Motivation zur Zertifizierung und notwendige Schritte

Know-how to go – ISMS-Zertifizierung

HiSolutions AG

Jerome Horn

Jerome Horn

Senior Consultant

- Einführung, Weiterentwicklung sowie Auditierung von Informationssicherheitsmanagement-Systemen nach BSI IT-Grundschutz sowie ISO 27001
- Zertifizierter Lead Auditor für Managementsysteme nach ISO 22301 und ISO 27001 nativ sowie im Energiewirtschaftssektor
- Themenverantwortlich bei HiSolutions für internes Auditmanagement & Zertifizierung
- Informationssicherheit im Banken- und Finanzdienstleistungsumfeld

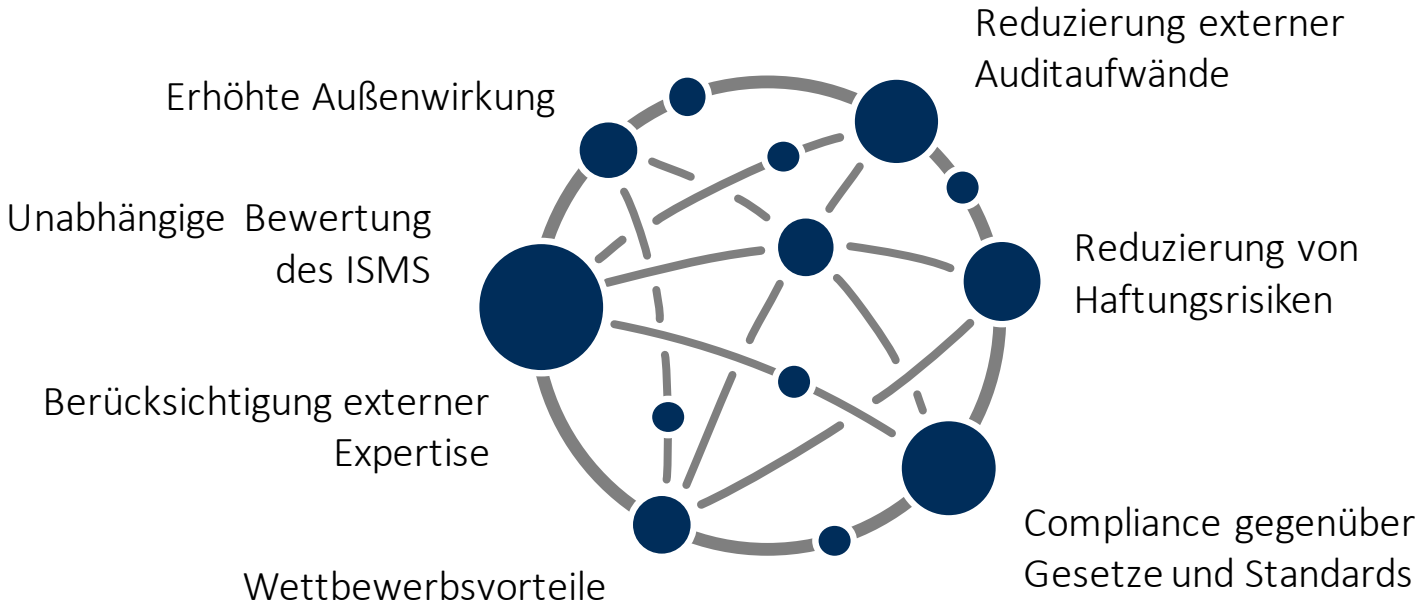
Ein ISMS ebnet die strukturelle Umsetzung von Informationssicherheit

Ein Informationssicherheitsmanagementsystem umfasst die Aufstellung von Prozesse, Vorgaben und Verfahren innerhalb eines Unternehmens, um die Informationssicherheit stetig zu definieren, zu steuern, zu überprüfen, aufrechtzuerhalten und kontinuierlich zu verbessern.

