

Zertifizierung nach ISO 27001

Herzlich Willkommen

13.01.2011



 **DEKRA**
DEKRA Certification

Inhaltsverzeichnis

Überblick an die Anforderungen zur Zertifizierung nach ISO 27001

- ⇒ Gründe für ein ISMS
- ⇒ Informationssicherheitsmanagementsystem (ISMS)
- ⇒ Die Struktur der ISO/IEC 27001
- ⇒ Allgemeine Anforderungen an ISMS nach 27001
- ⇒ Spezielle Anforderungskriterien (Anhang A)
- ⇒ Zertifizierungsverfahren

Gründe für ein ISMS

„Was soll bei uns schon zu holen sein, so geheim sind unsere Daten nicht.“

Diese Einschätzung ist in den meisten Fällen zu oberflächlich.

Was ist wenn Daten in falsche Hände geraten?

„Unsere Mitarbeiter sind vertrauenswürdig.“
Verschiedene Statistiken zeichnen ein
anderes Bild: Die Mehrzahl der Sicherheitsverstöße wird durch
Innentäter verursacht.

„Unser Netz ist sicher.“
Die Fähigkeit potentieller Angreifer werden oft unterschätzt.

„Bei uns ist noch nie etwas passiert.“ Diese Aussage ist
Mutig. Vielleicht hat bei früheren Sicherheitsvorfällen
niemand etwas bemerkt

Gründe für ein ISMS

Rechtliche Rahmenbedingungen

- Basel II
- Sarbanes-Oxley Act SOX
- KontrAG
- Datenschutz

- Konkurrenz
- Spionage
- Terrorismus

Physikalische Bedrohung

- Einbrecher & Diebe
- Vandalismus

Katastrophen

- Unwetter
- Blitzeinschlag
- Hochwasser
- Brand

Internet

- Viren & Würmer
- Hackerangriffe
- Unvorsichtiges Surfen

- Mitarbeiter
- Unwissenheit
- Leichtsinnigkeit
- Demotivation

Informationssicherheitssystem

Was ist Informationssicherheit?

Aufrechterhaltung der Vertraulichkeit, Integrität und Verfügbarkeit von Informationen, Werten unabhängig von ihrer Form. Dies umfasst sowohl schriftliche, bildliche als auch gesprochene Informationen.

