungen die Anwendung von Remote-Audit-Techniken vorgesehen wird.

3. Zuständigkeiten

Die Verantwortung für die Festlegung von allgemeinen Regelungen zur Nutzung von ICT liegt bei der Leitung der Zertifizierungsstelle.

Für die korrekte Berücksichtigung möglicher Remote-Audits im Rahmen der Angebotserstellung und ersten Auditprogrammerstellung ist der jeweilige Projektbearbeiter verantwortlich.

Der jeweilige Auditleiter ist zuständig für die wirksame Umsetzung der hier beschriebenen Regelungen im Audit sowie die anforderungsgerechte Dokumentation von Auditablauf und -ergebnissen.

4. Beschreibung

Remote-Audits sollen Vor-Ort-Audits ersetzen, unter Verwendung von technischen Hilfsmitteln zur Erfassung von Informationen, Befragung einer auditierten Organisation usw., wenn Methoden von Angesicht zu Angesicht nicht möglich oder nicht erwünscht sind. Die Auditzeit von Remote-Audits zählt immer als Vor-Ort-Zeit.

Remote-Audits können sowohl vom Büro des Auditors (oder einer anderen geeigneten Örtlichkeit) aus oder aber auch von einem Standort der auditierten Organisation aus durchgeführt werden.

Diese Regelung schließt prinzipiell auch die Verwendung von ICT in den Fällen ein, in denen diese durch den Kunden selbst betrieben und für Begutachtungszwecke zur Verfügung gestellt werden (z.B. eine vorhandene Videoüberwachung in Lagerhallen). In diesen Fällen ist der Auditleiter für die konkrete Umsetzung im Audit verantwortlich. Falls dabei Zweifel bezüglich der Wirksamkeit für Auditzwecke entstehen, ist die Leitung der Zertifizierungsstelle zu informieren, die dann über das weitere Verfahren entscheidet.

4.1. Risikobewertung

Für jedes Managementsystem wird durch den Fachleiter eine allgemeine Risikobewertung für den Einsatz von Remote-Audit-Techniken erstellt. Im Ergebnis wird festgestellt, in welchem zeitlichen Umfang Remote-Audit-Techniken bei der Auditierung je Standort ohne eine gesonderte individuelle Risikobewertung zulässig sind.

Falls der Auditleiter einen höheren Anteil an Remoteauditzeit nutzen möchte, ist dafür eine individuelle Risikobewertung mit FL162 erforderlich. Dabei werden v.a. die Themen und Aspekte bewertet, die in der allgemeinen Risikobewertung mit einem erhöhten Risikopotenzial aufgeführt wurden.

Dazu füllt der Auditleiter das FL162 aus, die Bewertung erfolgt dann durch den jeweiligen Fachleiter.

4.2. Angebotserstellung

Im Rahmen der Angebotserstellung wird die prinzipielle Möglichkeit von Remote-Audits durch die Zertifizierungsstelle gemeinsam mit dem Anfrager besprochen. Falls aus Sicht des Anfragers Interesse an der Nutzung von Remote-Audit-Techniken besteht und keine wesentlichen Hinderungsgründe bestehen (z.B. Vertraulichkeitsanforderungen, Fehlen der technischen Voraussetzungen), wird die Möglichkeit von Remoteaudits im Angebot erwähnt und im weiteren Verfahren berücksichtigt.

4.3. Antragsprüfung

Mit dem Antrag FL052 gibt der Kunde an, ob er mit der Nutzung von Remote-Audit-Techniken einverstanden ist. Dazu muss er angeben, ob die Voraussetzungen für deren Nutzung vorhanden sind:

- ausreichende Internetanbindung an den jeweiligen Standorten/Einrichtungen
- Vorhandensein der notwendigen Hardware (Videokonferenzsystem)
- Vorhandensein der notwendigen Software und deren Akzeptanz bzgl. Vertraulichkeitsanforderungen

Falls seitens des Kunden Videokonferenzsysteme oder andere Technik vorgeschlagen wird, die in der GUTcert nicht standardmäßig vorhanden sind, ist bei der Antragsprüfung eine Stellungnahme der internen IT dazu einzuholen.

Das Ergebnis der Antragsprüfung bzgl. der Nutzung von Remote-Audit-Techniken wird dokumentiert, dem Kunden mitgeteilt und in der Planung des Auditprogramms berücksichtigt.

