



Management Service

TÜV SÜD Management Service GmbH IT- Management ISO/IEC 27000





1. Warum ISO/IEC 27001

2. Grundlagen und Inhalte der ISO/IEC 27001

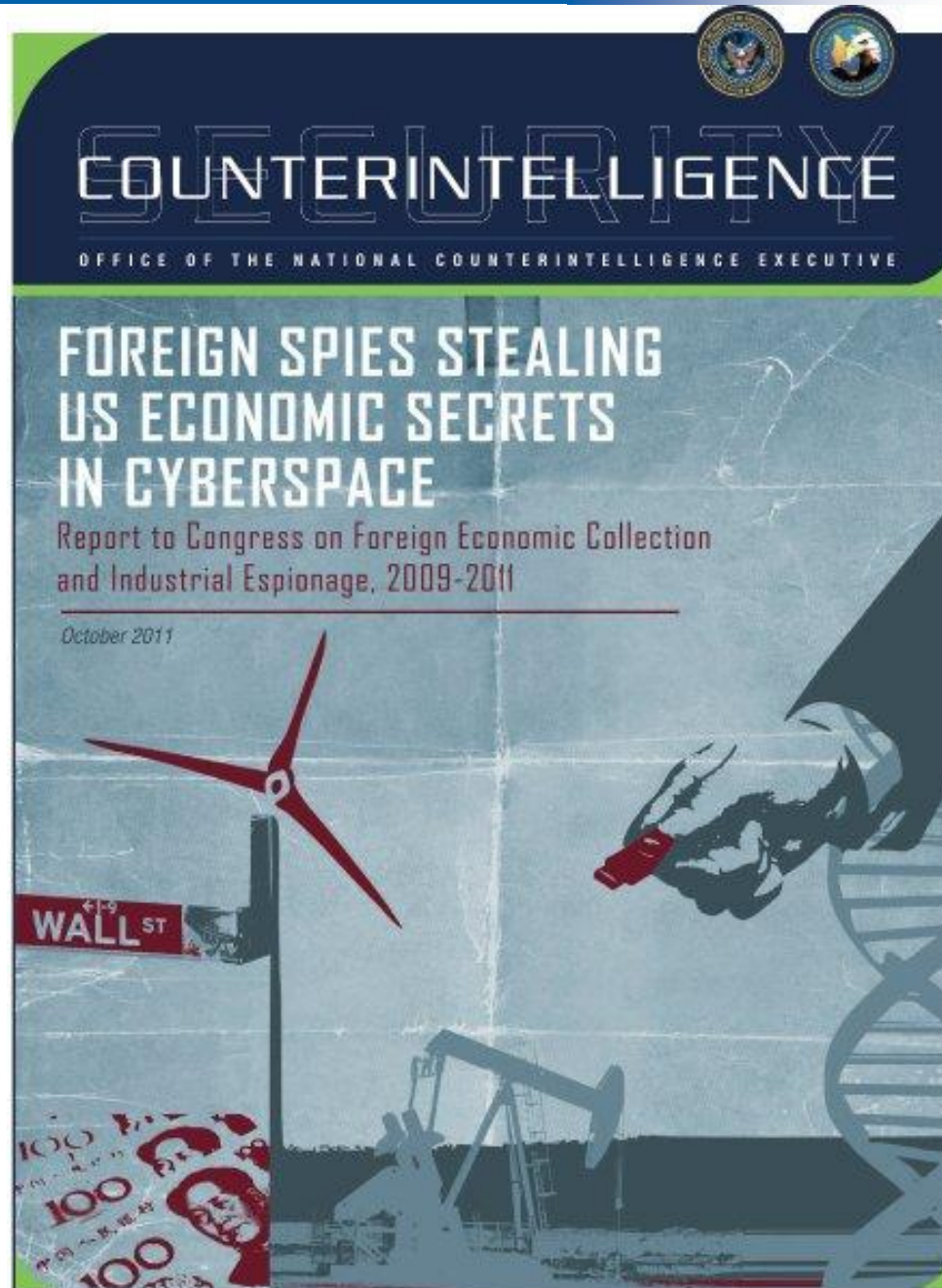
3. Die Implementierung

4. Kritische Erfolgsfaktoren

US-Geheimdienstler schlagen Alarm:

Digitale Wirtschafts- und Industriespionage kosten die Vereinigten Staaten Hunderte Milliarden Dollar, heißt es in einem Bericht an den Kongress. Schuldig seien vor allem Russland und China. [...]

Siehe Spiegel online vom 4.11.11
<http://www.spiegel.de/netzwelt/web/0,1518,795749,00.html>



