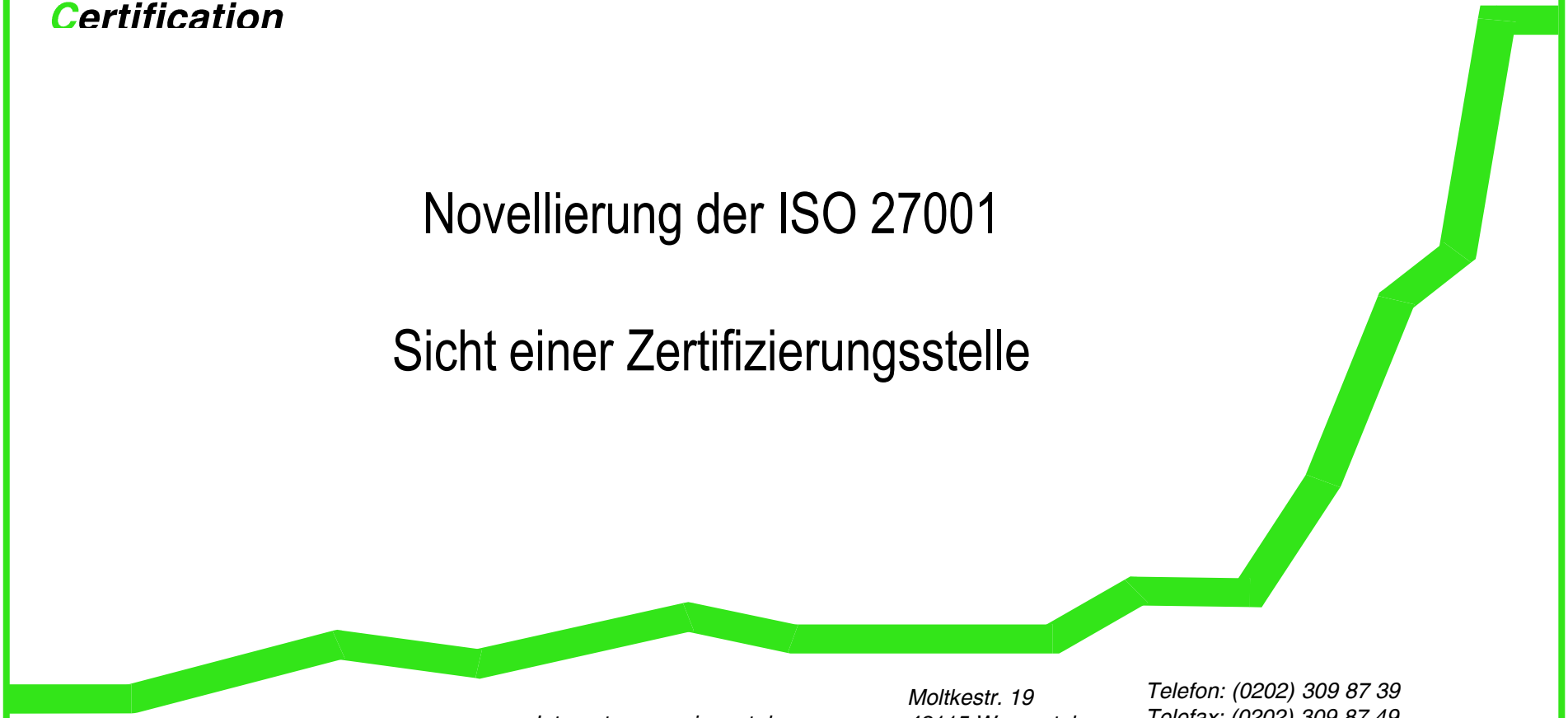
UIMCert®
GmbH

Unternehmens- und
Informations- Management
Certification

Novellierung der ISO 27001

Sicht einer Zertifizierungsstelle



Internet: www.uimcert.de

Moltkestr. 19
42115 Wuppertal

Telefon: (0202) 309 87 39
Telefax: (0202) 309 87 49
E-Mail: certification@uimcert.de