4.4. Auditplanung- und Durchführung

Nach Antragsprüfung ernennt die Zertifizierungsstelle ein entsprechend qualifiziertes Auditteam. Die Auditoren/Bewerter und andere beteiligte Personen (z.B. Drohnenpiloten, technische Experten) müssen über die Kompetenz und Fähigkeit verfügen, die eingesetzten Informations- und Kommunikationstechnologien zu verstehen und zu nutzen, um die gewünschten Ergebnisse der Audit(s)/Bewertung(en) zu erzielen.

Der verantwortliche Auditleiter plant dann auf Basis des Auditprogramms die weiteren Auditaktivitäten. Durch die Sammlung weiterer detaillierter Informationen zum Kunden kann dabei eine Neubewertung der Risiken und Chancen der geplanten Verwendung von Remote-Audit-Techniken im Audit notwendig werden. Gegebenenfalls ist dann auch eine Anpassung des geplanten Auditprogramms notwendig, das erfolgt in enger Absprache mit der Zertifizierungsstelle und dem Kunden und ist angemessen zu dokumentieren. Zu berücksichtigen sind dabei auch die Risiken durch die Übertragung von ggf. sensiblen Daten bei einzelnen TOPs im Rahmen von Remote-Prüfungen.

Im Rahmen der konkreten Planung des Audits durch Auditleiter und Kunde muss sichergestellt werden, dass die vorhandene Technik auf beiden Seiten kompatibel ist und eine ungestörte Durchführung von Remote-Audits ermöglicht. Gegebenenfalls muss diese vor dem Audit getestet werden, um technische Probleme zu erkennen und beheben zu können.

Die geplante Verwendung von ICT ist im Auditplan je TOP mit Angabe der jeweiligen Technik zu dokumentieren.

Die Dokumentation der Auditergebnisse erfolgt auf dem üblichen Weg. Der Auditleiter muss im Auditbericht auf die Verwendung von ICT hinweisen und eine Aussage zur Wirksamkeit deren Nutzung machen.

5. Allgemeine Hinweise für remote-Audits

5.1. Risikobetrachtung zur Nutzung von ICT, speziell für Remote-Audits

Nachfolgend sind Anwendungsmöglichkeiten für die Nutzung von ICT im Rahmen von Remote-Audits und deren allgemeines Risikoniveau aufgeführt:

- a) Anwendbarkeit sehr gut, Risiko gering:
Interviews oder Besprechungen, die üblicherweise in einem Meetingraum stattfinden und bei denen Präsentationen vorgestellt und Dokumente geprüft werden.
- b) Anwendbarkeit sehr gut, Risiko gering:
Einsichtnahme in Daten aus Datenbanken o.ä., auch mit Auswahl und Prüfung von Stichproben innerhalb der IT-Tools.
- c) Anwendbarkeit mäßig, Risiko gering:
Einsichtnahme in vorhandene Papierdokumente mittels Kamera bzw. Scanner (mit anschließender Übermittlung).
- d) Anwendbarkeit mäßig bis schlecht, Risiko mittel:
Rundgänge mit Video-Übertragung, Begutachtung der Anordnung von Anlagen/-teilen und sonstigen Einrichtungen.
- e) Anwendbarkeit schlecht, Risiko mittel bis hoch:
Begutachtung von Produkten in der Fertigung mit Stichprobennahme.
- f) Anwendbarkeit schlecht, Risiko hoch:
Interviews mit Produktionsarbeitern (die den Umgang mit Videokonferenz nicht gewohnt sind).

5.2. Für welche Auditteile sind Remote-Audits generell nicht geeignet?

- a) Interviews mit Mitarbeitern, bei denen die Beobachtung nonverbaler Signale wichtig ist.
- b) Prüfungen, bei denen neben Sehen und Hören weitere Sinne angesprochen werden (z.B. Temperaturempfinden, Zugluft, Tastsinn für Rauigkeiten) oder bei denen durch die Übertragung leicht Verfälschungen auftreten können (Begutachtung Beleuchtung, Farben etc.).
- c) Wenn Anforderungen an die Vertraulichkeit durch Remote-Techniken nicht erfüllt werden können.