Zielsetzung:

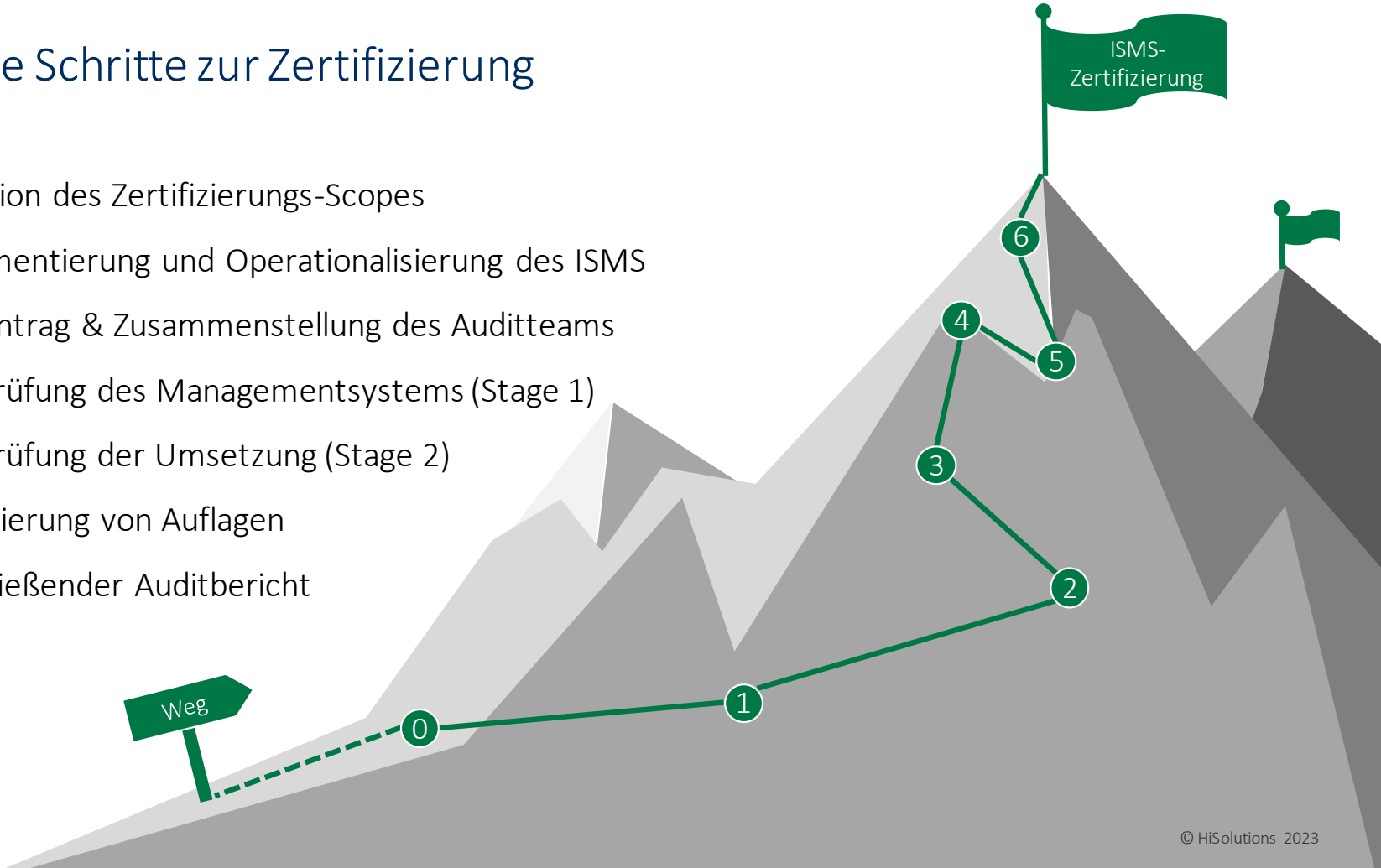
- Informationssicherheit eines Unternehmens risikoorientiert und kontinuierlich verbessern
- Mit einem strukturierten Ansatz die vorhandenen Risiken identifizieren und diese geeignet behandeln
- Definition von Regeln, Verfahren und Methoden, mit denen sich die Aufgaben und Aktivitäten der Informationssicherheit steuern und optimieren lassen

Je nach Branche befürworten unterschiedliche Gründe die Zertifizierung eines ISMS



Typische Schritte zur Zertifizierung

0. Definition des Zertifizierungs-Scopes
1. Implementierung und Operationalisierung des ISMS
2. Auditantrag & Zusammenstellung des Auditteams
3. Überprüfung des Managementsystems (Stage 1)
4. Überprüfung der Umsetzung (Stage 2)
5. Adressierung von Auflagen
6. Abschließender Auditbericht