The Nitro Attacks

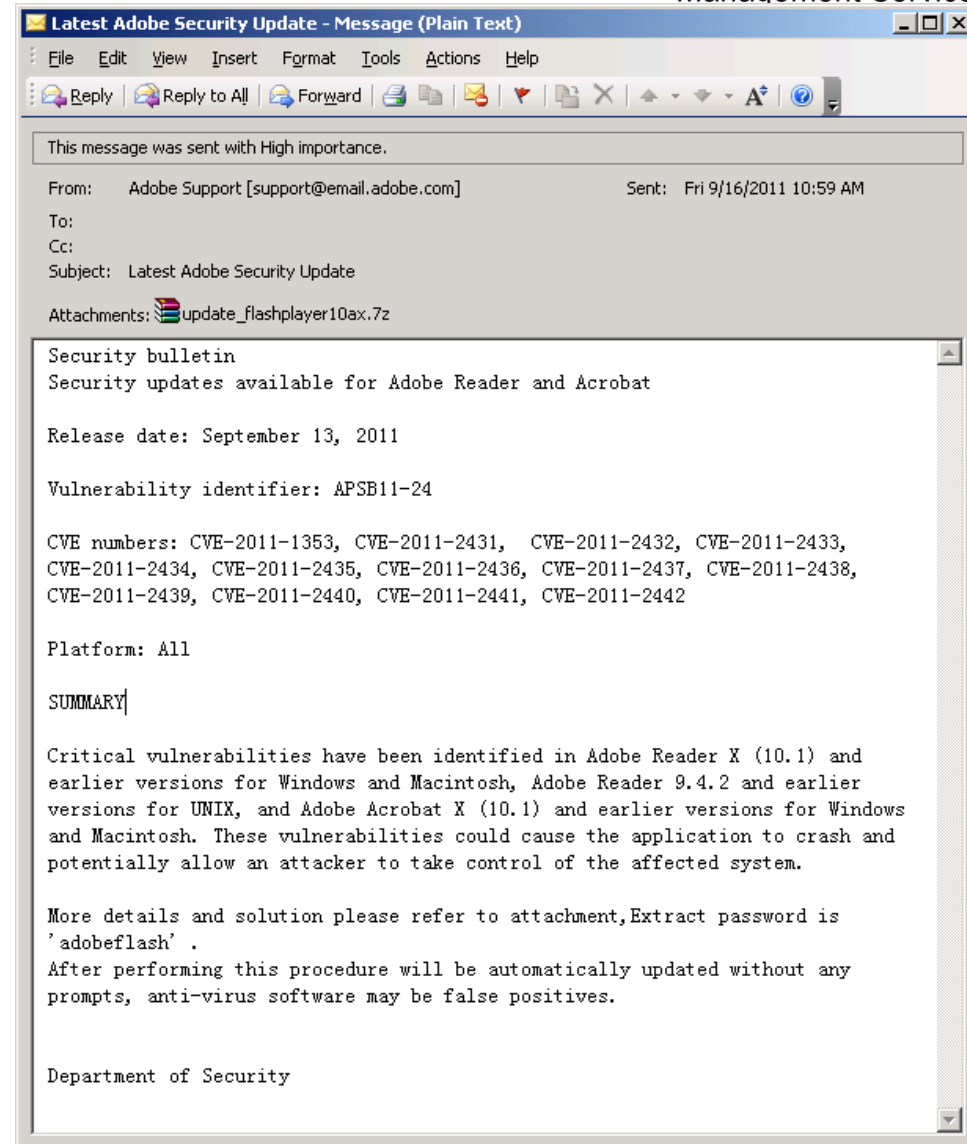
Stealing Secrets from the Chemical Industry

[...] a recent targeted attack campaign directed primarily at private companies involved in the research, development, and manufacture of chemicals and advanced materials. The goal of the attackers appears to be to collect intellectual property such as design documents, formulas, and manufacturing processes.

[...]

These attacks are primarily targeting private industry in search of key intellectual property for competitive advantage, military institutions, and governmental organizations often in search of documents related to current political events and human rights organizations.

Auszug aus einem Whitepaper von Symantec, siehe http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/the_nitro_attacks.pdf