5.3. In welchem Umfang können Remote-Techniken in Audits genutzt werden

- a) Der mögliche Remote-Anteil, der ohne individuelle Risikobewertung geplant werden kann, ist im Anhang durch den jeweiligen Fachleiter festgelegt.
- b) Falls dieser im Einzelfall überschritten werden soll, ist gemäß 4.1 eine individuelle Risikobewertung erforderlich.
- c) Es sind Fälle denkbar, in denen bis zu 100% der Auditzeit remote durchgeführt wird, z.B. bei Organisationen ohne physische Standorte (also nur virtuelle nach IAF MD 1). Das wären allerdings absolute Ausnahmen.
- d) Remote-Audits sind ein gutes Mittel, um Reiseaufwände zu reduzieren und so auch Umweltbelastungen durch das Audit zu verringern.

- e) Weiterhin sind sie geeignet, um audiovisuellen Zugang zu sehr abgelegenen oder gefährlichen Orten zu erlangen.

5.4. In welchen Verfahren existieren Einschränkungen bzw. Sonderregelungen für Remote-Audits

- a) Alle Verfahren bei denen behördliche Anforderungen andere Vorgaben haben.
- b) Im Rahmen von ISO 50001-Zertifizierungen kommen generell nur Standorte mit geringer Energielebensdauer (z.B. kleine Bürostandorte, Vertriebsbüros) für ein Remote-Audit in Betracht. An diesen Standorten sollte zudem auch kein wirksames Personal in Hinblick auf das Managementsystem ständig tätig sein.
- c) Bei Audits nach ISO 45001 ist der Einsatz von ICT im Allg. nicht geeignet, um Prozess- und Risikosteuerung zu auditieren. (Dies beinhaltet unter anderem die Beobachtung und Kontrolle der Einhaltung von Vorschriften, Verfahren, Regeln und Betriebsanweisungen, die die betriebliche Sicherheit gewährleisten. Sowie die Identifizierung, Bewertung und Minderung spezifischer Gefahren, um das Risiko von Unfällen zu reduzieren.) Besonders Gespräche mit einfachen Arbeitern oder anderen „nicht-Funktionsträgern“ liefern über ICT oft andere Ergebnisse als „an der Maschine“ und lassen nur bedingt Rückschlüsse über Körpersprache zu. Remote-Audits können daher im Allg. keine vor-Ort-Begehung und teilweise auch vor-Ort-Interviews nur eingeschränkt ersetzen. Besonders bei Erstzertifizierungen und wenn Standorte das erste Mal auditiert werden, ist davon auszugehen, dass eine vor-Ort-Begehung notwendig ist, um benötigte Informationen zu erlangen. Kann der Betriebsarzt nur remote interviewt werden, ist die Begründung zu dokumentieren.
- d) Bei Audits nach EfbV sind Remote-Audits ausgeschlossen, sobald es eine genehmigungspflichtige Anlage vor Ort gibt oder abfallwirtschaftliche Tätigkeiten ausgeübt werden. Remote-Audits sind nur unter bestimmten Voraussetzungen zulässig, bspw. Büros mit Dispositionstätigkeiten.
- e) Im Rahmen eines RSPO Audits sollten Remote-Audits nur nach Rücksprache mit dem RSPO erfolgen, da diese nicht explizit vom Standard vorgesehen sind.
- f) Bei Audits im Rahmen des Emissionshandels gelten die Vorschriften gem. Art 31 Akkreditierungs- und Verifizierungsverordnung sowie gem. EU-Guideline Kapitel 3.
- g) AZAV: Die Frage, ob Remote-Prüfungen ein Vor-Ort-Audit ersetzen können, ist immer eine Einzelfallentscheidung. Neben den in dieser Übersicht genannten Kriterien werden folgende Aspekte in die Bewertung mit einbezogen:
 - o Hat eine andere Stelle (z.B. Landesbehörden im Rahmen von Schulzulassungen, andere FKS, o.ä.) bereits die Räumlichkeiten geprüft?
 - o Sind die Räumlichkeiten in vorangegangenen Audits bereits durch GUTcert vor Ort geprüft worden?
 - o Hat der Anbieter von Schulungsstätten (z.B. Tagungsräume in Hotels) dokumentierte Mindeststandards an Seminarräume und ist somit von einer Einheitlichkeit der Räumlichkeiten an verschiedenen Orten auszugehen?
 - o Ist die Dokumentation der vor Ort durchgeföhrten Maßnahmen mit Remote-Techniken einzusehen?
 - o Standorte, in denen keine Gruppenmaßnahmen durchgeführt werden (z.B. Verwaltungstandorte), oder Räumlichkeiten für Einzelmaßnahmen bzw. Arbeitsvermittlungen, sind unabhängig von den oben genannten Kriterien für Remoteaudits geeignet.

