ISO/IEC 27001

Der internationale Standard für das Management der Informationssicherheit

Michael Brenner, Leibniz-Rechenzentrum
Markus Giese, TÜV Süd

Welche Fragen soll dieser Vortrag beantworten?

Was ist Informationssicherheit (und warum ist sie wichtig)?

Was heißt Management der Informationssicherheit?

Was ist ISO/IEC 27001? Was hat es mit den anderen 27000er-Normen auf sich?

Wie sieht Management der Informationssicherheit nach ISO/IEC 27001 aus?

Was bedeutet „ISO/IEC 27001 Zertifizierung“?

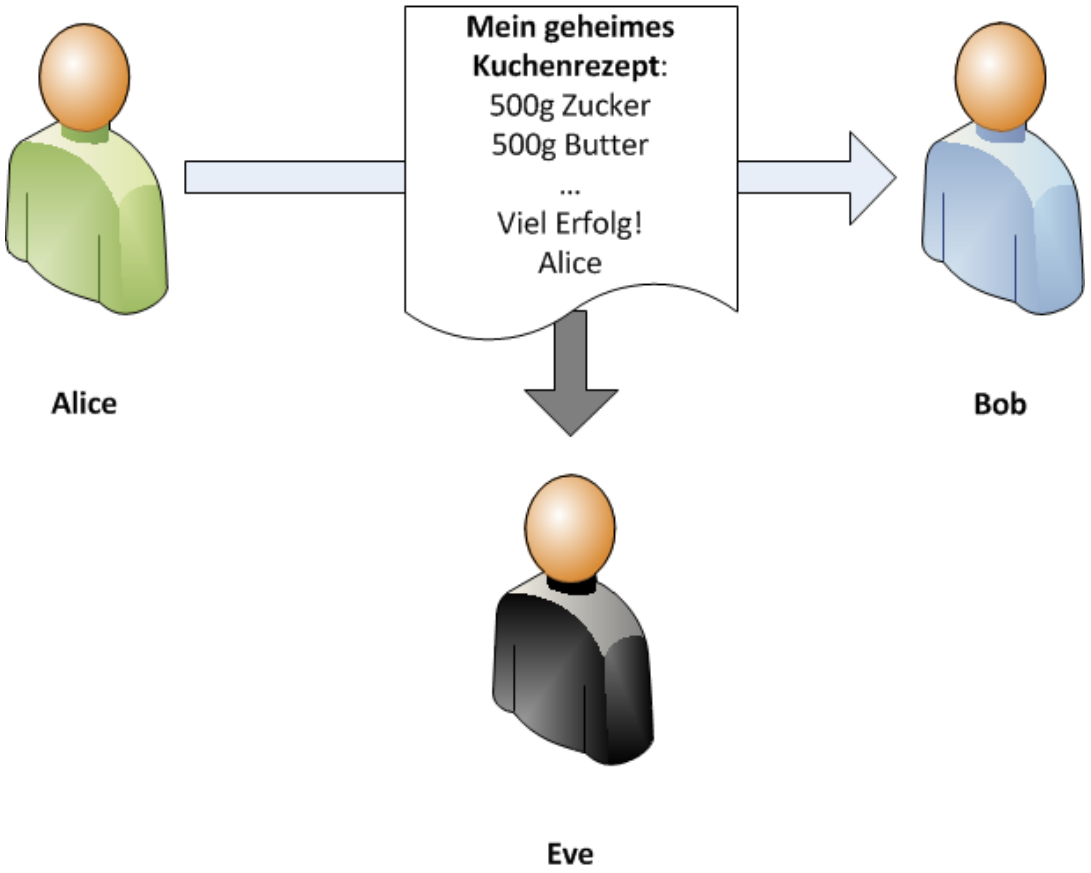
Was ist Informationssicherheit (und warum ist sie wichtig)?

Informationssicherheit

- Informationen sind wichtige Unternehmenswerte
- Informationssicherheit befasst sich mit der **Vertraulichkeit**, **Integrität** und **Verfügbarkeit** von Information;
  engl.: *Confidentiality, Integrity, Availability*
  (gerne CIA abgekürzt)
- Zusätzliche Schutzziele sind möglich: Authentizität, Nicht-Abstreitbarkeit, usw.
- Informationen werden heute überwiegend mit IT-Systemen übertragen, verarbeitet, gespeichert. Informationssicherheit daher auch (aber nicht nur) ein zentrales Thema des IT-Managements.

