27001-Zertifizierung

1. Zertifizierungsverfahren bei der DQS

2. Systematik im Audit

Dr. Volker Knauer
DQS-Auditleiter für die Regelwerke
9001,14001, 20000-1, 27001
und VDA Prototypenschutz

28.09.2011

DQS GmbH

Behandelte Themen

1. Das Zertifizierungsverfahren

Verfahren Erstzertifizierung

Self-Assessment
auf Basis DQS-Checkliste

Information

Angebot
und Vertrag

System-
Analyse

Audit vor Ort

System-
Begutachtung

Audit vor Ort

System-
Bewertung

Zertifikats-
erteilung

optional
Vorbegutachtung

Stage 1: Analyse und Bewertung der Dokumentation, erster Blick unter anderem auf interne Audits und Management-Review

Stage 2: Umfassende Begutachtung vor Ort , Feststellen der Norm-konformität und Aufzeigen von Verbesserungspotential

Der weitere Begutachtungsverlauf

Drei-Jahresrhythmus

1. System-Begutachtung vor Ort

2. System-Begutachtung vor Ort

Wiederholungs-Begutachtung vor Ort

Systembewertung und Zertifikatserteilung

Begutachtung zur Systemförderung („Überwachungsaudit“)

DQS Audit-Checkliste

G	I	J	K	L	M
4.3 Dokumentationsanforderungen					95%
4.3.1 Allgemeines					100%
Dokumentationen müssen Aufzeichnungen von Managemententscheidungen, enthalten, sicherstellen, dass Aktivitäten sich zu Managemententscheidungen und Politiken zurückverfolgen lassen, und sicherstellen, dass die aufgezeichneten Ergebnisse reproduzierbar sind. Es ist wichtig, dass es möglich ist, die Beziehung von den ausgewählten Maßnahmen zurück zu den Resultaten des Risikoeinschätzungs- und Risikobehandlungsprozesses nachzuweisen, und danach zurück zu der ISMS-Politik und den Zielen.	Schutzbedarfsanalyse und Risikobewertung, Auditplan und -berichte, Maßnahmenlisten, Protokolle des Security Circles	Schutzbedarfsanalysen und Risikobewertungen werden jährlich aktualisiert (z.B. Entwicklung/ Konstruktion Stand 03.05.2010 mit Update 01.05.2011), Auditplan und -berichte, Maßnahmenlisten, Protokolle des Security Circles	1		100%
Die Dokumentation des ISMS sollte Folgendes enthalten: - Dokumentation des Scopes, - Verfahren und Maßnahmen zur Unterstützung des ISMS, - Dokumentation der Risikomethode, - Report über die Risikobewertung, - Beschreibung der Messung der Effektivität des ISMS, - Erforderliche Aufzeichnungen, - Dokumentierte Liste der Anwendung der Maßnahmen aus Anhang A	Geltungsbereich_IMS_PB.pdf mit SOA, IMS, Risikobewertungen (z.B. RB_Fahrzeugtechnik_PP_QM-024), AA Schutzbedarfsfeststellung AA_GRP_008.4.1-B	Anwendungsbereich und Grenzen des ISMS sowie SOA sind im Dokument "Geltungsbereich_IMS_PB.pdf" dokumentiert (Stand 24.10.2008 weiterhin gültig). Verfahren und Maßnahmen des ISMS sind im IMS beschrieben. Eine Methode zur Schutzbedarfsfeststellung und zur Risikobewertung ist festgelegt, Risiken sind bewertet und werden jährlich überprüft. Die Wirksamkeit des ISMS wird laufend vom Security Circle überwacht und im jährlichen Management Review bewertet.	1		100%
4.3.2 Lenkung von Dokumenten					100%
Die für das ISMS notwendigen Dokumente müssen geschützt und gelenkt werden. Ein dokumentiertes Verfahren zur Festlegung der erforderlichen Managementaktionen muss eingeführt werden, das - die Freigabe, - den Review und die Überarbeitung, - die Identifizierung der Änderungen,	IMS	Lenkung der Dokumente im Management-System beschreiben, gelenkte Dok. sind gekennzeichnet mit Ausgabedatum und Verantwortlichem, in wichtigen Dokumenten ist Historie enthalten	1		100%