6. Notwendige Kompetenzen für Auditoren

Wenn in Prüfungen der Einsatz von ICT erfolgen soll, müssen die dafür vorgesehenen Auditoren über die notwendige Kompetenz verfügen, um

- a) den Einsatz von ICT im Audit unter Berücksichtigung vorhandener Risiken zu planen,
- b) Auditfeststellungen mit Hilfe von ICT zu erarbeiten und
- c) die allgemeinen Anforderungen an das Audit (v.a. bzgl. Vertraulichkeit) auch bei der Nutzung von ICT zu erfüllen.

Auditoren, die eine Berufung für ISO 9001 EAC 31/2 oder 33 bzw. ISO 20000-1 oder ISO/IEC 27001 haben, benötigen keinen gesonderten Nachweis ihrer Kompetenz.

Für die Nutzung von ICT, die durch den Kunden bereitgestellt wird, reicht die Berufung als Auditor als Kompetenznachweis für a) und b) aus.

Als Nachweis für die Kompetenz nach c) dient der Abschluss des entsprechenden e-learning-Kurses der GUTcert.

Allgemeine Risikobewertung bzgl. Remote-Audits

In dieser Übersicht erfolgt eine allgemeine Bewertung der Risiken, die bei der Anwendung von Remote-Audit-Techniken bei der Auditierung von Managementsystemen auftreten können. Dabei wird von der Verwendung einer Video-Konferenztechnik (z.B. Teams oder Zoom) im Remoteaudit ausgegangen.

In dieser Liste werden für jedes einzelne Normelement

- die üblicherweise eingesetzten Auditmethoden erfasst,
- das mit den Auditmethoden verbundene Risiko bei der Anwendung von Remote-audit-Techniken bewertet,
- Aspekte und Themen dokumentiert, bei denen bei Verwendung von Remote-Audit-Techniken ein erhöhtes Risiko für die Wirksamkeit des Audits besteht.
- Dann erfolgt eine Gesamtbewertung, in welchem zeitlichen Umfang die Einbeziehung von Remote-Audit-Techniken in die Auditierung je Standort möglich ist, ohne dass eine gesonderte individuelle Risikobewertung erforderlich ist.

Auditmethoden:

1. Prüfung von Dokumenten
2. Interview/Befragungen von Personen
3. Beobachtung von Tätigkeiten
4. Inaugenscheinnahme von Betriebseinrichtungen
5. Stichprobennahme
6. Technische Prüfungen

Risikobewertung:

gering: Effizienz und Wirksamkeit des Audits wird durch die Verwendung von Remote-Audit-Techniken nur sehr wenig beeinflusst; es ist nicht zu erwarten, dass das Auditergebnis durch die Verwendung von Remote-Audit-Techniken beeinflusst wird.

mittel: Effizienz und Wirksamkeit des Audits können durch die Verwendung von Remote-Audit-Techniken in einem überschaubaren Ausmaß beeinflusst werden; die Erreichung des Auditziels kann durch die Verwendung von Remote-Audit-Techniken in einem überschaubaren Maß beeinflusst werden.

hoch: Effizienz und Wirksamkeit des Audits können durch die Verwendung von Remote-Audit-Techniken wesentlich beeinflusst werden; die Erreichung des Auditziels kann durch die Verwendung von Remote-Audit-Techniken stark beeinflusst werden.