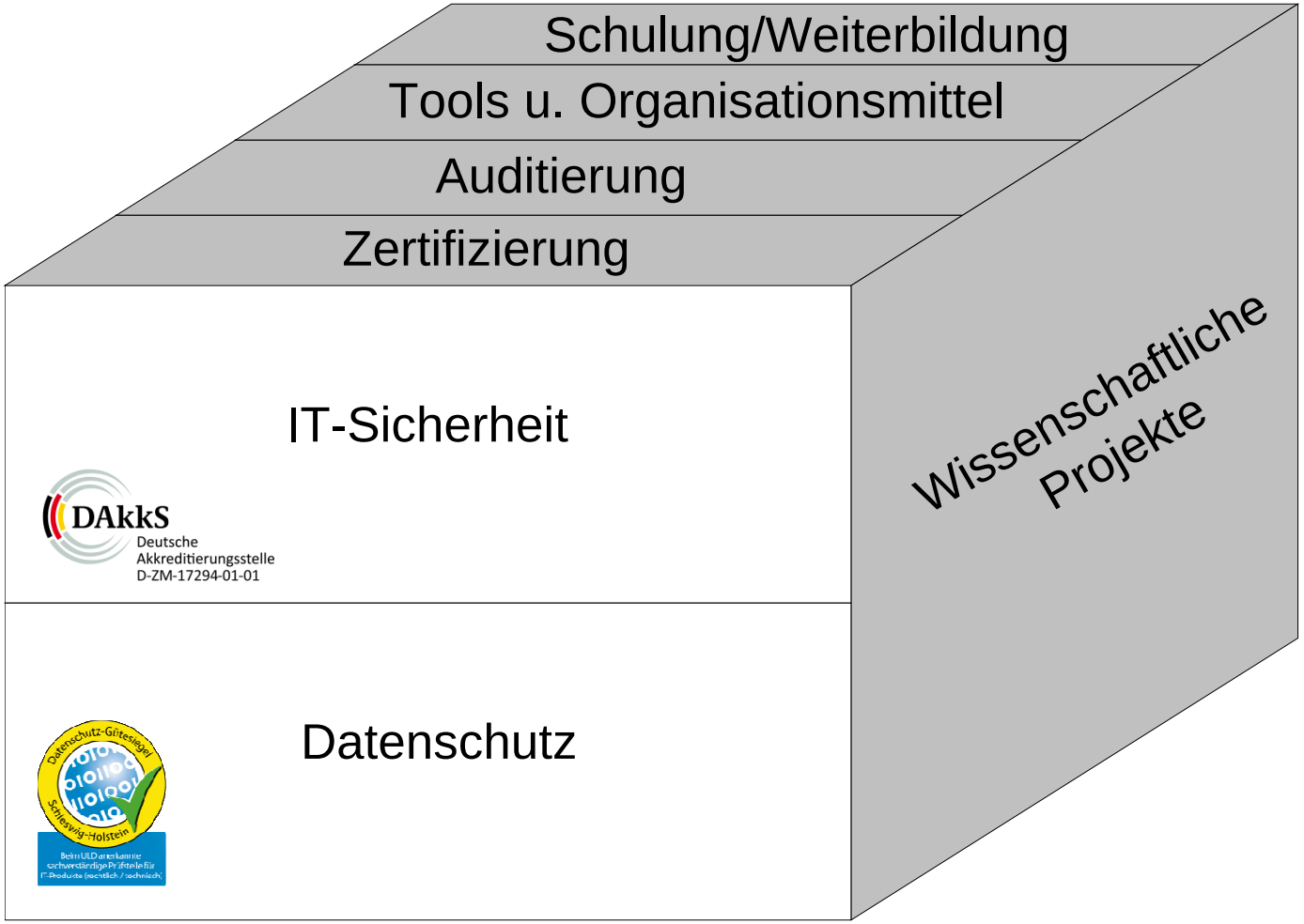
Inhalte

- Konsequenzen für den Zertifizierer
- Besonderheiten des Transition Audits
- Erfahrungen im Umgang mit der Normumstellung

