Sensibilisierung der Beteiligten für die Besonderheiten eines Audits

Know-how to go – ISMS-Zertifizierung

HiSolutions AG

Debora Röser

Debora Röser

Consultant

- Consultant bei HiSolutions
- Definition, Implementierung und Weiterentwicklung von vollumfänglichen Informationssicherheits-, Business Continuity- & Krisenmanagementsystemen
- Umsetzung von Anforderungen aus ISO/IEC 27001, IT-Grundschutz, ISO 22301 und BSI-Standards 200-1 und 200-4
- Planung, Durchführung und Nachbereitung von Notfall- und Krisenübungen

Agenda

Akteure

- Motivation
- Verantwortlich-keiten

Allgemeine Empfehlungen

- Arbeitsumgebung
- Arbeitsplatz

Nachweis-dokumentation

- Relevante Nachweise
- Bereichsspezifische Beispiele

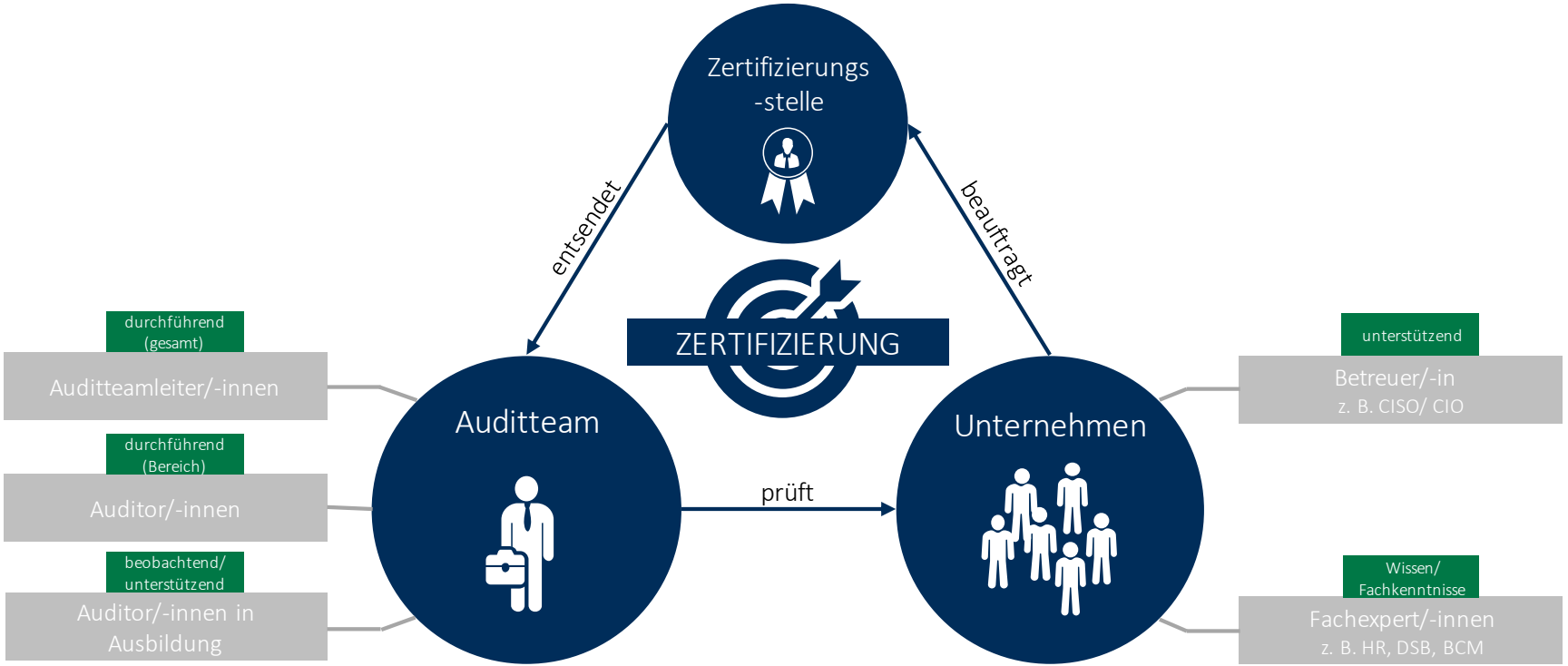
Verhaltensregeln und richtige Kommunikation

- Regeln für den Mitarbeitenden
- Regeln für den Auditor

Nachbereitung des Audits

- Nachreichen der Auditnachweise
- Nachbesserungen

Akteure und Verantwortlichkeiten innerhalb eines Audits



*Vorgehen ISO 27001

Vorbereitung auf ein Audit

Die personelle, infrastrukturelle und inhaltliche Vorbereitung auf ein Audit sind das A und O

"Gehe immer vom Besten aus, sei jedoch stets auf das Schlechteste vorbereitet."