Managementsysteme nach DIN EN ISO 9001

Normelement	Audit-methoden	Risikobewertung bzgl. Remoteaudits	Aspekte/Themen mit erhöhtem Risikopotenzial bzgl. Remoteaudit
Kontext und MS	1, 2	gering	
Oberste Leitung, Politik	1, 2	gering	
Verantwortung und Befugnisse	1, 2	gering	
Risiken und Chancen	1, 2	gering	
Q-Ziele	1, 2	gering	
Änderungen MS	1, 2	gering	
Ressourcen, Infrastruktur	1, 2, 4	mittel	- Infrastruktur, Anlagen
Messmittel	1, 2, 3, 4, 5	hoch	- Ressourcen für Messungen und Prüfungen - Status von Prüf- und Betriebsmitteln
Personal, Wissens-management	1, 2, 3, 5	mittel	- Kenntnisse der Mitarbeiter und ggf. Externer zum Managementsystem
Kommunikation	1, 2	gering	
dokumentierte Information	1, 2, 4	mittel	- Verfügbarkeit dokumentierter Informationen am Arbeitsplatz
Planung	1, 2	gering	
Anforderungen an Produkte	1, 2, 5	gering	
Entwicklung	1, 2, 5	gering	
Beschaffung	1, 2, 3, 4, 5	hoch	- Eingangsprüfung für externe Zulieferungen - Steuerung ausgelagerter Leistungen
Produktion	1, 2, 3, 4, 5, 6	hoch	- Prozesssteuerung - Kennzeichnung des Status von Produkten einschl. Rückverfolgbarkeit - Umgang mit Kundeneigentum - Umgang mit (Zwischen-) Produkte (Handhabung, Lagerung, Transport)
Freigabe, fehlerhafte Produkte	1, 2, 3, 4, 5, 6	hoch	- Umgang mit nichtkonformen Produkten
Datenanalyse und -bewertung	1, 2	gering	
internes Audit	1, 2	gering	
Managementreview	1, 2	gering	
Verbesserung	1, 2	gering	

Gesamtbewertung:

Die Einbeziehung von Remote-Audit-Techniken in die Auditierung von Standorten nach DIN EN ISO 9001 ist bis zu einem Umfang von 50% der jeweiligen Auditzeit ohne eine gesonderte individuelle Risikobewertung möglich.

Datum: 15.01.2025

gez. Fachleiter QM: Andreas Lemke

Managementsysteme nach DIN EN ISO/IEC 27001

Normelement	Audit-methoden	Risikobewertung bzgl. Remoteaudits	Aspekte/Themen mit erhöhtem Risikopotenzial bzgl. Remoteaudit
Kontext und MS	1, 2	gering	
Oberste Leitung, Politik	1, 2	gering	
Verantwortung und Befugnisse	1, 2	gering	
A.I Organisation	1, 2	gering	
Risiken und Chancen	1, 2	gering	
Informationssicherheitsrisikobeurteilung	1, 2, 4, 5	hoch	- Bewertung vorhandener Risiken
Informationssicherheitsrisikobehandlung	1, 2, 4, 5	mittel	- Bewertung der Wirksamkeit umgesetzter Maßnahmen
Netzstrukturplan	1, 2	gering	
ISMS-Ziele	1, 2	gering	
Änderungen MS	1, 2	gering	
Ressourcen	1, 2, 4, 5	mittel	- Infrastruktur, Hardware
A.II Verwaltung der Werte	1, 2, 4, 5	hoch *)	- Vollständigkeit Werte-Inventar
Personal	1, 2, 3, 5	mittel	- Kenntnisse der Mitarbeiter und ggf. Externer zum Managementsystem
A.III Personalsicherheit	1, 2, 3, 5	mittel	- Einhaltung vorgegebener Regelungen
Kommunikation	1, 2	gering	
Dokumentierte Information	1, 2, 4	mittel	- Verfügbarkeit dokumentierter Informationen am Arbeitsplatz
A.IV Physische Sicherheit	1, 2, 3, 4, 5, 6	hoch	- Umsetzung technischer Anforderungen (Zutritt, Überwachung, Schutz vor phys. Bedrohungen, Schutz Übertragungswegs)
Betriebliche Planung und Steuerung	1, 2	gering	
A.V Zugangssteuerung	1, 2, 3, 4, 5, 6	hoch *)	- Umsetzung technischer Anforderungen (Zugang, Authentifizierung)
A.VI Betriebssicherheit	1, 2, 3, 4, 5, 6	hoch *)	- Umsetzung technischer Anforderungen (Schutz vor Schadsoftware, Umgang mit Speichermedien, Backup)

Normelement	Audit-methoden	Risikobewertung bzgl. Remoteaudits	Aspekte/Themen mit erhöhtem Risikopotenzial bzgl. Remoteaudit
A.VII Netzwerksicherheit	1, 2, 3, 4, 5, 6	hoch *)	- Umsetzung technischer Anforderungen (Netzwerkgeräte, Netzwerk-Infrastruktur)
A.VIII Entwicklung von Systemen	1, 2, 3, 5	gering	
A.IX Lieferanten-beziehungen	1, 2, 3, 4, 5, 6	mittel	- Umsetzung technischer Anforderungen (externe Zugänge für Dienstleister) - Eingangsprüfung für externe Hardware-Zulieferungen
A.X Business Continuity Management	1, 2	gering	
Datenanalyse und -bewertung	1, 2	gering	
internes Audit	1, 2	gering	
Managementreview	1, 2	gering	
A.XI Compliance	1, 2	gering	
Verbesserung	1, 2	gering	
A.XII Informations-sicherheitsvorfälle	1, 2	gering	