Timo Noll

- Informatikkaufmann
- Lead Auditor ISO 27001
- Lizenzierter Auditteamleiter für ISO 27001 Audits auf der Basis von IT-GS
- Lead Auditor IDW PS 880
- Lead Auditor IDW PS 330/331
- Beim ULD anerkannter Mitarbeiter der Prüfstelle UIMCert GmbH

UIMCert GmbH



Konsequenzen für den Zertifizierer

- Nachweis über Qualifikation der Auditoren
- Änderung der Akkreditierung nach ISO 27001:2013
- Umstellung auf ISO 27006:2011 und ISO 17021:2011
  => Konsequenzen für die Auditees

Qualifikation der Auditoren

Die Zertifizierungsstelle muss die Kompetenz der Auditoren sicherstellen:

- Ermittlung von Schulungsbedarf der Auditoren
- Bereitstellung von Ressourcen zur Aus-/Weiterbildung oder
- Bereitstellung des Zugangs dazu

Aber:

Auch die Auditoren haben die Pflicht, ihr Wissen und ihre Fähigkeiten im Bereich der Informationssicherheit und der Auditierung ***fortlaufend aktuell*** *zu halten.*

Änderung der Akkreditierung

Antrag an die DAkkS (Deutsche Akkreditierungsstelle GmbH) zur Akkreditierungsänderung auf ISO 27001:2013

- Formeller Antrag
- Umstellungsplan mit Verzeichnis erteilter Zertifikate gem. ISO 27001:2005
- Liste der zugelassenen ISMS-Auditoren
- Nachweise der Schulungen zur ISO/IEC 27001:2013

Konsequenzen für die Auditees

- Bildung des Auditteams:
  - Berücksichtigung von integrierten oder gemeinschaftlichen Audits
  - Berücksichtigung bereits durchgeführter Audits der Auditoren beim Auditee
- Risikoorientierte Ermittlung der Auditdauer
  (Berücksichtigung der Produkte, Prozesse oder Tätigkeiten des Auditees)
- Zeit von Auditteammitgliedern, die nur zur Unterstützung teilnehmen, wird nicht gewertet (Fachexperten, Übersetzer/Dolmetscher, Beobachter, Trainees)
- Formelle detaillierte Forderung nach Eröffnungs- und Abschlussbesprechung einschließlich der Empfehlung bzgl. der Zertifizierung

Konsequenzen für die Auditees

- Hinzufügen der formalen Rollen Beobachter und Betreuer
- Verbesserungsmöglichkeiten dürfen aufgezeigt werden, wenn diese keine Nichtkonformitäten sind.
- Der Auditor darf keine Ursachen oder Lösungen von Nichtkonformitäten benennen / vorschlagen
- Analyse der Ursachen von Nichtkonformitäten durch den Auditee
- Verifizierung der Wirksamkeit der Korrekturmaßnahmen durch die Zert.-Stelle
- Ablehnung eines Antrags auf Zertifizierung durch die Zert.-Stelle muss begründet werden
- Bewertung der Leistungsfähigkeit des ISMS des Auditees in Bezug auf Gesetzestreue

Besonderheiten des Transition Audits

- Besondere Aspekte der Normumstellung
- Auditschwerpunkte aus Sicht des Zertifizierers
- Verständnis der Zertifizierungsstelle / wesentliche Unterschiede
- Freiheitsgrade des Auditees

Besondere Aspekte der Novellierung

- PDCA ist nicht mehr zwingend vorgeschrieben, es können auch andere Prozesse zur „kontinuierlichen Verbesserung“ genutzt werden
- Anforderungen an das ISMS Umfeld und an den Scope werden stärker definiert. Die Anforderungen aller relevanten externen „interested Parties“ bzw. interessierten Parteien müssen als Teil des ISMS beachtet werden
- Umsetzung des Annex A „freiwillig“
  (weiterhin Nachweis der Umsetzung der Anforderungen erforderlich)
- Eigenes Kapitel im Annex A zur Überwachung der Tätigkeiten von Lieferanten