Angemessen, aber nicht übertrieben auf das Audit vorbereiten

Arbeitsumgebung vorbereiten

- Verzeichnisse mit relevanter Dokumentation (Nachweisdokumente) geöffnet halten
- Papierordner mit Dokumentation in „Griffweite“ halten
- (korrekte) Anmeldung zu Administrationsumgebungen sicherstellen

Arbeitsplatz vorbereiten

- Anwendungen mit vertraulichen Inhalten bitte schließen – soweit nicht für das Audit benötigt
- Vertrauliche Unterlagen bitte wegschließen

Keine künstliche Testumgebung oder Testfälle einrichten.
Der Auditor möchte die Praxis sehen!

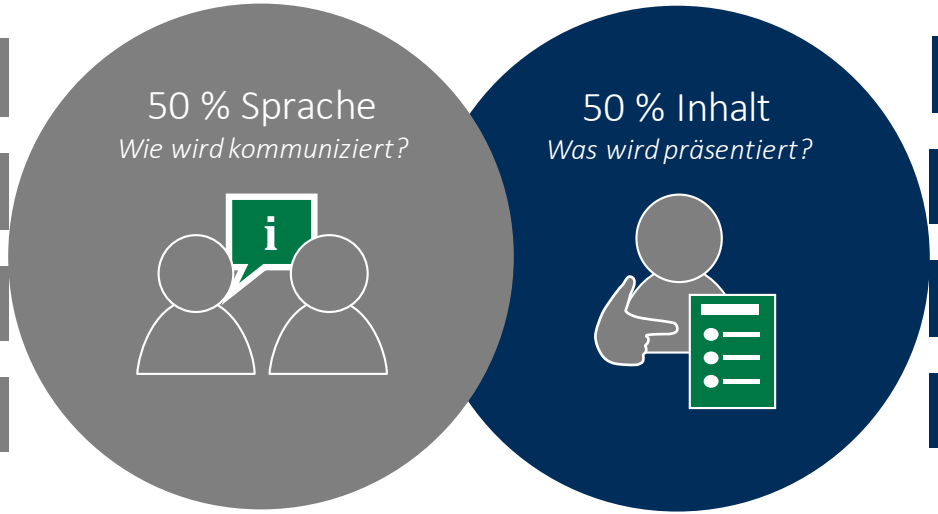
Mögliche Unterbrechungen und Verzögerungen im Vorfeld abschalten

- Zutritte für den Auditor einrichten/beantragen
- Erforderliche Kollegen informieren, sich eventuell für Informationen bereit zu halten
- Konkurrierende Termine absagen
- Konkurrierende Aufgaben (z. B. Regelaufgaben) verschieben oder delegieren
- Kollegen, Vorgesetzte und andere Mitarbeitende über die persönliche Nicht-Verfügbarkeit informieren

Der Auditplan des Auditors kann als Unterstützung bei der Vorbereitung herangezogen werden.

Auditerfolg mithilfe von Sprache und ausreichenden Evidenzen – Das Wichtigste aus fachlich und sprachlich

- Angemessene Kommunikation
- Engagement und Interesse zeigen
- Stimmige Argumentation
- Ehrlichkeit und Berücksichtigung geltender Regelungen



- Verfügbarkeit der Evidenzen
- Qualität der Evidenzen
- Umfang der Evidenzen
- Klassifizierung der Evidenzen

Auditnachweise als objektiver Nachweis, dass die überprüften Normforderungen entsprechend umgesetzt worden sind.

- Antworten mittels einer repräsentativen und verifizierbaren Sammlung von Auditnachweisen belegen
- Nachweise als einziges objektives Mittel gegen die subjektive Meinung des Auditors
- Grundsätzlich müssen alle Dokumentationen, die gezeigt werden, klassifiziert sein!

Wenn Sie aussagekräftige Unterlagen haben, zeigen und erläutern Sie diese.