Behandelte Themen

2. Ablauf eines 27001-Audits / Audit-Schwerpunkte

Schwerpunkte im Audit

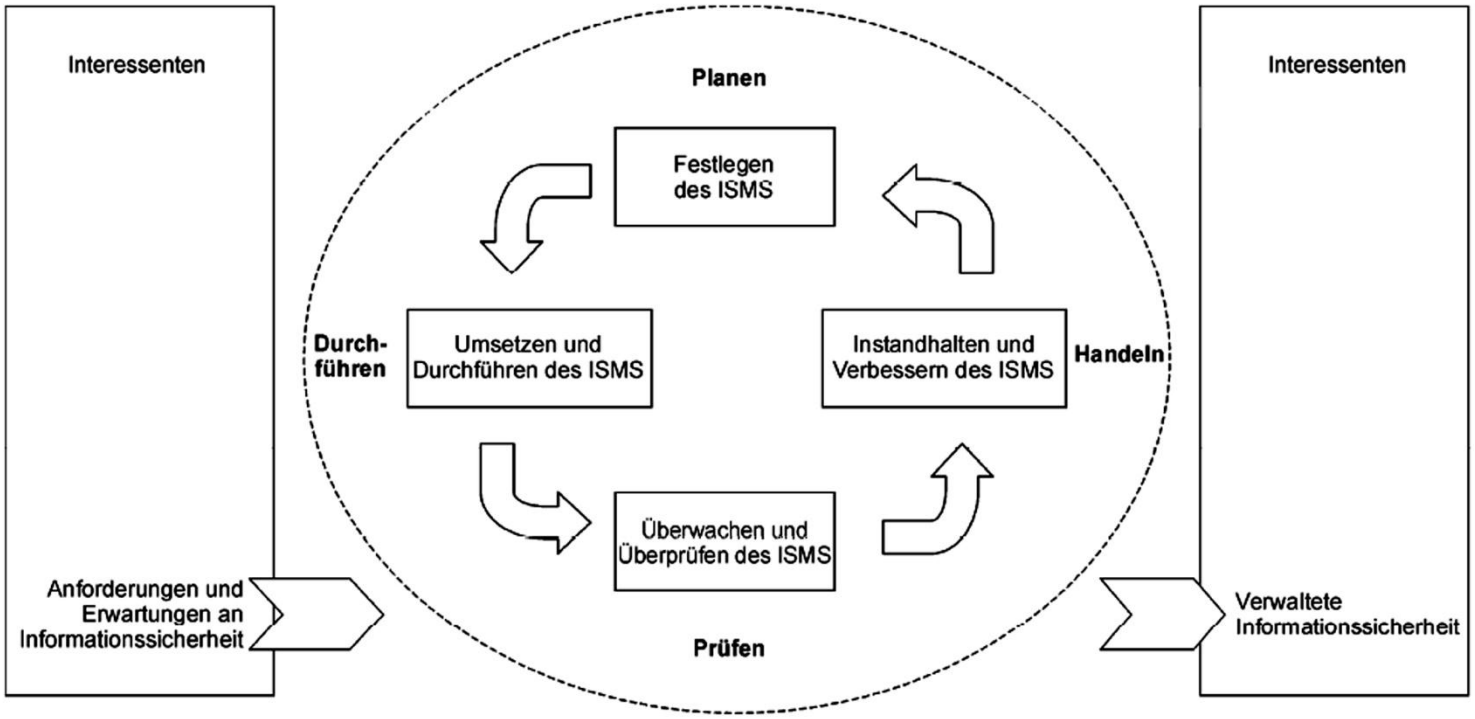
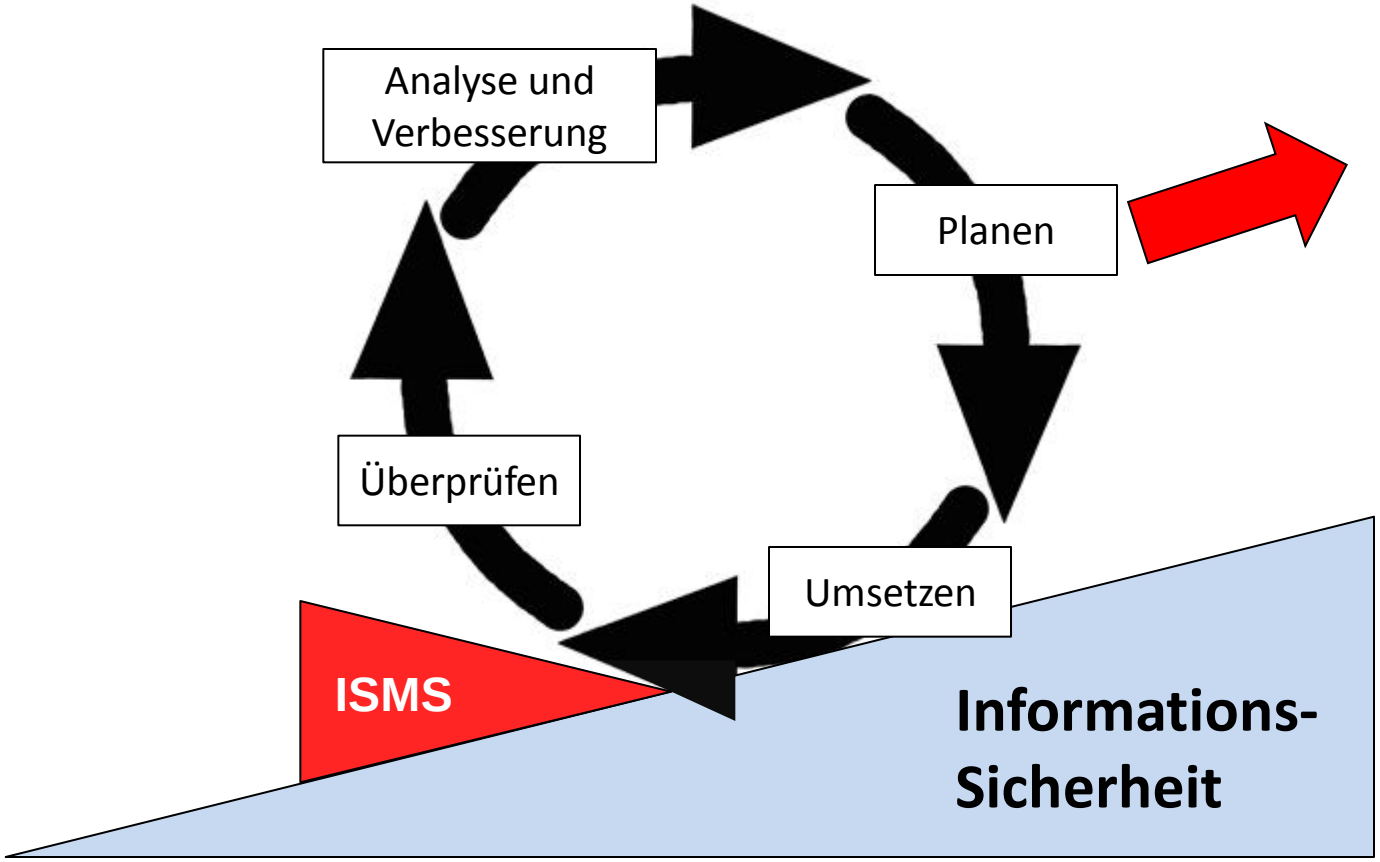
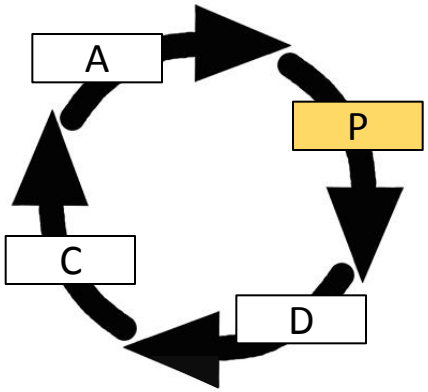