Besondere Aspekte der Novellierung

- Risikoansatz geändert, es muss ein „Risk-Owner“ definiert werden; Risiken sind in Bezug auf Vertraulichkeit, Verfügbarkeit und Integrität zu identifizieren.
  => In Anlehnung an die Risikomanagementstandards ISO 27005 und ISO 31000
- „Incident Management“ wird nun weiter gefasst, das Normkapitel „Nichtkonformität“ deckt nicht nur Zwischenfälle und den Umgang mit solche ab, sondern auch alle andere Arten von „Normabweichungen“.
- Es gibt nun ein eigenes Kapitel zum Thema Überwachung und Effizienz des ISMS. Ein Unternehmen muss nun die Effizienz der umgesetzten Controls identifizieren, beschreiben und dokumentieren, KPIs müssen entwickelt werden.

Auditschwerpunkte aus Zertifizierersicht

- Umfeld der Organisation
- Risik management
- Incident management
- Informationssicherheit im BCM
- Umgang mit Dienstleistern/Lieferanten
- Measurement

Verständnis der Zertifizierungsstelle

- Auditoren sollten besonders auf Umgang der Auditees mit der Normumstellung eingehen
- Begutachtung des (geregelten) Verfahrens zur Umstellung
- u. U. Diskussion der Scope-Definition
- Beleuchtung der ISMS-Änderungen, bspw.:
  - PDCA
  - Definition der Objectives und Controls
  - Risk management
  - Incident Management
  - BCM

Änderung der Freiheitsgrade der Auditees

Erhöhung der Freiheitsgrade

+ PDCA Zyklus
+ Umgang mit Annex A

Verringerung der Freiheitsgrade

– Scope-Definition (Änderungen marginal)
– Risk management
– Performance evaluation

Delta-Audit oder integriertes Transition Audit?

Delta-Audit:

- Eigenständiges Audit zur Prüfung der neuen Normforderungen

Transition Audit:

- Im Rahmen eines regulären Audits werden die Anforderungen der ISO 27001:2013 geprüft, besonderes Augenmerk auf neue Normforderungen

Vorteile Delta-Audit:

- Freiere Zeitwahl beim Delta Audit
- Umstellung kann u. U. später erfolgen

Nachteil:

- insgesamt aufwändiger, da 2 Audits durchgeführt werden müssen

Erfahrungen mit Auditees

- Kenntnis über Normumstellung
- Keine genaue Vorstellung über Inhalte/ Änderungen
- Häufig kein gesichertes Wissen über Umstellungszeiten vorhanden
- Umstellungswunsch: Transition Audit im Rahmen von Überwachungs-/Rezertifizierungsaudit
- Umstellung zum spätmöglichsten Zeitpunkt

Übergangszeiten; Konsequenzen für Auditees

- Ab 1. Oktober 2014 nur noch Erst- und Re-Zertifizierung gem. ISO 27001:2013
- Überwachungsaudits nach 27001:2005 bei bestehenden Zertifikaten bis 09/2015 noch möglich
- Umstellung auf ISO 27001:2013 muss bis 30. September 2015 erfolgen, ab 01. Oktober 2015 ist die alte Norm ungültig

Konsequenzen (Diskussion)

ISO 27001:2005

4.2.1 Festlegen des ISMS

Definition des Anwendungsbereiches und der Grenzen des ISMS, unter Berücksichtigung der Eigenschaften des Geschäfts, der Organisation, ihres Standortes, ihrer Werte (Assets) und ihrer Technologie, einschließlich der Details über und Rechtfertigung von jeglichen Ausschlüssen aus dem Anwendungsbereich.

ISO 27001:2013 (Scope-Definition)

4.3 Geltungsbereich des ISMS

Die Organisation muss die Grenzen und die Anwendbarkeit des ISMS und damit seinen Geltungsbereich festlegen.

Bei der Festlegung des Geltungsbereichs muss die Organisation folgendes berücksichtigen:

a) die in 4.1 genannten externen und internen Angelegenheiten;
b) die in 4.2 genannten Anforderungen; und
c) Schnittstellen und Abhängigkeitsverhältnisse zwischen Tätigkeiten, die von der Organisation selbst durchgeführt werden, und Tätigkeiten anderer Organisationen.