*) für Systeme nicht physischer Art (z.B. Software, Cloud), für die ein Remotezugriff auf diese Systeme möglich ist, verringert sich das Risiko auf gering

Gesamtbewertung:

Die Einbeziehung von Remote-Audit-Techniken in die Auditierung von Standorten nach DIN EN ISO/IEC 27001 ist bis zu einem Umfang von 50% der jeweiligen Auditzeit ohne eine gesonderte individuelle Risikobewertung möglich.

Bei Standorten, bei denen physische Assets nur eine geringe Rolle spielen, ist eine Erhöhung des Remote-Anteils auf 70% möglich.

(Zurzeit gilt für die GUTcert noch die Akkreditierung nach DIN EN ISO/IEC 27006:2021, danach ist eine Überschreitung des Remote-Anteils von 30% nur mit Zustimmung der DAkkS möglich).

Datum: 15.01.2025

gez. Fachleiter QM: Andreas Lemke

Managementsysteme nach DIN EN ISO 45001

Normelement	Audit-methoden	Risikobewertung bzgl. Remoteaudits	Aspekte/Themen mit erhöhtem Risikopotenzial bzgl. Remoteaudit
Kontext und MS	1, 2	gering	
Oberste Leitung, Politik, Mitarbeiterbeteiligung	1, 2	gering	
Verantwortung, Befugnisse und Konsultation Mitarbeiter	1, 2	hoch	- Konsultation von Mitarbeitern (auch auf unteren Hierarchieebenen)
Risiken und Chancen, Gefährdungsermittlung	1, 2, 3, 4, 5	hoch	- Identifikation von Arbeitsplatzgefahren und Bewertung ihrer Schwere und Wahrscheinlichkeit.
SGA-Ziele	1, 2	gering	
Änderungen MS	1, 2	gering	
Ressourcen, Infrastruktur	1, 2, 4	hoch	- Infrastruktur, Anlagen - Sicherheits- und Notfallausrüstungen lassen sich nur vor Ort richtig zuordnen
Personal	1, 2, 3, 5	hoch	- Mitarbeiter auf unteren Hierarchieebenen - Kenntnisse der Mitarbeiter und ggf. Externer zum Managementsystem
Kommunikation	1, 2, 3, 5	mittel	
Dokumentierte Information	1, 2	gering	
Betriebliche Steuerung und Planung	1, 2, 3, 4, 5	hoch	- Verfügbarkeit dokumentierter Informationen am Arbeitsplatz - Prüfung der Einhaltung von Sicherheitsrichtlinien/Betriebsanweisungen - Arbeitserlaubnisse - Wartungsaufzeichnungen - Beobachtung von Arbeitspraktiken - Überwachung von Sicherheitsdokumentationen - Nutzung PSA - Inspektion physischer Sicherheitsmaßnahmen
Beschaffung	1, 2, 3	mittel	- Eingangsprüfung für externe Zulieferungen - Steuerung ausgelagerter Leistungen - Beobachtung externes Personal
Notfallvorsorge, Gefahrenabwehr	1, 2, 4, 5	hoch	- Inaugenscheinnahme von Überwachungs- und Alarmsystemen, Fluchtwegen - Sicherheits- und Notfallausrüstungen lassen sich nur vor Ort richtig zuordnen
Datenanalyse, -bewertung, Compliance	1, 2, 5	hoch	- „gelebte“ Compliance
internes Audit	1, 2	gering	
Managementreview	1, 2	gering	
Verbesserung	1, 2, 4	mittel	- Wirksamkeitsprüfung auch von (Beinahe-)Unfällen mit Einbezug Mitarbeiter, ggf. Transferleistung auf ähnliche Arbeitsplätze

Gesamtbewertung:

Die Einbeziehung von Remote-Audit-Techniken in die Auditierung von Standorten nach DIN EN ISO 45001 ist bis zu einem Umfang von 35% der jeweiligen Auditzeit ohne eine gesonderte individuelle Risikobewertung möglich.

Datum: 04.04.2025

gez. Fachleiter SGA-MS: Seán Oppermann