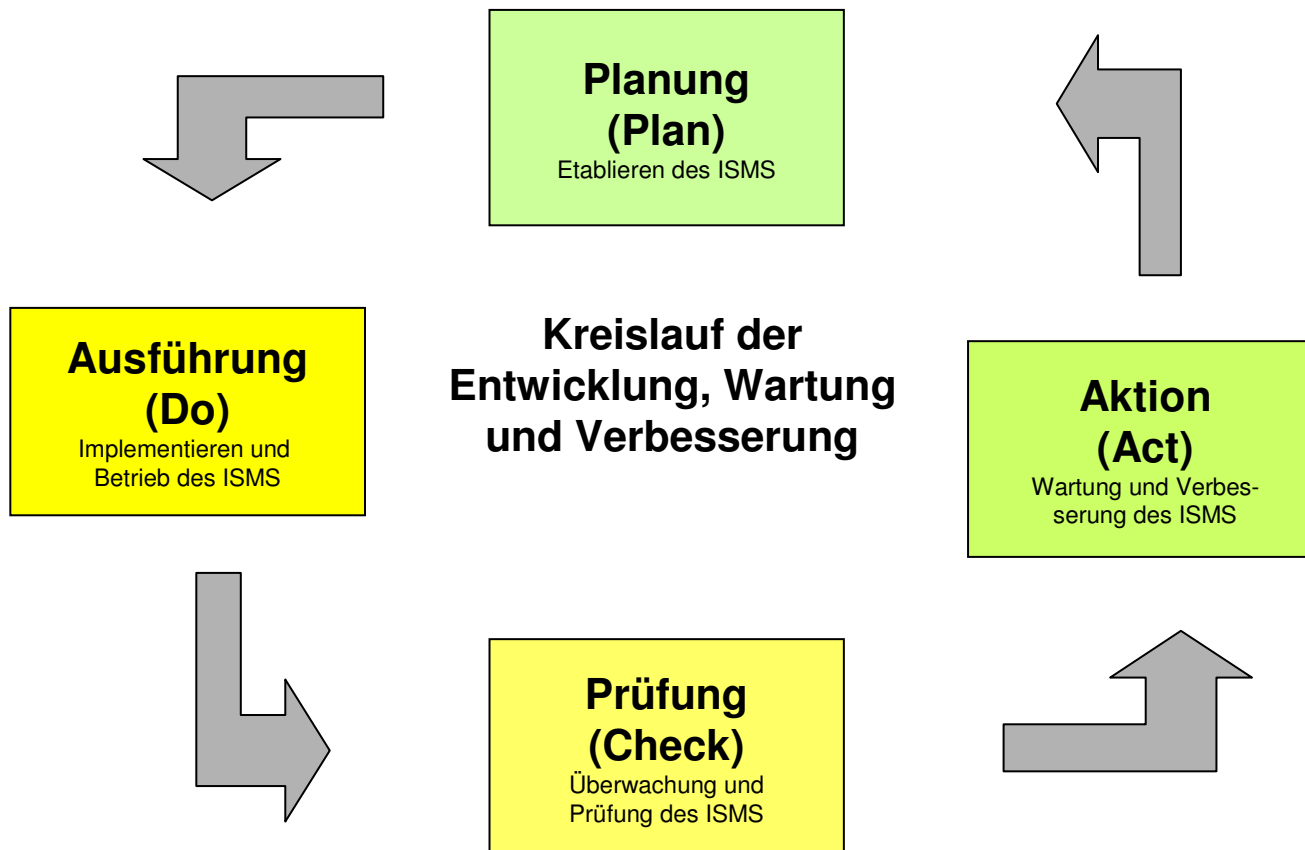
- Vertraulichkeit:** Eigenschaft dass Informationen unberechtigten Personen, Einheiten oder Prozessen nicht verfügbar gemacht oder enthüllt werden.
- Integrität:** Eigenschaft der Absicherung von Richtigkeit und Vollständigkeit von Werten.
- Verfügbarkeit:** Eigenschaft, einer berechtigten Einheit auf verlangen zugänglich und nutzbar zu sein.

Ziel der ISO/IEC 27001

Die ISO/IEC 27001 wurde als Modell für den Aufbau, die Verwirklichung Durchführung, Überwachung, Bewertung, Aufrechterhaltung und Verbesserungen eines Informationssicherheitsmanagementsystems ISMS erarbeitet.

Die ISO/IEC 27001 ist Prozessorientiert.
Die ISO 27001 basiert auf dem PDCA – Zyklus.
Die ISO 27001 hat große Übereinstimmung mit ISO 9001.

ISO/IEC 27001 / PDCA - Modell



Aufbau und Inhalte der ISO 27001

Die ISO/IEC 27001 besteht aus zwei Teilen.

- 1. Generelle Anforderungen an ein ISMS nach 27001**
→ Kapitel 4-8
- 2. Spezielle Anforderungen**
→ Anhang A (normativ) Maßnahmenziele und Maßnahmen

Aufbau und Inhalte der ISO 27001

Kapitel 4 - 8

4. **Informationssicherheitsmanagementsystem**
→ Aufbau und Umsetzung eines ISMS
Risikomanagement
5. **Verantwortung der Leitung / Management**
→ Verpflichtung (Sicherheitspolitik, ISMS)
Ressourcenmanagement
6. **Interne ISMS Audits**
→ In geplanten Abständen durchführen
7. **Managementbewertung**
→ Eingaben für Bewertung
8. **Verbesserung des ISMS**
→ Korrektur- und Vorbeugemaßnahmen

Aufbau und Inhalte der ISO 27001

- √ Klassifizierung der Unternehmenswerte
- √ Durchführung einer Risikoanalyse
- √ Erstellung eines Maßnahmenkataloges
- √ Bereitstellung der erforderlichen Mittel
- √ Verpflichtung der Unternehmensführung zur Sicherheit
- √ Implementierung eines ISMS
- √ Dokumentation der Unternehmensregeln (Security Policy)
- √ Sensibilisierung der Mitarbeiter
- √ Regelmäßige Bewertung des ISMS
- √ Korrektur- und Vorbeugemaßnahmen

Aufbau und Inhalte der ISO 27001

Anhang A (normativ) Maßnahmenziele und Maßnahmen

Maßnahmenziele und Maßnahmen:

- A.5 Sicherheitsleitlinie / Sicherheitspolitik**
- A.6 Organisation der Informationssicherheit**
- A.7 Management von organisationseigenen Werten** (Wert = Alles was für die Organisation von Wert ist.)
- A.8 Personelle Sicherheit**
- A.9 Physische und umgebungsbezogene Sicherheit**
- A.10 Betriebs- und Kommunikationsmanagement**
- A.11 Zugangskontrolle**
- A.12 Beschaffung, Entwicklung und Wartung von Informationssystemen**
- A.13 Umgang mit Informationssicherheitsvorfällen**
- A.14 Sicherstellung des Geschäftsbetriebes (Kontinuitätsmanagement)**
- A.15 Einhaltung von Vorgaben (Compliance)**

Anhang A: Maßnahmenziele und Maßnahmen

A.5 Sicherheitsleitlinie / Sicherheitspolitik

Ziel: Richtungsvorgabe und Unterstützung des Managements bei der Informationssicherheit, in Übereinstimmung mit geschäftlichen und gesetzlichen Anforderungen.

- Definition einer Informationssicherheitspolitik
- Regelmäßige Überprüfung der Informationssicherheitspolitik

Anhang A: Maßnahmenziele und Maßnahmen

A.6 Organisation der Informationssicherheit

A.6.1 Interne Organisation

Ziel: Handhabung der Informationssicherheit innerhalb der Organisation.

- Definition der Zuständigkeiten, Verantwortlichkeiten, Genehmigungsverfahren, Vertraulichkeitsvereinbarungen etc.

A.6.2 Externe Beziehungen

Ziel: Aufrechterhaltung der Sicherheit von Informationen und informationsverarbeitenden Einrichtungen der Organisation, die mit Externen in Kontakt kommen.

- Umgang mit externen Dienstleistern und Kunden

Anhang A: Maßnahmenziele und Maßnahmen

A.7 Management von organisationseigenen Werten (Assets)

A.7.1 Verantwortung für organisationseigene Werte Interne

Ziel: Aufbau und Aufrechterhaltung des angemessenen Schutzes von organisationseigenen Werten. (Informationen zugehörige Prozesse, Systeme und Netzwerke)

- Inventarisierung von Vermögenswerten.
- Verantwortlichkeiten und Regeln für Umgang mit Vermögenswerten

A.7.2 Klassifizierung von Informationen

Ziel: Sicherstellung des angemessenen Schutz von Informationen.

- Regelung welche Informationen wichtig bzw. unwichtig sind.
- Kennzeichnung der Informationen (z.B. Vertraulich, nur für Intern, etc.)

Anhang A: Maßnahmenziele und Maßnahmen

A.8 Personelle Sicherheit

A.8.1 Vor der Anstellung

Ziel: Sicherstellung das Angestellte, Auftragnehmer, Dritte ihre Verantwortlichkeiten verstehen und für die Aufgaben geeignet sind. Diebstahl, -Betrug und Missbrauchrisiko verringern.

- Überprüfung vor der Anstellung im Rahmen der gesetzl. Möglichkeiten
- Arbeitsvertragsklauseln

A.8.2 Während der Anstellung

Ziel: Sicherstellung das sich alle Ihrer Verantwortlichkeiten und der Bedrohungen bewusst sind und danach handeln.

- Regelmäßige Überprüfung und Schulung
- Disziplinarverfahren

A.8.3 Beendigung oder Änderung der Anstellung

Ziel: Sicherstellung das ordnungsgemäß das Unternehmen verlassen bzw. die Anstellung gewechselt wird.

- Verantwortlichkeit für Änderungen festlegen. (Zugriffsrechte / Rückgabe Computer)

Anhang A: Maßnahmenziele und Maßnahmen

A.9 Physische und umgebungsbezogene Sicherheit

A.9.1 Sicherheitsbereiche

Ziel: Schutz vor unerlaubtem Zutritt, Beschädigung und Störung der Infrastruktur und der Informationen der Organisation.

- Sicherheitszonen, Zutrittskontrollen, Sicherung von Büros, etc.
- Schutz gegen Umwelteinflüsse (Feuer, Wasser, etc)

A.9.2 Sicherheit von Betriebsmitteln

Ziel: Verhinderung von Verlust, Beschädigung, Diebstahl oder Kompromittierung von Informationen und den zugehörigen Systemen.

