



Verhaltenstipps für Mitarbeitende

Dieses Handout soll Mitarbeitenden helfen, sich auf Gespräche mit externen Auditoren (z. B. ISO 27001) vorzubereiten. Es zeigt, wie man authentisch und professionell antwortet, ohne sich unter Druck zu setzen. Auditoren prüfen Prozesse – nicht Personen.

Warum sind diese Tipps wichtig?

Externe Auditoren haben wenig Vorlaufzeit und nutzen direkte und indirekte Fragen, um gelebte Prozesse zu verstehen. Ihre Neutralität schafft Objektivität, kann aber distanziert oder gar einschüchternd wirken. Souveränes Verhalten stärkt das Vertrauen in Ihr ISMS und den Audit-Erfolg.

Die 8 goldenen Verhaltensregeln im Audit

- » **Bleiben Sie authentisch.**
Beschreiben Sie, wie Sie im Alltag wirklich vorgehen – nicht die „perfekte“ Theorie. Ehrliche Antworten sind glaubwürdiger als auswendig gelernte Texte. Außerdem machen Auditoren ihren Job meist lange genug, um schnell zu merken was geschönt ist.
- » **Innehalten bei kniffligen Fragen.**
Nehmen Sie sich 2-3 Sekunden Zeit - der Auditor erwartet keine schnellen Antworten, sondern solche die zeigen, das Prozesse gelebt und das Thema verstanden wird.
- » **Nachfragen zeigt Stärke.**
Unklar? Fragen Sie nach: „Meinen Sie den Incident-Prozess oder die Dokumentation?“ Gute Auditoren erklären gerne ihr Ziel.
- » **Konkrete Beispiele nennen.**
Statt „Wir haben Schulungen“: „Im letzten Phishing-Test haben 95% auf die Testmail geklickt – danach folgten Awareness-Workshops.“ Praxisbeispiele überzeugen am meisten.
- » **Neutral und sachlich bleiben.**
Vermeiden Sie Rechtfertigungen („Das liegt am alten System“). Fokus auf Fakten und Lösungen: „Aktuell manuell, Automatisierung Q2 geplant.“
- » **Zeitmanagement respektieren.**
Antworten Sie präzise (1–2 Minuten). Vermeiden Sie lange Monologe mit häufigen Wiederholungen. Antworten Sie präzise und fragenbezogen. Der Auditor wird nachfragen, wenn er tiefer in das Thema einsteigen möchte.
- » **Vorfälle offen ansprechen.**
Sicherheitsvorfälle passieren, das weiß auch ein Auditor. Wichtig ist das Verbesserungen laufen und die Vorfälle analysiert werden. „Nach dem Vorfall X haben wir aufgrund der Analyse den Prozess Y angepasst“. Dies zeigt, dass ein ISMS umfassend eingeführt wurde und gelebt wird.

ISO



Verhaltenstipps für Mitarbeitende

Audit-Frageszenarien und Musterantworten

Situationen	Typische Auditorfragen	Souveräne Antwort
Incident-Response	„Letzter Vorfall - wie haben Sie reagiert?“	„Vor 3 Monaten Phishing: Gemeldet an ISB, System gescannt, Nutzer geschult.“
Zugriffs-kontrolle	„Fremdes Gerät im Netzwerk - was tun?“	„Gerät isolieren, IT-Sicherheit informieren, Incident-Prozess starten.“
Schulungen	„Wie wirken die getroffenen Maßnahmen?“	„Jährliche Tests: Letztes Jahr Erkennungsrate um 20% gestiegen.“
Kritische Fragen	„Warum haben Sie das nicht“ / „Warum fehlt...“	„Auf Basis der Bewertung/der Ressourcen/der Vorgaben wurde entschieden, Maßnahme X (noch) nicht umzusetzen. Die Umsetzung ist für xxx geplant.“

Vor dem Audit: Checkliste (5 Minuten)

- ☐ Verstehen Sie die Prozesse die Sie als Mitarbeiter aber ggf. auch in Ihrer gesonderten Rolle betreffen, kennen Sie die relevanten Richtlinien.
- ☐ Notieren Sie sich vorab Vorfälle oder Änderungen die Ihren Bereich betroffen haben
- ☐ Den Teil verstehe ich nicht, soll man sich austauschen wie das Audit läuft oder wie die Prozesse laufen ? Letzteres sollte man nicht erst kurz vor dem Audit tun...
- ☐ Atmen Sie durch, bewahren Sie Ruhe - Auditoren prüfen Unternehmensprozesse, nicht Sie als Person
- ☐ Lesen Sie den Auditbericht vom letzten Jahr, gab es dazu Veränderungen / Verbesserungen

Kontakt bei Fragen

Fügen Sie hier Ihren ISMS-Beauftragten ein...

Haben Sie Fragen oder möchten Sie beraten werden? Dann rufen Sie uns einfach unter 040 - 229 47 19 - 0 an oder schicken eine E-Mail an info@anmatho.de.