Der Geltungsbereich muss als dokumentierte Information verfügbar sein.

Konsequenzen (Diskussion)

ISO 27001:2005

4.2.1 g) Auswahl der Maßnahmen für die Risikobehandlung

Die Maßnahmenziele und Maßnahmen in Anhang A, die geeignet sind, die identifizierten Anforderungen abzudecken, müssen als Teil dieses Prozesses ausgewählt werden.
Die in Anhang A angegebenen Maßnahmenziele und Maßnahmen sind nicht erschöpfend, und zusätzliche Maßnahmenziele und Maßnahmen dürfen ebenfalls ausgewählt werden.

ISO 27001:2013

6.1.3 b) Festlegen aller Maßnahmen, die zur Implementierung der gewählten Optionen für die Sicherheitsrisikobehandlung erforderlich sind;
ANMERKUNG: Organisationen können Maßnahmen nach Bedarf gestalten oder vorgefertigte Maßnahmen aus einer beliebigen Quelle wählen.
c) Vergleich der nach 6.1.3 b) festgelegten Maßnahmen mit den Maßnahmen in Anhang A und Vergewisserung, dass keine erforderlichen Kontrollmaßnahmen ausgelassen wurden;
ANMERKUNG 1: […] Anwender dieser Internationalen Norm werden für die Sicherstellung, dass keine wichtigen Maßnahmen übersehen wurden, auf Anhang A verwiesen.
ANMERKUNG 2 […] Die Liste der Maßnahmenziele und Maßnahmen in Anhang A ist nicht erschöpfend; u. U. sind weitere Maßnahmenziele und Maßnahmen erforderlich.

Konsequenzen (Diskussion)

ISO 27001:2005

Anhang A (normativ)
Als Teil des in 4.2.1 beschriebenen ISMS-Prozesses müssen Maßnahmenziele und Maßnahmen aus diesen Tabellen gewählt werden.

ISO 27001:2013

Anhang A (normativ)
Die Auswahl von Maßnahmenzielen und Maßnahmen aus diesen Tabellen stellt einen Teil des ISM-prozesses nach Abschnitt 6.1.3 (Risikobehandlung) dar.

Konsequenzen (Diskussion)

ISO 27001:2005

4.2.2 d) Umsetzen und Durchführen des ISMS

Definition eines Maßes für die Wirksamkeit der ausgewählten Maßnahmen oder Maßnahmengruppen;
außerdem muss festgelegt werden, wie diese Maße benutzt werden können, um die Wirksamkeit der Maßnahmen einzuschätzen, und um dabei vergleichbare und reproduzierbare Resultate
zu erhalten.

ANMERKUNG Das Messen der Wirksamkeit von Maßnahmen ermöglicht es Managern und Personal, zu bestimmen, wie gut die Maßnahmen die vorgesehenen Maßnahmenziele erreichen.

ISO 27001:2013

9.1 Überwachung, Messung, Analyse und Auswertung

Die Organisation muss die Leistung und die Wirksamkeit des ISMS auswerten.

a) Was
b) Wie
c) Wann
d) Wer
e) […]
f) […]

ANMERKUNG Die ausgewählten Verfahren sollten zu vergleichbaren und reproduzierbaren Ergebnissen führen, die
als aussagekräftig zu betrachten sind.

Mapping Guide ISO 27001:2005 -> ISO 27001:2013

http://www.bsigroup.com/Documents/iso-27001/resources/BSI-ISO27001-mapping-guide-UK-EN.pdf

Transition Guide ISO 27001:2005 <-> ISO 27001:2013

http://www.bsigroup.com/LocalFiles/en-GB/iso-iec-27001/resources/BSI-ISO27001-transition-guide-UK-EN-pdf.pdf

UIMCert®

... noch Fragen

Vielen Dank für Ihre Aufmerksamkeit!

Kontakt::
Timo Noll
UIMCert GmbH
Moltkestraße 19
42115 Wuppertal

0202 – 309 87 39
tnoll@uimcert.de
www.UIMCert.de