- Schutz (unerlaubter Zugriff)
- Versorgungseinrichtungen (Notstrom)
- Verkabelung (Anzapfen),
- Instandhaltung (Verfügbarkeit auf Datenzugriff gewährleisten)
- Sichere Entsorgung (Festplatte)

Anhang A: Maßnahmenziele und Maßnahmen

A.10 Betriebs- und Kommunikationsmanagement

A.10.1 Verfahren und Verantwortlichkeiten

Ziel: Korrekter und sicherer Betrieb der Informationsverarbeitenden Einrichtungen.

- Dokumentierte Betriebsprozesse einschl. Änderungsverwaltung, Verantwortlichkeiten
- Trennung von Test- und Produktiveinrichtungen

A.10.2 Management der Dienstleistungserbringung von Dritten.

Ziel: Aufrechterhaltung der Informationssicherheit bei gleichzeitiger Sicherstellung der Dienstleistungserbringung entsprechend der Liefervereinbarung.

- Regelmäßige Überwachung und Überprüfung der Einhaltung

A.10.3 Systemplanung und Abnahme

Ziel: Das Risiko von Systemfehlern und Systemausfällen zu minimieren.

- Kapazitätsplanung (Serverüberlastung)
- System-Abnahme (Kriterien definieren zur Abnahme / Was muss es können?)

A.10.4 Schutz vor Schadsoftware

Ziel: Schutz der Integrität von Software und Informationen.

- Maßnahmen gegen Schadsoftware, Regelung für mobilen Programmcode

Anhang A: Maßnahmenziele und Maßnahmen

A.10 Betriebs- und Kommunikationsmanagement

A.10.5 Backup

Ziel: Erhaltung der Integrität und der Verfügbarkeit von Informationen

- Erstellung von Backup

A.10.6 Management der Netzsicherheit

Ziel: Informationen in Netzen und Infrastruktur zu schützen.

- Angemessene Verwaltung und Kontrolle von In und Externen Netzen
- Sicherheitseigenschaften und Adminanforderungen für alle Netze definieren

A.10.7 Handhabung von Speicher- und Aufzeichnungsmedien

Ziel: Unerlaubte Veröffentlichung, Veränderung, Zerstörung von Informationen und Systemen (Assets) sowie Störung des Geschäftsbetriebs verhindern.

- Verwaltung von Wechselmedien (Verfahrensanweisungen)
- Entsorgung von Medien
- Umgang mit Informationen (Verfahren für Umgang und Speicherung von Informationen festlegen)

Anhang A: Maßnahmenziele und Maßnahmen

A.10 Betriebs- und Kommunikationsmanagement

A.10.8 Austausch von Informationen

Ziel: Sicherheit von Informationen und Software die intern und extern ausgetauscht werden.

- Regeln festlegen. (z.B. was wird wann Verschlüsselt)
- Physische Medien und elektronische Nachrichten schützen

A.10.9 E-Commerce-Anwendungen

Ziel: Sicherheit und sichere Benutzung von E-Commerce.

- E-Commerce und Online Transaktionen schützen

A.10.10 Überwachung

Ziel: Aufdeckung nicht genehmigter informationsverarbeitender Aktivitäten.

- Protokolle
- Zeitsynchronisation (gemeinsame Referenzzeit)

Anhang A: Maßnahmenziele und Maßnahmen

A.11 Zugangskontrolle

A.11.1 Geschäftsanforderungen für Zugangskontrolle

Ziel: Kontrolle des Zugangs zu Informationen.

- Regelwerk zur Zugangskontrolle

A.11.2 Benutzerverwaltung

Ziel: Sicherstellung des Zugangs zu Informationssystemen / Verhindern bei Unbefugten.

- Benutzerregistrierung
- Verwaltung und Überprüfen von Rechten und Passwörtern

A.11.3 Benutzerverantwortung

Ziel: Verhinderung von unbefugtem Zugriff, Diebstahl, Kompromittierung von Informationen.

- Passwortverwendung (Sicherheitsregeln für Auswahl und Anwendung von Passw.)
- Unbeaufsichtigte Benutzerausstattung schützen (Bildschirmsperre)
- Aufgeräumter Schreibtisch (Keine wichtigen Informationen offen liegen lassen)
- „Leerer Monitor“ (Bsp. Personalabteilung)

Anhang A: Maßnahmenziele und Maßnahmen

A.11 Zugangskontrolle

A.11.4 Zugangskontrolle für Netze

Ziel: Verhinderung von unbefugtem Zugang zu Netzdiensten.