Bild 1 — Auf die ISMS-Prozesse angewandtes PDCA-Modell

Schwerpunkte im Audit



Auditsystematik: Plan



IS-Leitlinie
Grundsätze, Ziele

Risikoeinschätzung
Methode, Kriterien

Assets
identifizieren: „Alles was einen Wert hat“

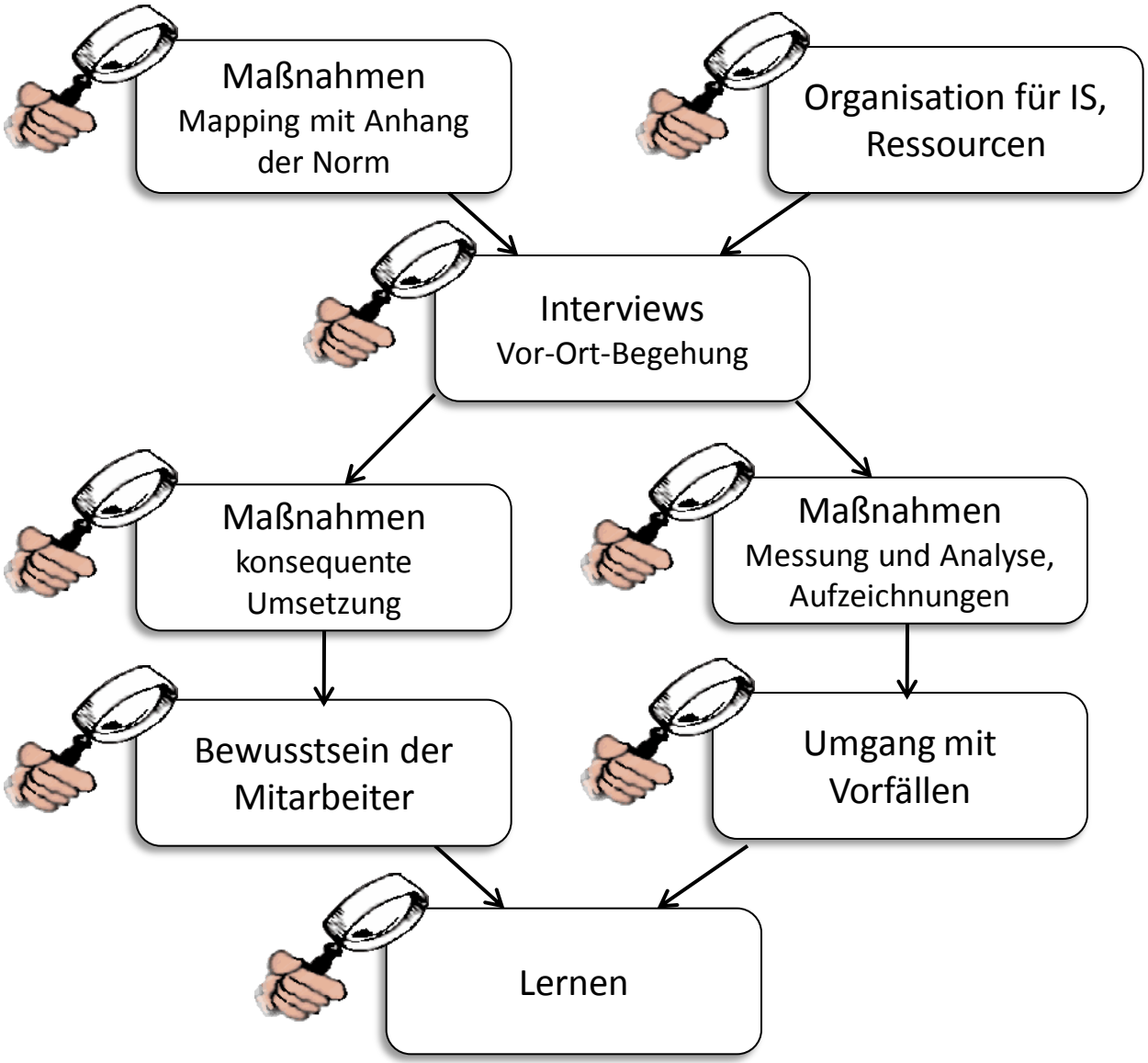
Risiken
identifizieren, analysieren, bewerten