Warum ISO/IEC 27001



Information Security's Biggest Enemy

Management Service

HUMAN BEHAVIOR AND THE PRINCIPLE OF LEAST EFFORT

An Introduction to Human Ecology

by
GEORGE KINGSLEY ZIPF, Ph.D.
Harvard University

www.tspik.ch



Copyright 2002 by Randy Glasbergen. www.glasbergen.com



***“Someone got my Social Security number off the internet
and stole my identity. Thank God — I hated being me!”***



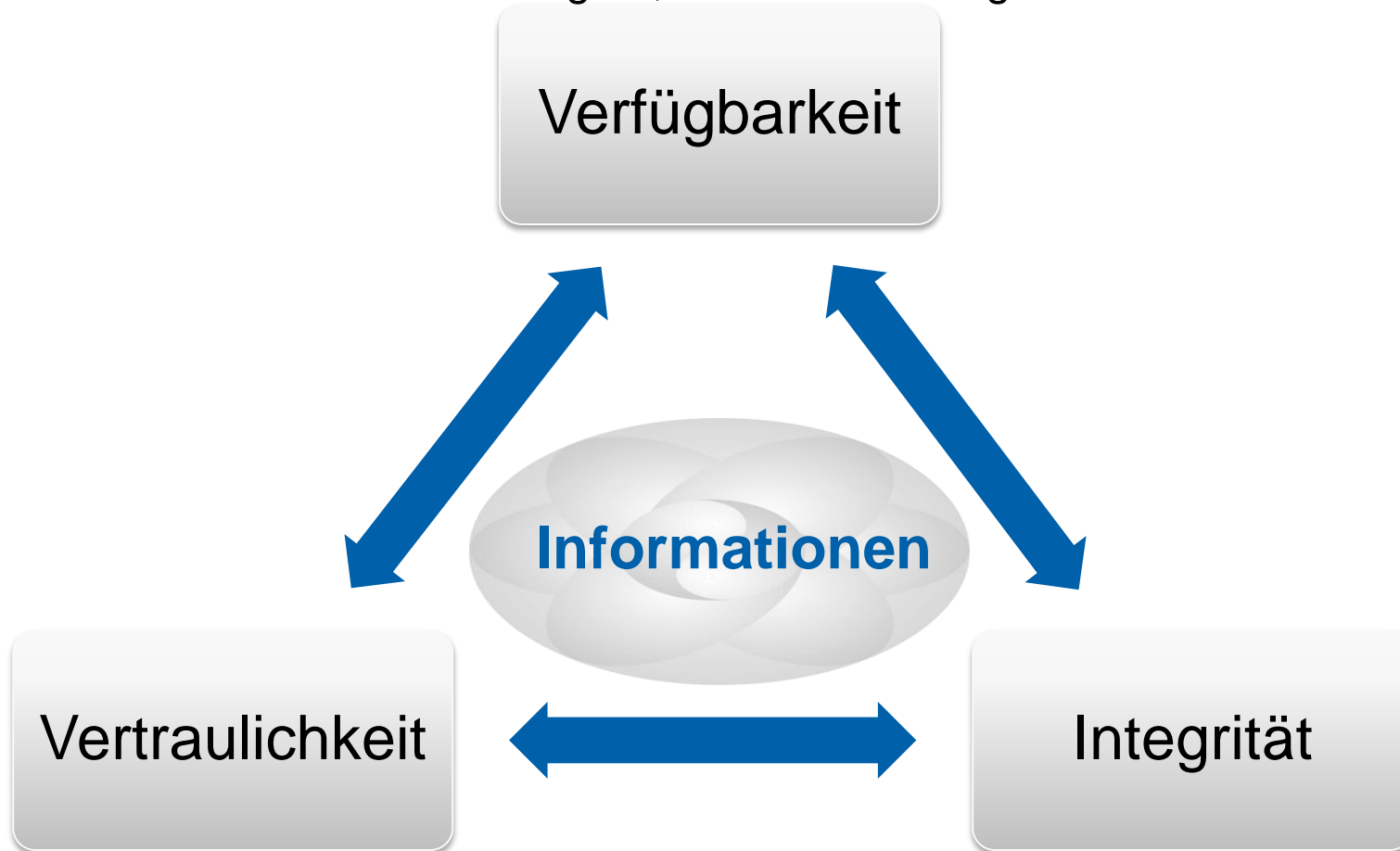
1. Warum ISO/IEC 27001

2. Grundlagen und Inhalte der ISO/IEC 27001

3. Die Implementierung

4. Kritische Erfolgsfaktoren

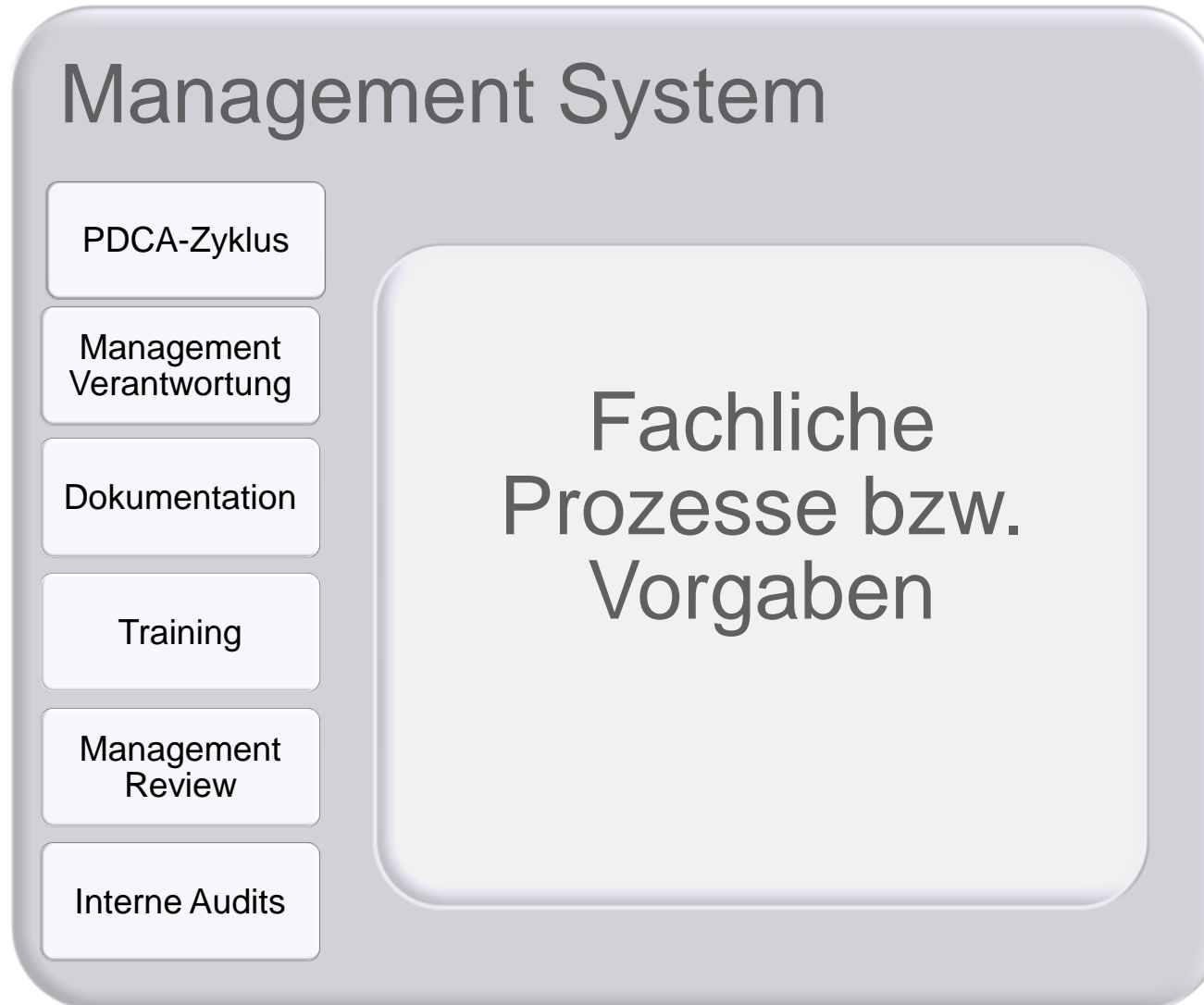
Geschäftskritische Informationen sind dann verfügbar, wenn sie benötigt werden