Notwendige Schritte im Falle einer IT-Grundschutz-Zertifizierung

Vorbereitungsphase

Definition des Informationsverbundes, Beauftragung eines Auditteams, mögliches einmaliges Voraudit

Antragsphase

Einreichung des Auditantrag beim BSI, Unabhängigkeitserklärungen des Auditteams

Dokumentenreview (Stage 1)

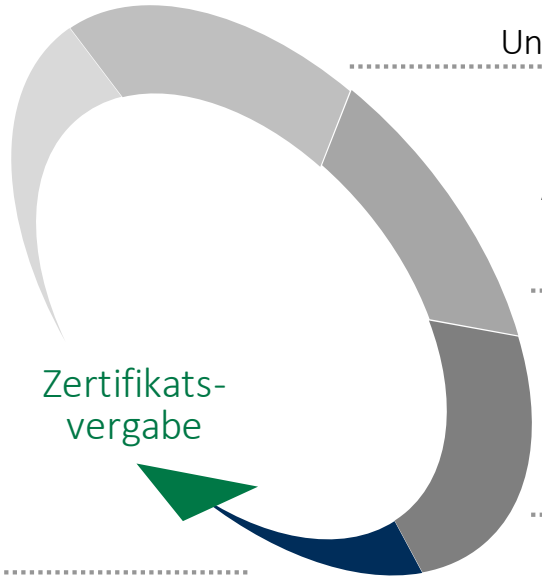
Abgabe der Referenzdokumente A.0 - A.6, Dokumentenreview durch das Auditteam, Auditplan

Vor-Ort-Überprüfung (Stage 2)

Vor-Ort-Audit und Standortüberprüfung, Prüfung ausgewählter Grundschutzbausteine an Zielobjekten

Berichtsphase

Vorlage des Auditberichts inkl. Auditorenvotum, optionale Adressierung von Nachforderungen/Auflagen des BSI



Notwendige Schritte im Falle einer ISO 27001-Zertifizierung nativ

Optionales Voraudit

Ersteinschätzung der Zertifizierungsreife,
Identifizierung schwerwiegender Mängel

Auditplanung

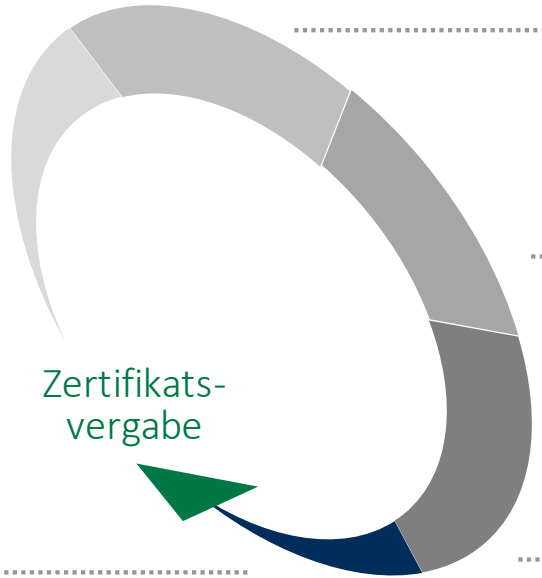
Definition des Zertifizierungsscopes,
Anfrage und Bestellung eines Auditteams

Stage 1 Audit

Überprüfung des Managementsystems,
Standortprüfung,
Adressierung von Nebenabweichungen