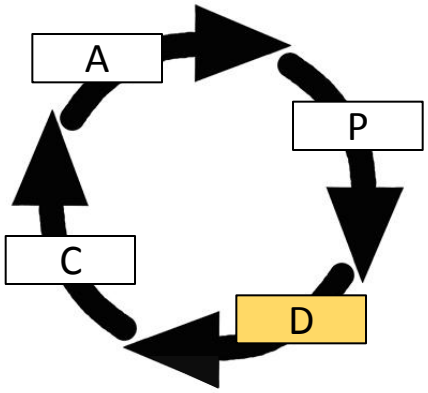
Maßnahmen
auswählen, einführen

Restrisiken
genehmigen

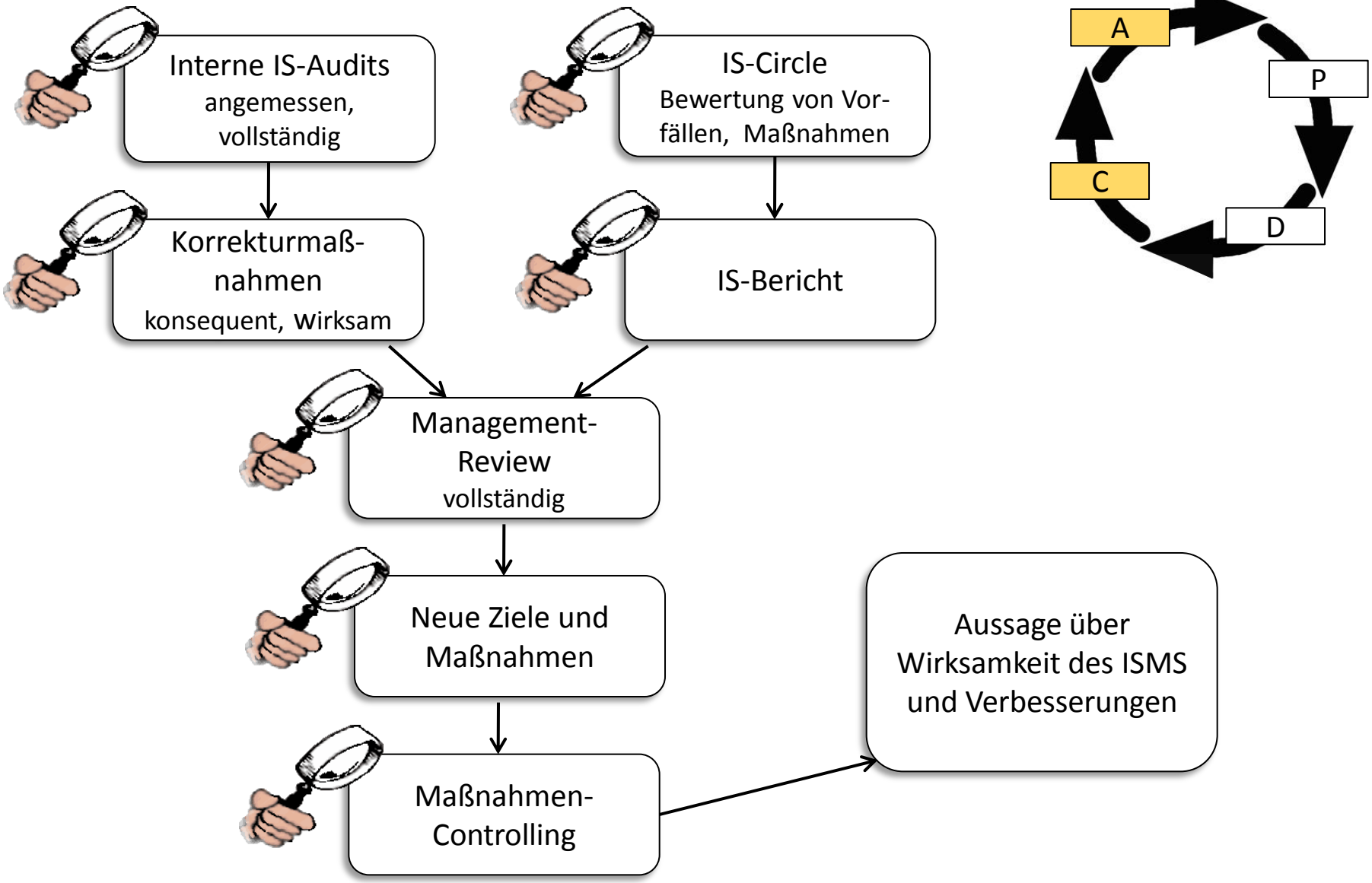
Statement of Applicability