Vertraulichkeit

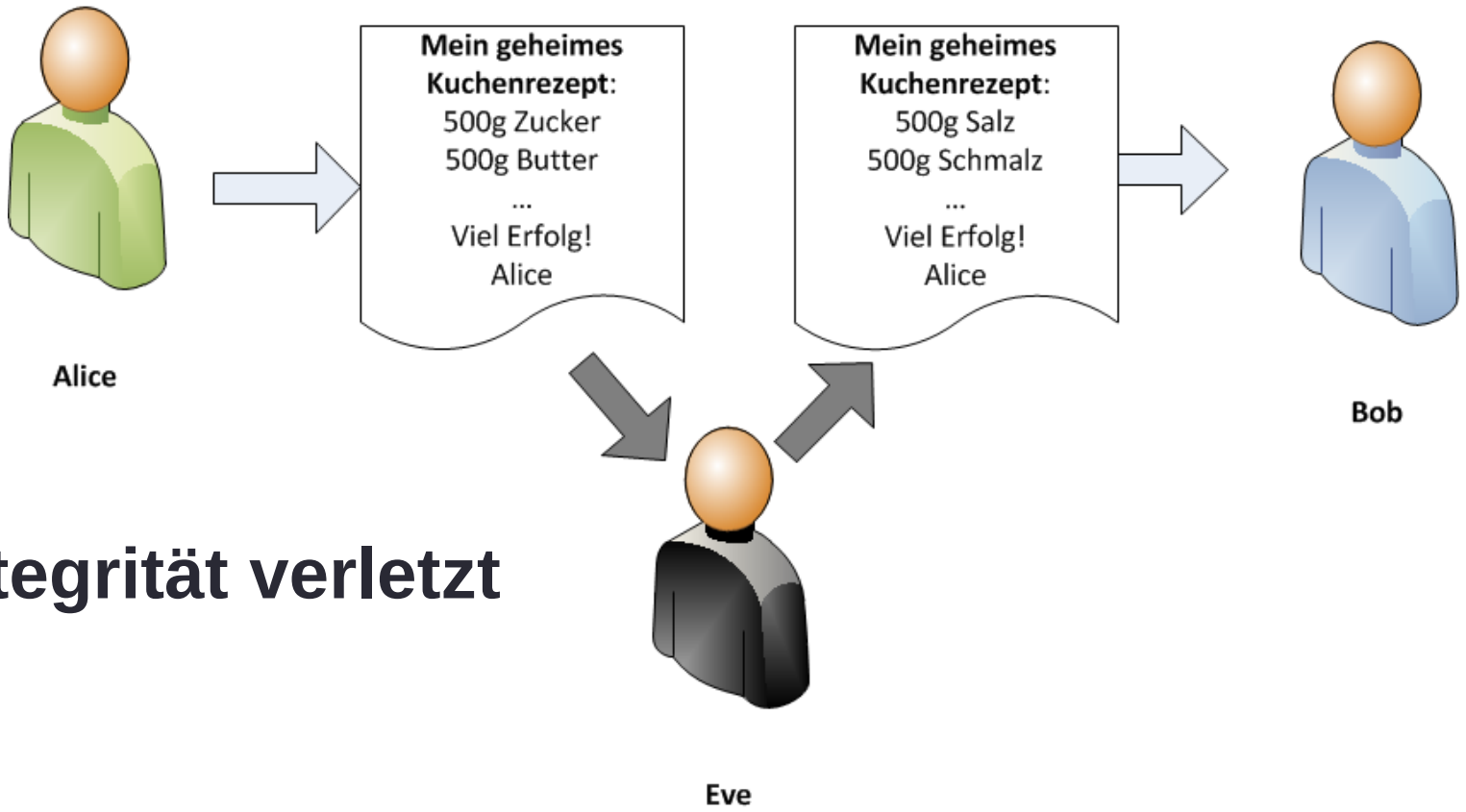
- Alice möchte Bob mit seinem Coffeeshop helfen und ihm dafür ihr geheimes Kuchenrezept zur Verfügung stellen.
- Bobs Konkurrentin Eve kann das Rezept ebenfalls lesen