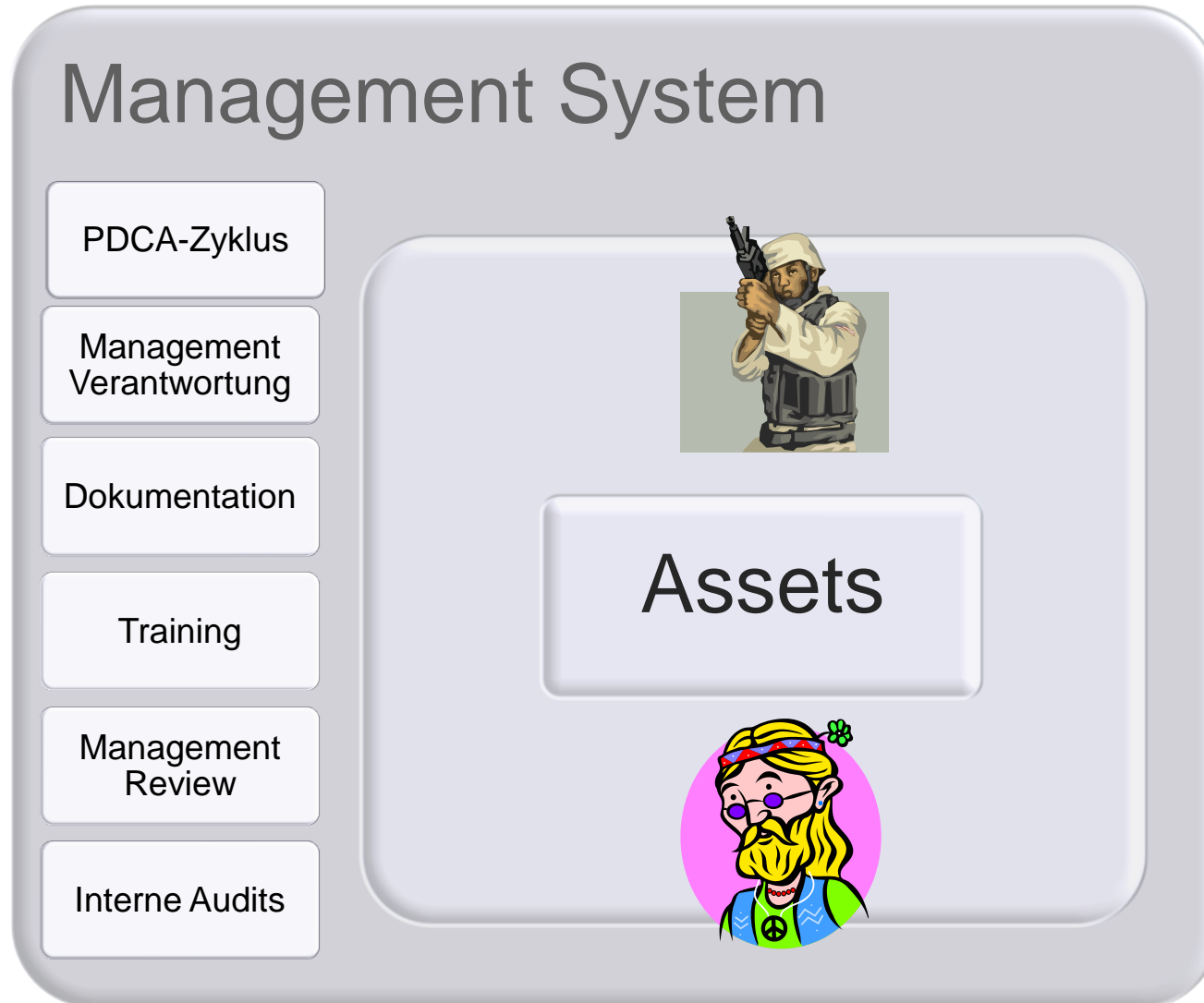
Nur berechtigte Personen dürfen auch auf Informationen zugreifen

Geschäftskritische Informationen sind komplett und vertrauenswürdig

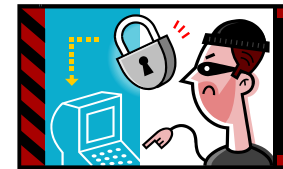
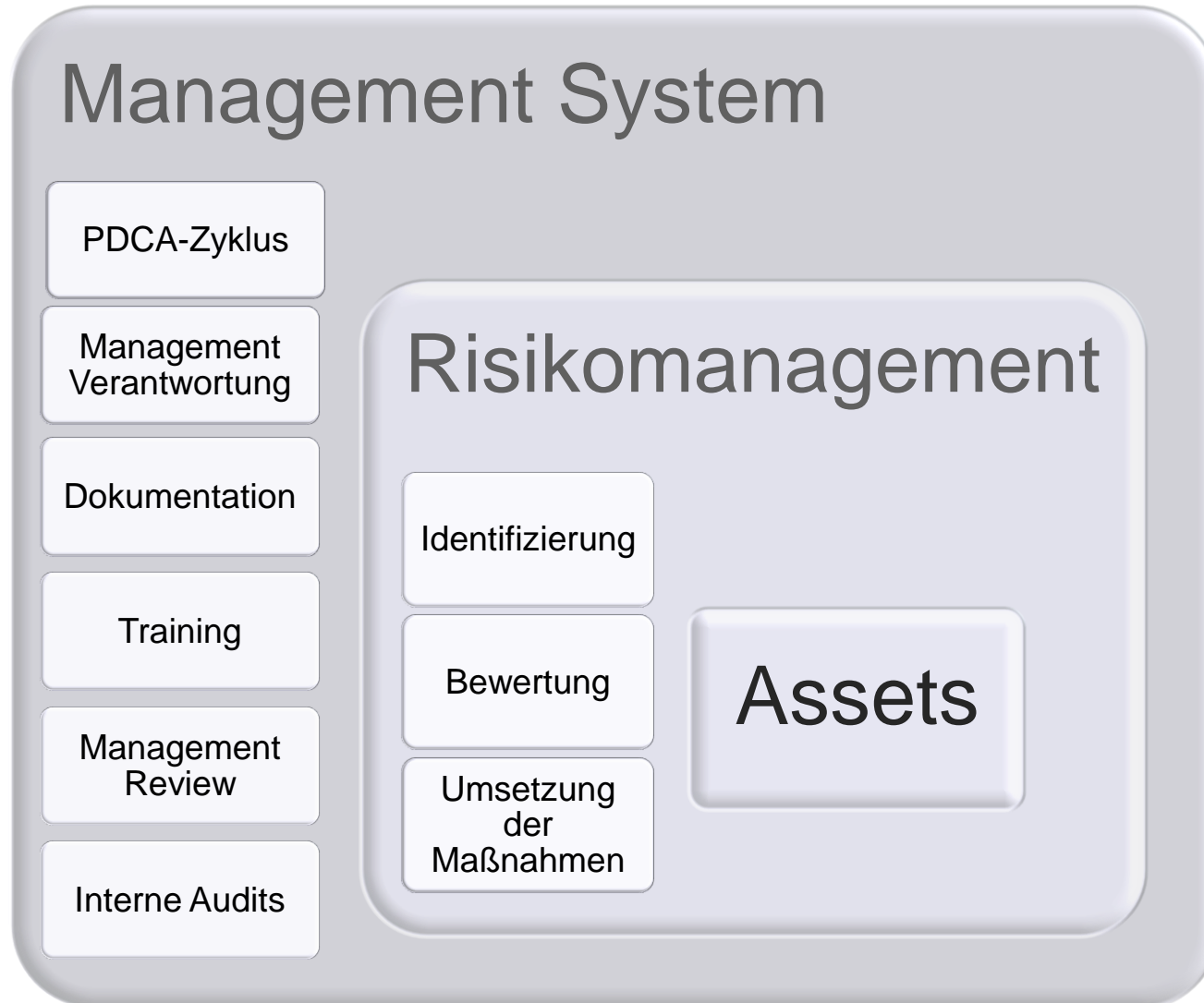
Inhalt einer modernen Norm