- Regeln zur Nutzung von Netzen
- Technische Möglichkeiten beachten und nutzen (Routingkontrolle etc.)

A.11.5 Zugriffskontrolle auf Betriebssysteme

Ziel: Verhinderung von unbefugtem Zugriff auf das Betriebssystem.

- Sichere Anmeldung, Benutzerauthentisierung, Passwortverwaltung
- Dienstprogramme einschränken kontrollieren / Session Time-out

A.11.6 Zugangskontrolle zu Anwendungen und Information

Ziel: Verhinderung des unbefugten Zugangs zu Informationen in Anwendungssystemen.

- Einschränkung von Informationszugriff (Benutzerspezifische Zugangskontrolle)
- Isolation sensibler Systeme

A.11.7 Mobile Computing und Telearbeit

Ziel: Sicherstellen der Informationssicherheit bei mobile Computing und Telearbeit.

- Regelungen, Leitlinien und Maßnahmen zur sicheren Nutzung.

Anhang A: Maßnahmenziele und Maßnahmen

A.12 Beschaffung, Entwicklung und Wartung von Informationssystemen

A.12.1 Sicherheitsanforderungen von Informationssystemen

Ziel: Sicherheit ist ein integraler Bestandteil von Informationssystemen.

- Analyse und Spezifikation der Sicherheitsanforderungen an Informationssysteme

A.12.2 Korrekte Verarbeitung in Anwendungen

Ziel: Verhinderung von Fehlern, Veränderung, Verlust von Informationen in Anwendungen.

- Kontrolle und Überprüfung von EVA

A.12.3 Kryptographische Maßnahmen

Ziel: Schutz der Informationen durch Verschlüsselung.

- Leitfaden zum Anwenden der Verschlüsselung
- Verwaltung der Schlüssel

Anhang A: Maßnahmenziele und Maßnahmen

A.12 Beschaffung, Entwicklung und Wartung von Informationssystemen

A.12.4 Sicherheit von Systemdateien

Ziel: Sicherheit von Systemdateien gewährleisten.

- Zugriff auf Quellcode beschränken
- Bei Installation von Software müssen entsprechende Verfahren eingehalten werden

A.12.5 Sicherheit bei Entwicklungs- und Unterstützungsprozessen

Ziel: Erhalt der Sicherheit von Software und Informationen.

- Formelles Verfahren zur Änderung an Informationssystemen
- Negative Auswirkungen durch Veränderungen sollen verhindert werden.
- Ausgelagerte Softwareentwicklung überwachen.

A.12.6 Schwachstellenmanagement

Ziel: Veröffentlichte technische Schwachstellen dürfen nicht Ausgenutzt werden.

- Kontrolle der Schwachstellen

Anhang A: Maßnahmenziele und Maßnahmen

A.13 Umgang mit Informationssicherheitsvorfällen

A.13.1 Melden von Informationssicherheitsereignissen und Schwachstellen

Ziel: Schwachstellen in Informationssystemen müssen gemeldet werden, sodass rechtzeitig reagiert werden kann.

- Verpflichtung zur Meldung für Schwachstellen für Alle (Intern und Extern)
- Sicherstellung der geeigneten Kommunikationswege (Managementkanäle)

A.13.2 Umgang mit Informationssicherheitsvorfällen und Verbesserungen

Ziel: Einhaltung eines einheitlichen und effektiven Ansatzes zum Umgang mit Informationssicherheitsvorfällen.

- Verantwortlichkeiten für den Umgang mit Vorfällen festlegen
- Lernen aus den Vorfällen sicherstellen
- Sammeln von Beweisen

Anhang A: Maßnahmenziele und Maßnahmen

A.14 Sicherstellung des Geschäftsbetriebes (Business Continuity Management)

A.14.1 Informationssicherheitsaspekte bei der Sicherstellung des Geschäftsbetriebs

Ziel: Schutz vor Unterbrechung von Geschäftsaktivitäten. Schutz von kritischen Geschäftsprozessen vor den Auswirkungen von Störungen von Informationssystemen sowie Katastrophen. Rechtzeitige Wiederaufnahme von Geschäftsprozessen.