Vertraulichkeit verletzt

Integrität

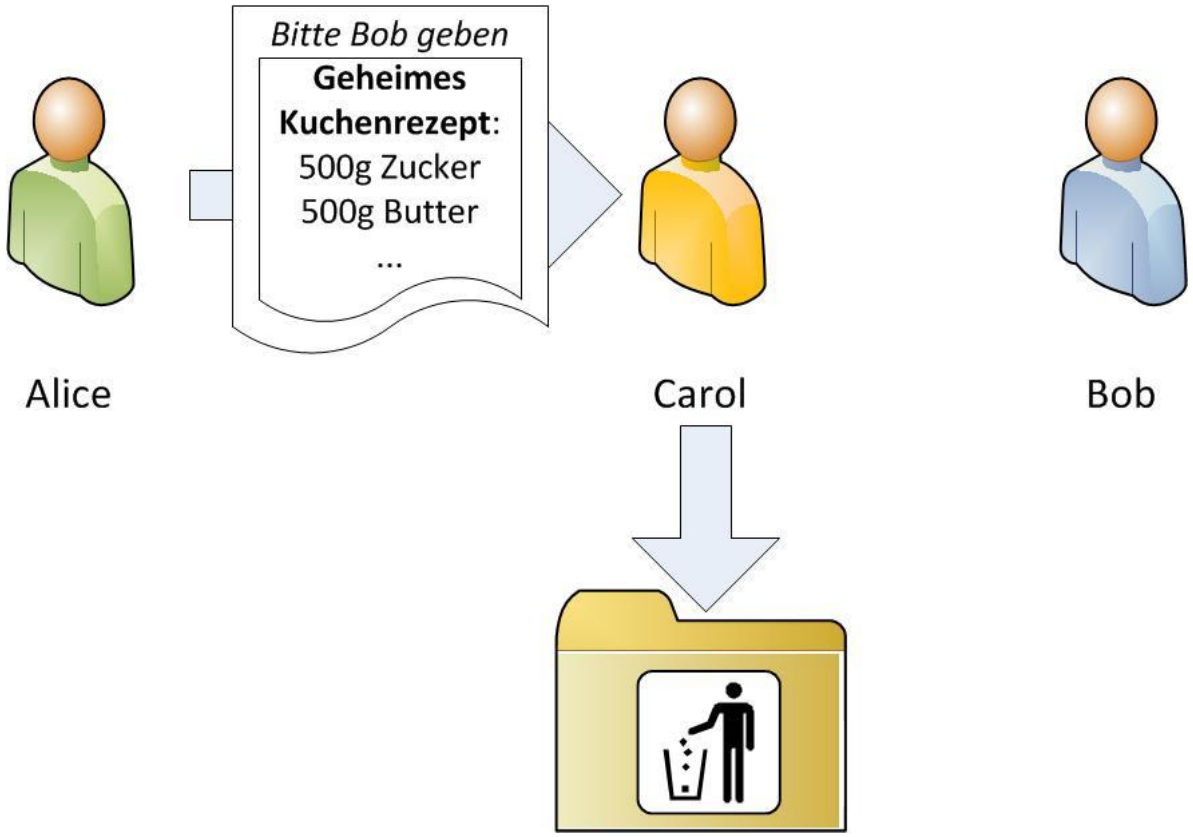
- Eve manipuliert das Rezept (unbemerkt von Bob)



Integrität verletzt

Verfügbarkeit

- Carol „entsorgt“ versehentlich das für Bob bestimmte Rezept



Verfügbarkeit verletzt

Öffentlich bekannte Informationssicherheitsvorfälle

- Sony, April 2011
  - Hacker nutzen eine bekannte Schwachstelle der für das Playstation Network verwendeten Web Applikation Server Plattform
  - 77 Millionen Kundendaten gestohlen, Playtstation Network 23 Tage offline
  - 170 Millionen US$ direkte Kosten (ca. 1% der Marktkapitalisierung)
- RSA (EMC-Tochter), März 2011
  - Mitarbeiter öffnet Phishing-Mail, Installation einer Backdoor im Mitarbeiter-PC durch Ausnutzen einer bis dahin unbekannten Flash-Schwachstelle
  - Daten zu SecureID-Token-System in unbekanntem Ausmaß gestohlen, Ausnutzung dieser Daten bei späteren Angriffen u.a. auf Lockheed Martin
  - 63 Millionen US$ direkte Kosten
- HMRC (Britische Steuerbehörde), 2007
  - Mitarbeiter versenden Daten aller britischen Kindergeldempfänger auf CD; die Sendung kommt nie an
  - Verbleib der Personen- und Kontodaten von 7,25 Millionen Familien unklar
  - Schatzkanzler bleibt, Vorsitzender der Steuerbehörde nimmt seinen Hut