Inhalt der ISO/IEC 27001:2005



Inhalt der ISO/IEC 27001:2005



Controls der ISO/IEC 27001:2005

- Management von Informationswerte
- Sicherheit der Personalressourcen
- Physische und umgebungsbezogene Sicherheit
- Management der Kommunikation und der Betriebsabläufe
- Zugriffskontrolle
- Erwerb, Entwicklung und Wartung von Informations-Systemen
- Management von Informationssicherheits-Vorfällen
- Management des kontinuierlichen Geschäftsbetriebes
- Einhaltung von Verpflichtungen



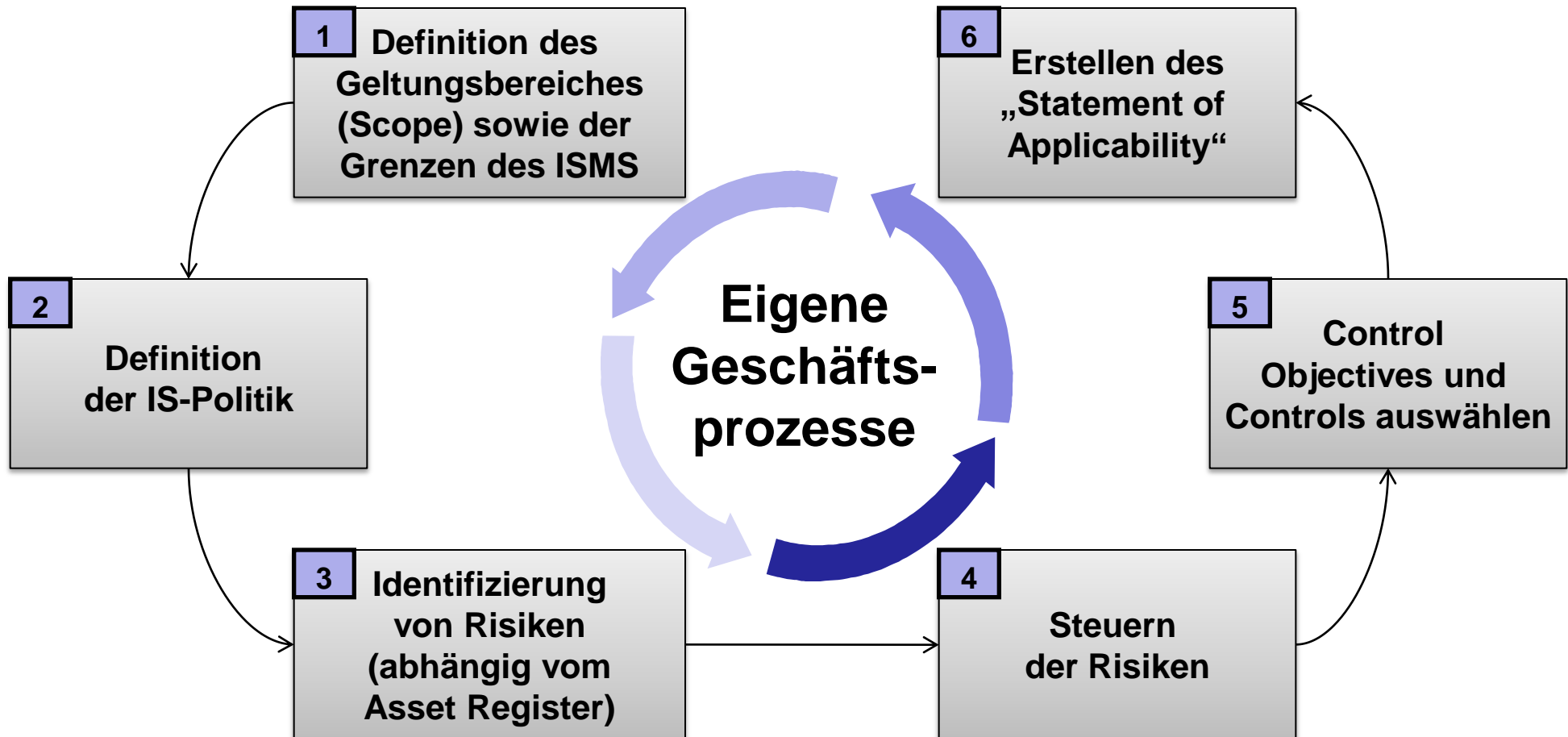
1. Warum ISO/IEC 27001

2. Grundlagen und Inhalte der ISO/IEC 27001

3. Die Implementierung

4. Kritische Erfolgsfaktoren

Die 6 notwendigen Schritte für die Implementierung eines Management-Systems



Control Objectives & Controls auswählen

| | | | |
|---|---|--|--|
| A.5 Security policy (1/2)* | | | |
| A.6 Organization of information security (2/11) | | | |
| A.7 Asset management (2/5) | | | |
| A.8 Human resources security (3/9) | A.9 Physical & environmental security (2/13) | A.10 Communications & operations management (10/32) | A.12 Information systems acquisition, development & maintenance (6/16) |
| A.11 Access control (7/25) | | | |
| A.13 Information security incident management (2/5) | | | |
| A.14 Business continuity management (1/5) | | | |
| A.15 Compliance (3/10) | | | |

* (control objectives / controls)