- Gelenkter Prozess zur Sicherstellung des Geschäftsbetriebs
- Identifizierung und Risikobetrachtung von Ereignissen die den Geschäftsbetrieb stören können
- Notfallpläne
- Rahmenwerk für die Notfallpläne festlegen. (Widersprüche vermeiden)
- Regelmäßiges Testen, Überprüfen und Neubewerten der Notfallpläne

Anhang A: Maßnahmenziele und Maßnahmen

A.15 Einhaltung von Vorgaben (Compliance)

A.15.1 Einhaltung gesetzlicher Vorgaben

Ziel: Vermeidung von Verstößen gegen Gesetze, amtliche oder vertragliche Verpflichtungen, sowie gegen Sicherheitsanforderungen.

- Identifikation der relevanten Gesetze
- Schutz von geistigem Eigentum. Beachtung von Urheberschutz bei Software
- Datenschutz und Vertraulichkeit. Verhinderung von Missbrauch

A.15.2 Einhaltung von Sicherheitsregelungen –standards, und technischer Vorgaben

Ziel: Sicherstellung, dass Systeme die Sicherheitsregelungen und -Standards einhalten.

- Manager müssen in Ihrem Verantwortungsbereich die Einhaltung sicherstellen
- Regelmässige Prüfung der Einhaltung der Vorgaben

A.15.3 Überlegungen zu Revisionsprüfungen von Informationssystemen

Ziel: Steigerung der Effektivität und Minimierung der Störungen bei Revisionsprozessen für Informationssysteme.

- Sorgfältige Planung von Revisionsprozessen, um Störungen der Geschäftsprozesse zu vermeiden
- Missbrauch von Tools zur Untersuchung von Informationssystemen vermeiden

Informationssicherheit bedeutet

Risiken managen und innerhalb einer wirtschaftlichen und sicheren Toleranzbreite halten.