Öffentlich bekannte Informationssicherheitsvorfälle (cont.)

- Barings Bank, 1993-1995
  - Trader Nick Leeson manipuliert die Berichtsdaten seiner Futures- und Optionsgeschäfte
  - Verluste bleiben unentdeckt, bis ein Schaden von 827 Mio. Pfund entstanden ist (berichtet werden Gewinne von 56 Mio. Pfund)
  - Barings Bank erklärt Bankrott, wird für den symbolische Preis von 1 Pfund von der ING Group übernommen
- Ma.gnolia, 2009
  - Datenbank aufgrund eines Festplattenfehlers korrumpiert; Wiederherstellung des Backups erfolglos
  - Ca. 500GB Dienst- und Kundendaten verloren
  - Einstellung des Betriebs

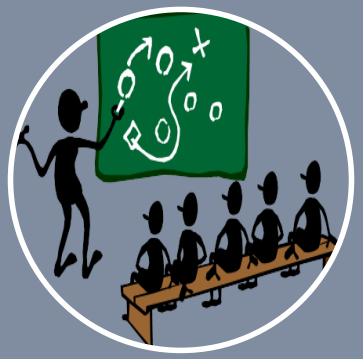
Verlust von Vertraulichkeit, Integrität und Verfügbarkeit kann erhebliche Konsequenzen, bis hin zur Gefährdung der Unternehmensexistenz, haben.

Was heißt Management der Informationssicherheit?

Technische und organisatorische Sicht auf die Informationssicherheit

Sicherheitstechnik

- Verschlüsselung, Signatur
- Systemhärtung
- Firewall, Intrusion Detection System
- ISO/IEC 10181, ISO/IEC 15408
- …



Sicherheitsmanagement

- Information Security Policy
- Risikoanalyse
- Security Incident Response Prozess
- ISO/IEC 27001, ISO/IEC 27002
- …

Informationssicherheits-Managementsystem

- Ein rein technisches „Management“ der Informationssicherheit greift zu kurz!
- Benötigt wird ein ***Informationssicherheits-Managementsystem*** / ***Information Security Management System*** (***ISMS***)
- Ein ISMS ist ein System aus Leitlinien, Verfahren, Regelungen und zugehörigen Ressourcen, welche dazu dienen, die Ziele einer Organisation im Bereich Informationssicherheit zu erreichen.

Was ist ISO/IEC 27001? Was hat es mit den anderen 27000er-Normen auf sich?