1. Warum ISO/IEC 27001

2. Grundlagen und Inhalte der ISO/IEC 27001

3. Die Implementierung

4. Kritische Erfolgsfaktoren

Informations Sicherheits Management System (1):

- Informationssicherheits Policy, -Ziele und Maßnahmen
→ müssen sich auf die Geschäftsziele beziehen
- Vorgehen und Vorgehensmodell (PDCA-Framework)
→ in Übereinstimmung mit der Unternehmenskultur
- Unterstützung und Zustimmung vom Management
→ aus allen Hierarchieebenen
- gutes Verständnis von Risiko-Bewertung und -Management
→ Training aller Betroffenen
- Kenntnis der Informationssicherheits Policy
→ Schulung von Managern, Mitarbeitern und Anderen

Informations Sicherheits Management System (2):

- Budgets für Informationssicherheits Management Aktivitäten bereitstellen
 - realistische Kosten einplanen
- vernünftiges Problem-Bewußtsein herbeiführen
 - „Erziehung“ im Schulungsplan aufnehmen
- wirksamen Prozess für Informationssicherheits -Vorfälle einrichten
 - klare Anforderungen vorgeben
- Effizienz und Verbesserung des Informationssicherheits-Management managen
 - Aufbau eines Kennzahlen-Systems

Vielen Dank!
Sie haben noch Fragen ...





Management Service

Backup

1. Warum ISO/ IEC 27000



Management Service



In der heutigen Zeit ist das Business

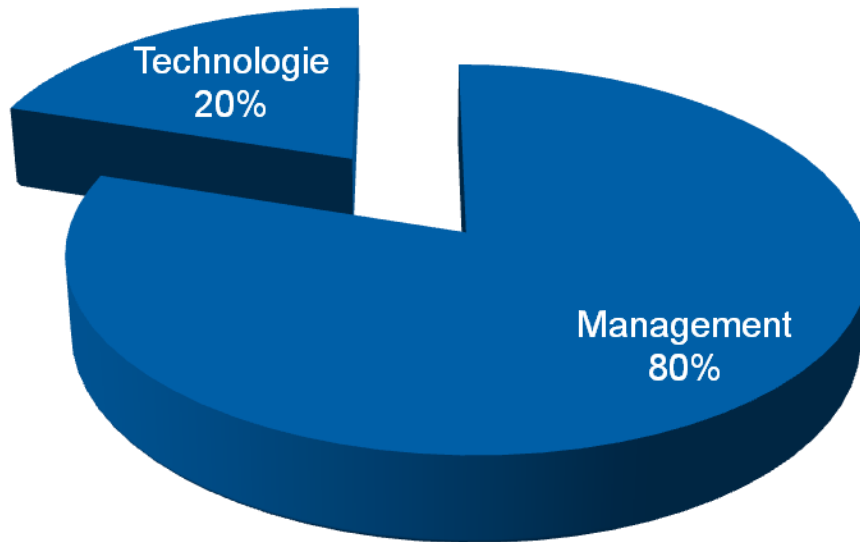
- auf seine Informationen angewiesen
- sehr stark durch IT unterstützt

Jede Unterbrechung des Geschäftsbetriebes in jeglicher Form stellt ein Geschäftsrisiko dar

Jeder Verlust von unternehmenskritischen Informationen kann zu einem bedeutendem Nachteil für das Unternehmen führen

Ein aktives Management der geschäftskritischen Informationen ist dadurch unabdingbar

Informationssicherheit ist ...



MANAGEMENT CHALLENGE OR TECHNICAL ISSUE?

Information security must be seen as a management and business challenge, not simply as a technical issue to be handed over to the experts. To keep your business secure, you must understand both the problems and the solutions. These vary in

... 80 % Management

IS-Policy,
IS-Verantwortlichkeiten,
Bewusstsein & -Training, Reporting,
Business Continuity Planung,
Prozesse, etc.

... 20 % Technologie

Systeme, Tools,
Architektur etc.



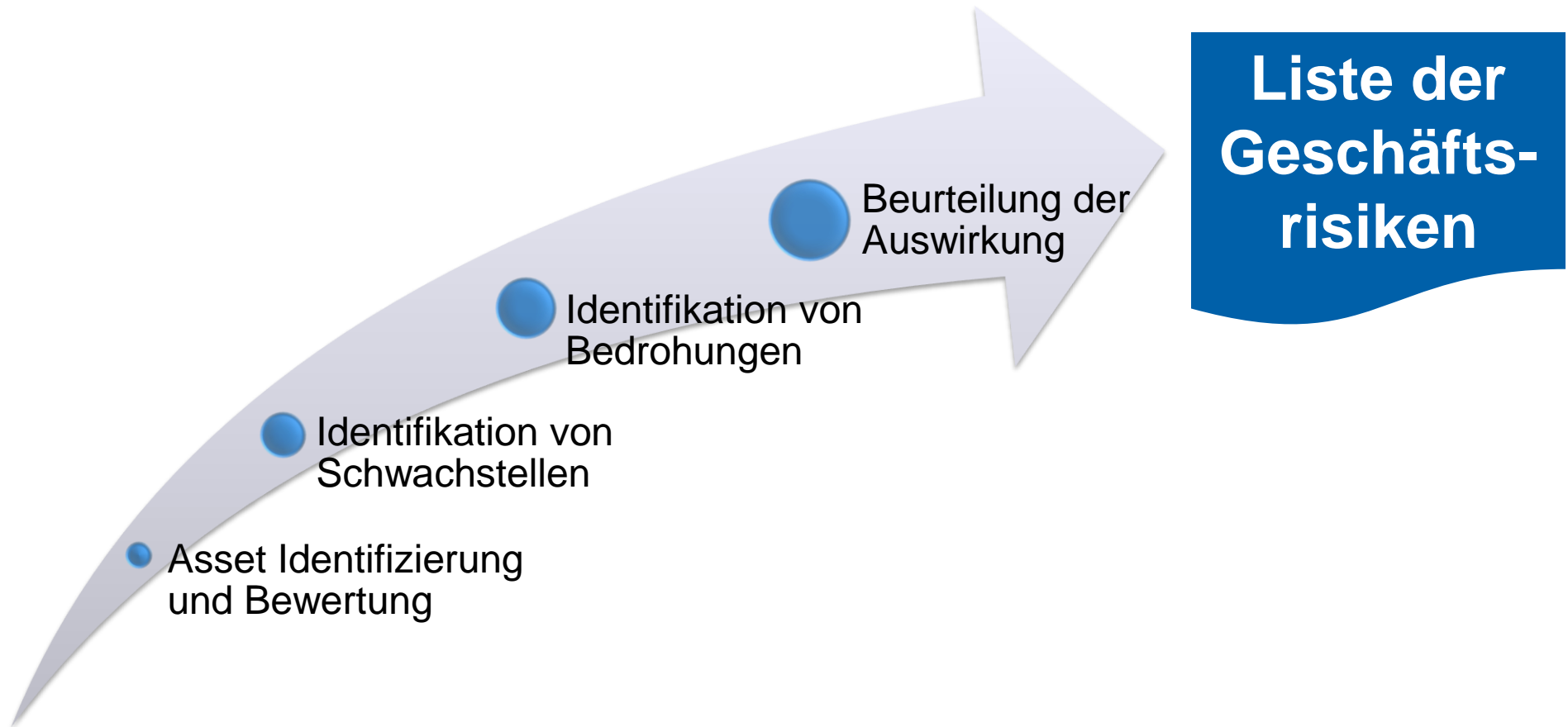
- Schritt 1:
 - Festlegung des Geltungsbereiches (Scope), damit eindeutig ist, für welche Bereiche das ISMS gelten soll
- Schritt 2:
 - Für diesen Geltungsbereich ist eine IS-Policy festzulegen.