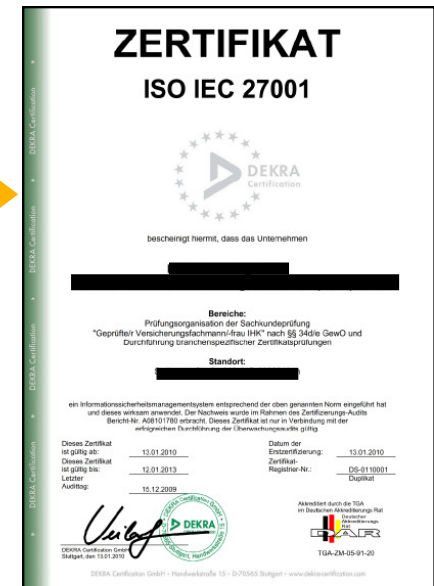
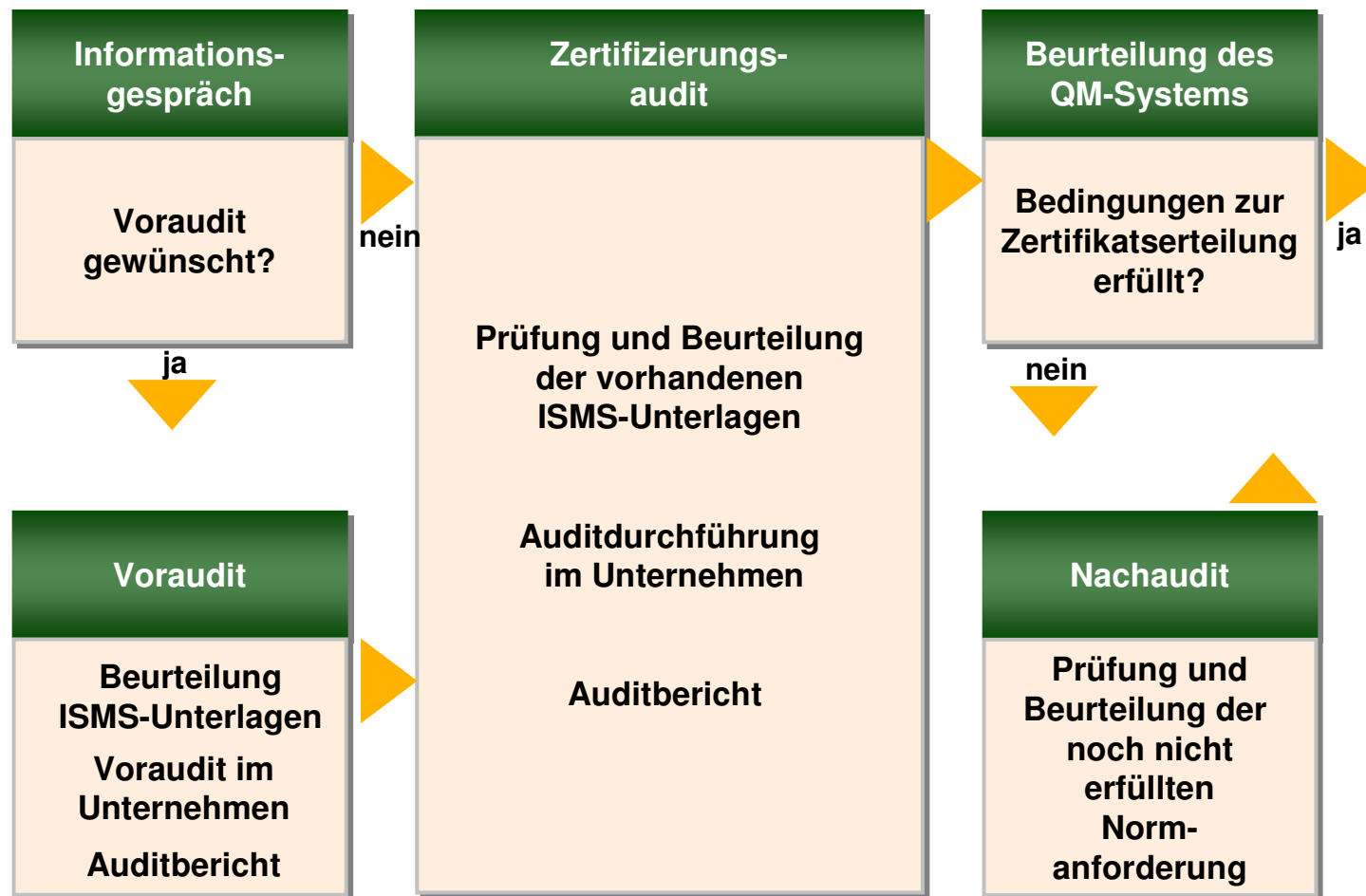
Spielregeln festlegen (Security Policy)

Veränderungen wahrnehmen und berücksichtigen

ISM-System regelmäßig prüfen

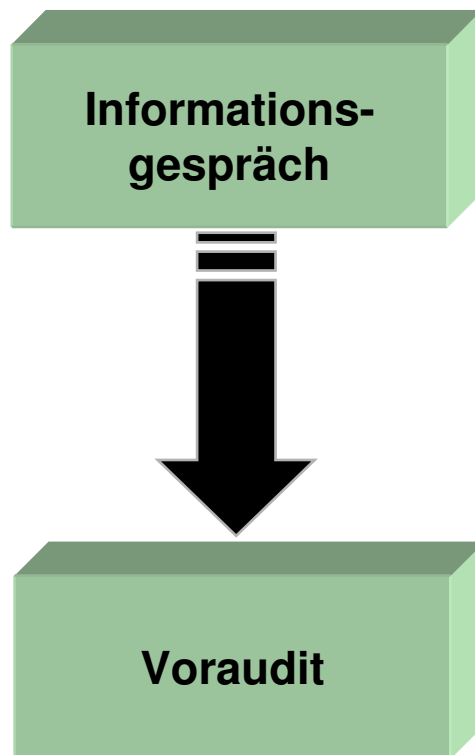
Korrektur- und Verbesserungsprozess umsetzen