Durchführung eines Audits

Mit Diplomatie und Überzeugung zum Ziel

Kommunizieren Sie angemessen und mit dem Auditor

Angemessene Kommunikation

+ Höflich und professionell
+ Freundliche/sachliche Aussagen
+ Durchatmen und nachdenken
+ Argumentationen versuchen nachzuvollziehen
+ Nachfragen, um Missverständnisse zu vermeiden
+ Kurze und prägnante Antworten

− Beleidigungen/Vorwürfe
− Etwas persönlich nehmen
− Mitarbeit verweigern
− Ausfällig/unverschämt werden
− Verallgemeinerungen
− Aufschieben und ignorieren
− Ungenauigkeiten und Konjunktive

Mit einer positiven Einstellung und Kooperation den Auditor überzeugen.

Engagement und Interesse zeigen

- Kein Desinteresse aufzeigen
- Anmerkungen des Auditors angemessen würdigen
- An den Auditor anpassen:
  - Wenn der Auditor schweigt, schweigen Sie auch.
  - Keine Antworten auf Fragen geben, die der Auditor nicht gestellt hat.
- Fragen nach bestem Wissen und Gewissen und mit gesundem Menschenverstand beantworten:
  - Wissen wer die Antworten auf die jeweiligen Fragen geben kann.
  - Ggf. Frage notieren und Nachlieferung der Antwort zusagen.
  - Nicht spontan online suchen oder etwas vorführen.
- Commitment zum eigenen Managementsystem

Angemessenheit und Wirksamkeit sind Trumpf.

Stimmige Argumentation

Bei Meinungsverschiedenheiten kein hartes Gegenargumentieren, sondern darlegen, wieso die Umsetzung wirksam und angemessen ist.

Schlagfertige Argumente:

Do`s

- Aussagen sachlich widerlegen
- Rückfragen stellen
- Begrenzte Zustimmung

Maybe

- Meta-Technik
- „Gerade weil“

Don´t

- Retourkutsche
- Verweigerung
- Übertriebene Komplimente
- Übergehen
- 2-Silben-Antworten

Das Audit soll ehrlich und sachlich geführt werden.

Ehrlichkeit und Berücksichtigung geltender Regelungen

- Nicht aus der Ruhe bringen lassen – an die geltenden Regelungen und Vorschriften halten:
  - Berücksichtigung geltender Regelungen für Benutzer
  - Berücksichtigung geltender Regelungen für den IT-Betrieb
- Das Audit ist keine Beschwerdeplattform
- Keine Lügen und Ausreden
- Kein „Fingerpointing“ betreiben

Denken Sie daran:
Der Auditor darf nicht alles.

- Der Auditor darf sich nicht alleine in zutrittsgeschützten Bereichen aufhalten oder bewegen. Begleiten Sie ihn stets.
- Der Auditor darf nicht selbstständig auf IT-Systeme zugreifen. Er muss benennen, was er sehen möchte, und Sie zeigen es ihm erst dann.
- Der Auditor darf vertrauliche Informationen einsehen. Teilen Sie diese Informationen jedoch nur auf Anfrage, und wenn ein Nachweis nicht anderweitig erbracht werden kann.

Zwei Arten von Auditoren!

Will Qualität verbessern

Will Fehler finden

Überlässt das WIE der Organisation

Drückt der Organisation eigenen Stempel auf

Nachbereitung eines Audits

Nach dem Wettkampf ist vor dem Wettkampf

Viele Unternehmen machen genau in dieser Phase entscheidende Fehler.

Nach dem Audit ist vor dem Audit: Kontinuierliche Verbesserung ist Pflicht

- Auditnachweise zeitnah nachreichen!
  - Die vereinbarten Auditnachweise schicken
  - Besprochene Dokumente, keine neueren oder korrigierten Versionen (soweit nicht mit dem Auditor vereinbart)
- Ein Zertifikat entbindet die Organisation nicht von ihrer grundsätzlichen Pflicht, die Sicherheitsprozesse innerhalb des ISMS weiterhin konsequent umzusetzen und kontinuierlich zu verbessern.
- Es muss der Nachweis erbracht sein, dass die Prozesse auch „gelebt“ werden.

Sicherheit ist kein einmaliges Projekt, sondern ein kontinuierlicher Prozess!

Haben Sie Fragen?

Schloßstraße 1 | 12163 Berlin

info@hisolutions.com | +49 30 533 289 0

www.hisolutions.com