3. Die Implementierung



Management Service

Schritt 3: Identifizierung von Risiken

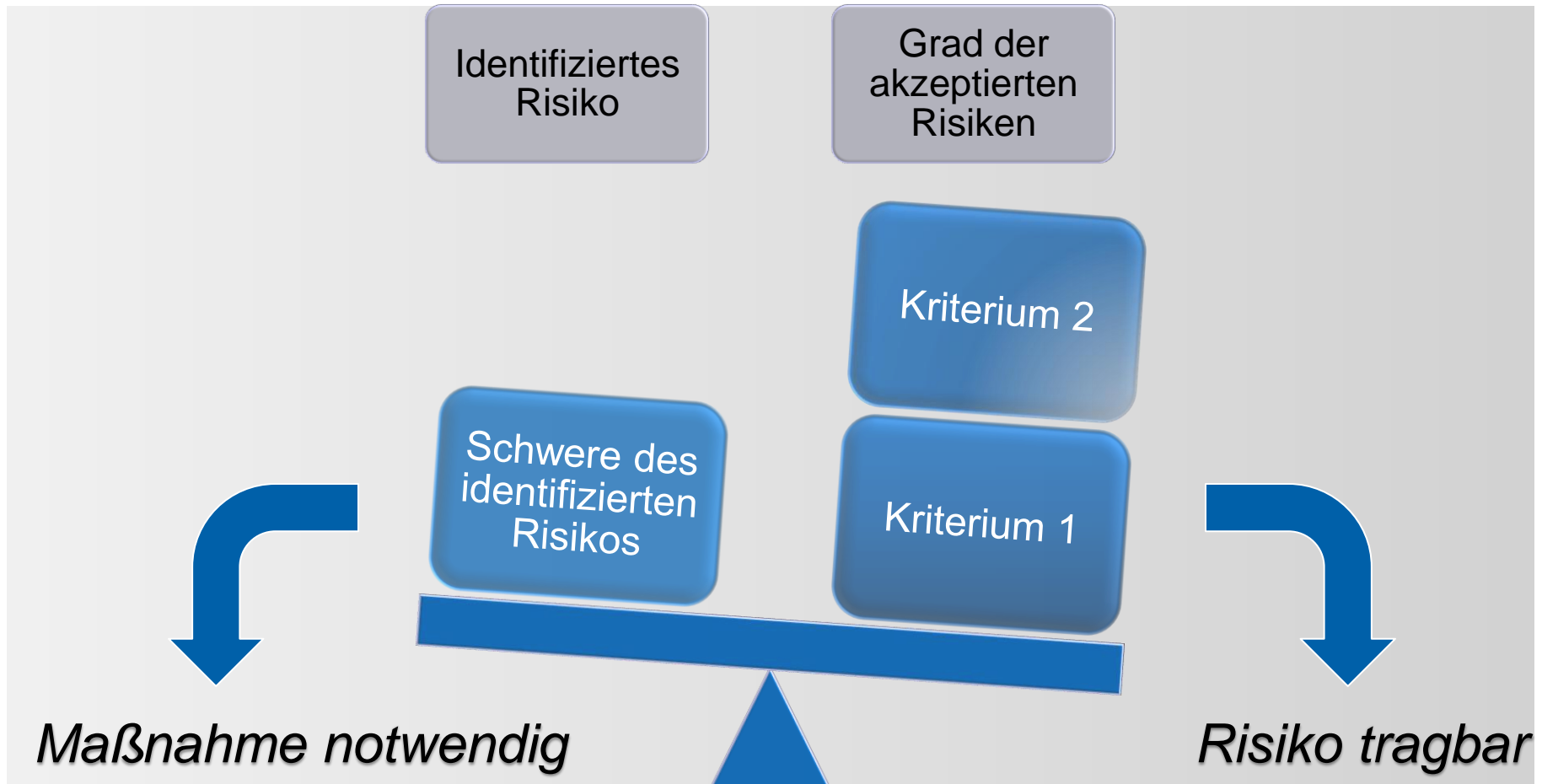


3. Die Implementierung



Management Service

Schritt 4: Steuern der Risiken



3. Die Implementierung



Management Service

Schritt 6: Erstellen des SOA

SOA (Anwendbarkeitserklärung)

Statement of Applicability enthält:

- aktuelle Kontrollziele und Maßnahmen
- Gründe für ihre Auswahl
- Ausschlüsse von Normforderungen
- Rechtfertigungen für die Ausschlüsse

Die SOA enthält zusammen gefasst die Entscheidungen aus dem Risikobehandlungs-Plan.