Der Ablauf einer ISM-System-Zertifizierung



DEKRA Certification GmbH, Axel Dröge 0170 -76 77 481

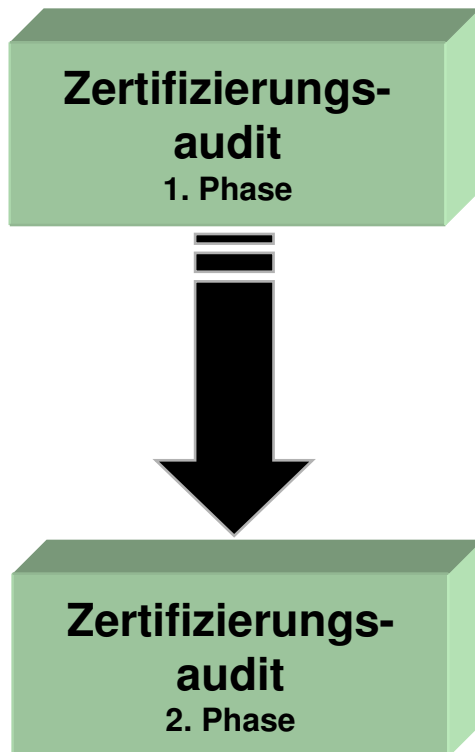
Ablauf des ISO 27001-Zertifizierungsverfahrens



Ziel: Klären offener Fragen hinsichtlich der Normenanforderungen und des Zertifizierungsablaufes.

Ziel: Feststellen ob das Unternehmen grundsätzlich zertifizierungsfähig ist.

Ablauf des ISO 27001-Zertifizierungsverfahrens



Ziel: Die 1. Phase dient dazu ein Verständnis des ISMS im Kontext der Sicherheitspolitik und Ziele der Organisation zu gewinnen. Darüber hinaus soll eine erste Einschätzung erfolgen, ob und inwieweit die 2. Phase erfolgreich abgeschlossen werden kann.

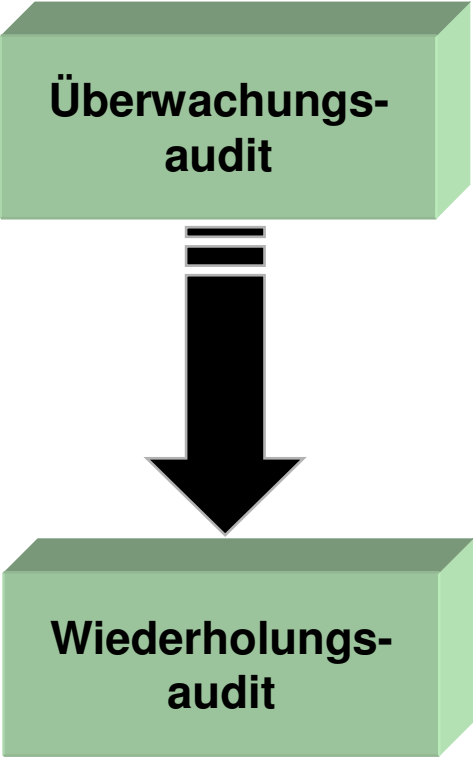
Folgende Themen werden dabei geprüft:

- Bewertung der Risikoanalyse
- Bewertung der Anwendbarkeitserklärung
- Bewertung der ISMS Dokumentation
- Erfassung der offenen Punkte die für eine erfolgreiche Durchführung der 2. Phase kritisch sind

Ziel: Bei der Durchführung der zweiten Phase werden folgende Punkte geprüft:

- Maßnahmen aus der 1. Phase
- Überprüfung der Elemente aus der ISO 27001
- Managementreview
- Interne Audits

Ablauf des ISO 27001-Zertifizierungsverfahrens



**Überwachungs-
audit**

Ziel: Überprüfung der Wirksamkeit des ISMS gemäß der Risiken, neuen Anforderungen, Veränderungen und des KVP -Prozesses.

**Wiederholungs-
audit**

Ziel: Feststellen, ob das bestehende Zertifikat um weitere 3 Jahre verlängert werden kann.

Vorteile einer Zertifizierung

Reduzierung des Haftungsrisikos gegenüber Dritten (Gesetzgeber, Kunden und Partner)

Beherrschung der Risiken (Restrisiken)

Sicherheit als integraler Bestandteil der Geschäftsprozesse

Kostenreduzierung durch transparente Prozesse/Strukturen

Sicherheitsbewusstsein der Mitarbeiter stärken

Beurteilung der Organisationsprozesse nach Sicherheits Gesichtspunkten

Wettbewerbsvorteil (Nachweis eines ISMS)

Vorteile bei Krediten (Basel II) und Versicherungen

DEKRA Certification – Go for Quality

Vielen Dank für Ihre Aufmerksamkeit!