Auditsystematik: Do

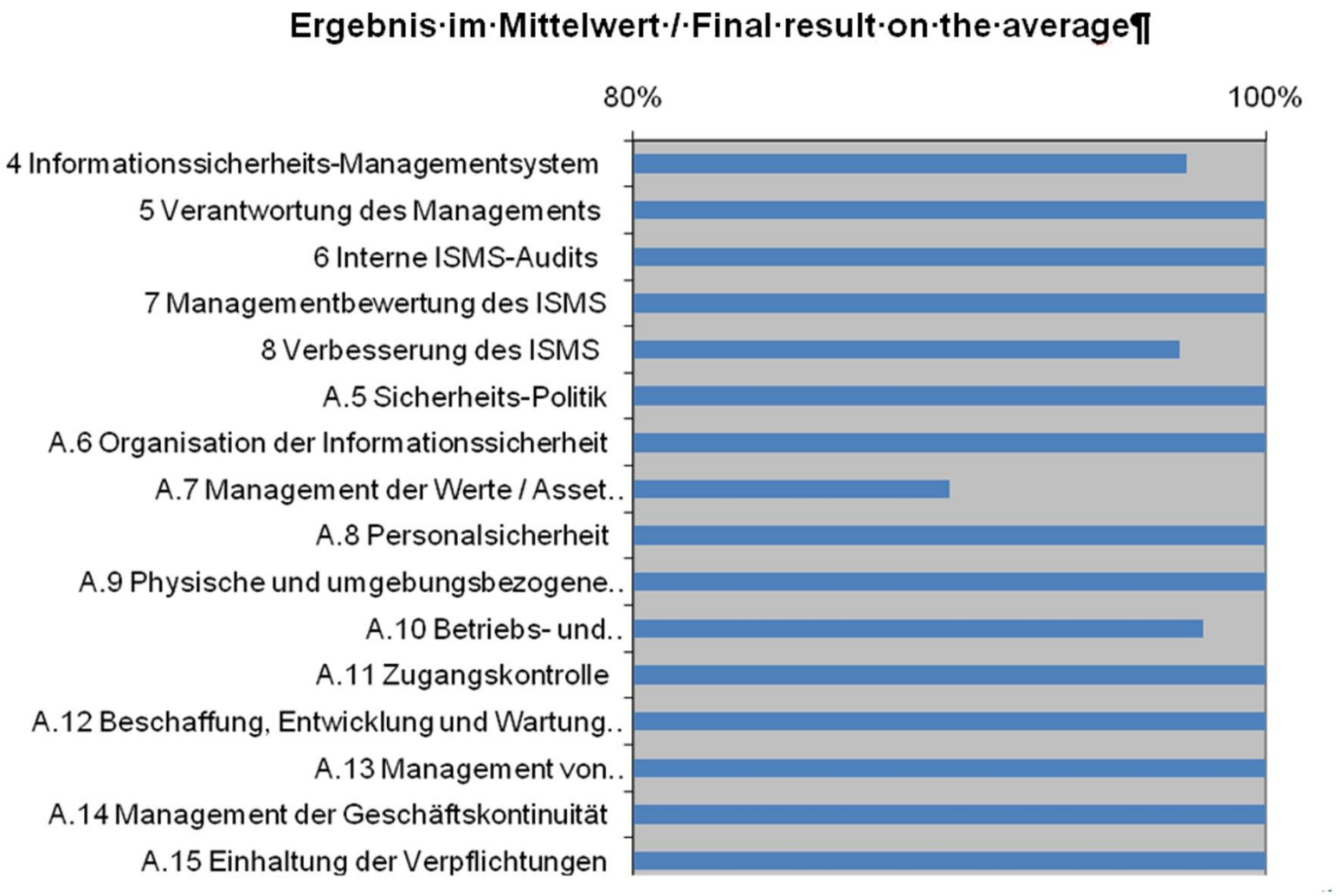




Auditsystematik: Check und Act



Darstellung des Auditergebnisses



Vielen Dank für Ihre Aufmerksamkeit!