Das Rechtfertigen der Ausschlüsse wird als Cross-Check verstanden, dass keine Maßnahme vergessen wurde.

(Quelle: ISO 27001:2005; keine Angabe in ISO 17799:2005)

1. Warum ISO/ IEC 27000

2. Grundlagen und Inhalte der ISO/ IEC 27000

3. Die Implementierung

4. Kritische Erfolgsfaktoren

5. Ihr Nutzen

6. Die Zertifizierung

Nutzen einer ISO 27001 Zertifizierung



AGENDA

1. Warum ISO/ IEC 27000

2. Grundlagen und Inhalte der ISO/ IEC 27000

3. Die Implementierung

4. Kritische Erfolgsfaktoren

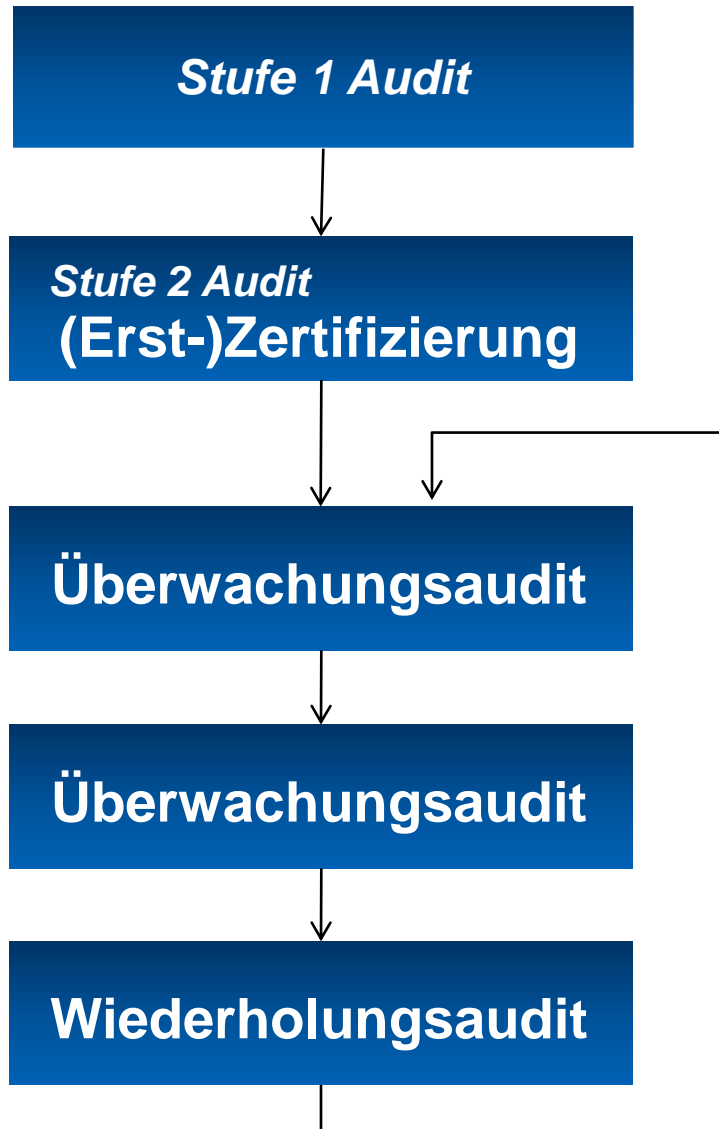
5. Ihr Nutzen

6. Die Zertifizierung

6. Die Zertifizierung



Management Service



Der Ablauf:

- **Projektgespräch**
- **Stufe 1 Audit**
 - Scope und Anwendungsbereich
 - Verständnis und Dokumentation
 - Vorbereitung für die Zertifizierung (Erfolgswahrscheinlichkeit)
- **Stufe 2: Zertifizierungsaudit**
 - Nachweis der Erfüllung der Normforderungen und ihre Wirksamkeit
 - Schritte sind Unterlagenprüfung, Überprüfung vor Ort und Berichterstellung
 - Teilnehmer: (Top-)Management, Prozess-/Systemverantwortliche, Mitarbeiter
- **Gültigkeit**
 - Zertifikat gilt 3 Jahre
 - jährliche Überwachung
- **Aufwand**
 - richtet sich nach Anzahl der Mitarbeiter und der Zahl der Standorte
 - Tabelle als Orientierungsrahmen

6. Die Zertifizierung



Management Service

Ein Zertifikat bedeutet Weitblick



- ihr Managementsystem ständig weiter entwickeln
- effizienter und effektiver werden
- auf das Wesentliche konzentrieren
- weltweit akzeptiert werden
- unsere Stärken nutzen durch
 - erfahrene Auditoren mit hoher Branchenkompetenz
 - das Kommunikationsinstrument „TÜV“
- bessere Chancen bei Ausschreibungen
- Bestätigung durch unabhängigen Dritten

6. Die Zertifizierung



Management Service

Ihr neues Prüfzeichen



Nach bestandener Zertifizierung stellen wir Ihnen Ihr neues Prüfzeichen zum Download im Internet zur Verfügung.

Nutzen Sie die Chance und kommunizieren Sie Ihren ERFOLG an Ihre Mitarbeiter, Lieferanten, Partner und Kunden!

Werben Sie mit unsere starken Marke und binden Sie diese aktiv in Ihre interne und externe Unternehmenskommunikation ein z.B. im Rahmen einer Marketingkampagne

Einsatzbeispiele: im Internet, auf Geschäftspapieren, Flyer, Prospekten, etc.

6. Die Zertifizierung



Management Service

Worauf Sie achten müssen



Qualität eines Zertifikats

- Geltungsbereich
Leistung(en) des Unternehmens, die zertifiziert wurde(n).
- Norm
relevante Bezugsnorm (z. B. ISO/IEC 27001:2005)

IAF-MLA-Logo

- Aussteller des Zertifikats ist eine vom Deutschen Akkreditierungsrat (DAR) anerkannte und ermächtigte Stelle
- weltweite Anerkennung