Stage 2 Audit

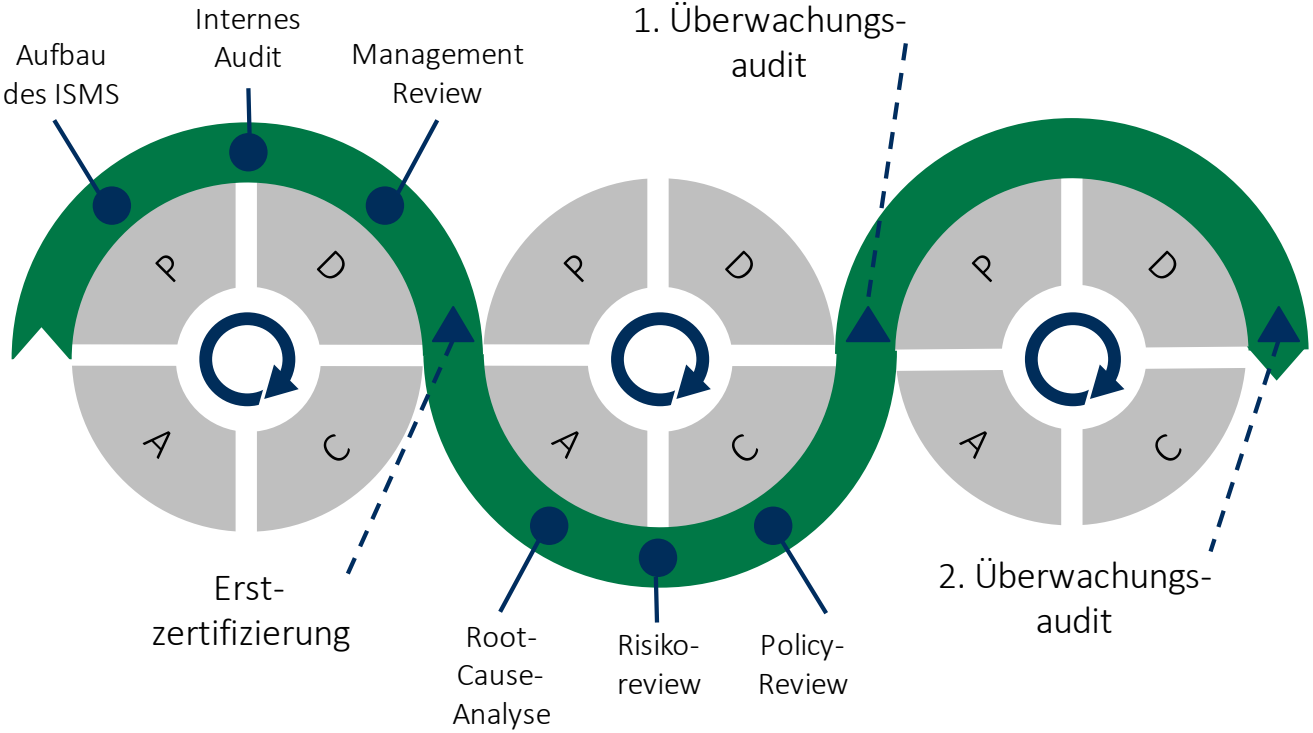
Überprüfung der Konformität zur ISO 27001 sowie Controls der ISO 27002,
Umfassende Stichprobenprüfung des ISMS durch Interviews, Begehungen und Beobachtungen



Berichtsphase

Finalisierung des Auditberichts inkl. Gesamtvotum,
Zertifikatsvergabe für drei Jahre

Vor dem Audit ist nach dem Audit



IT-Grundschutz und ISO 27001: Die Standards im Vergleich

Determinante/Parameter	IT-Grundschutz	ISO 27001
Internationalität	−	+ +
Standard-IT-Infrastruktur	+ +	−
Generell hoher Schutzbedarf	○	○
Besonderes Einsatzszenario	−	○
Anzahl umzusetzender Anforderungen	○	+
Dauer bis Erstzertifizierung	○	○
Klare Vorgaben an den IT-Betrieb	+ +	−
Stufenkonzept/Migrationspfad	+ +	−
Standard frei verfügbar	frei	kostenpflichtig
Aktualisierung des Standards	jährlich	unregelmäßig

Entscheidende Erfolgsfaktoren mit der Zertifizierung

Erfolgsfaktoren bei der Auditvorbereitung

- Frühzeitige Anfrage und Einbindung des Auditteams
- Sensibilisierung der Auditbeteiligten („Audit-Defense“)
- Frühzeitige Planung des gesamten Zertifizierungszyklus
- Beauty-Contest / Anbieterwettbewerb

Erfolgsfaktoren für das ISMS

- Unterstützung durch die Geschäftsleitung
- Verständnis, Kooperationsbereitschaft und aktive Unterstützung durch alle Verantwortlichen
- Konsequente Gruppenbildung
- GRC-Tool-Unterstützung

Haben Sie Fragen?

Schloßstraße 1 | 12163 Berlin

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

www.hisolutions.com