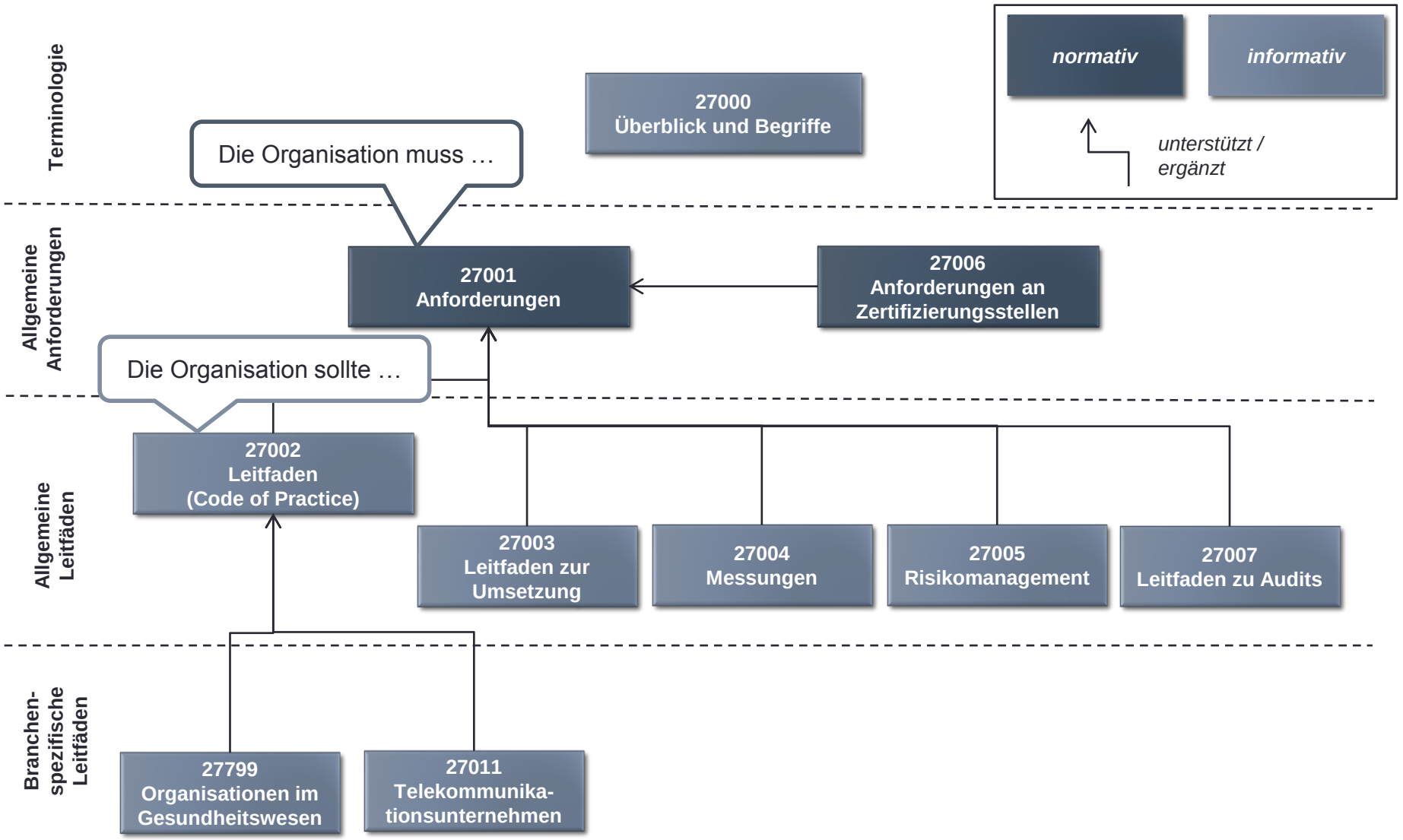
ISO/IEC 27001

- Vollständiger Titel:
  Informationstechnik – IT-Sicherheitsverfahren – Informationssicherheits-Managementsysteme – Anforderungen (ISO/IEC 27001:2005)
- Historie: Britischer Standard BS 7799 als Grundlage
  - BS 7799-1 → ISO/IEC 17799 → ISO/IEC 27002
  - BS 7799-2 → ISO/IEC 27001
- Zur Zeit halten über 7500 Organisationen ein ISO/IEC 27001 oder äquivalentes Zertifikat (http://www.iso27001certificates.com/)

Was liefert ISO/IEC 27001? Was nicht?

- ISO/IEC 27001 ist
  - Ein Dokument mit 34 Standard-Seiten
  - Eine Sammlung von Anforderungen an ein Information Security Management System (ISMS)
  - Ein internationaler, zertifizierbarer Standard zum Management der Informationssicherheit
  - Ein zentraler Bestandteil der ISO/IEC 27000 Standardfamilie
  - In Bereichen überlappend mit ISO 9001 und ISO/IEC 20000-1
- ISO/IEC 27001 ist **nicht**
  - Geeignet zur Bewertung von Sicherheitstechnik oder Software
  - Ein fertiges Referenzmodell für ein ISMS
  - Ohne Hintergrundwissen oder „Sekundärliteratur“ einsetzbar

Die ISO/IEC 27000-Familie



Wie sieht Management der Informationssicherheit nach ISO/IEC 27001 aus?

ISO/IEC 27001 - Aufbau

1 Anwendungsbereich
- 1.1 Allgemeine
- 1.2 Anwendung

2 Normative Verweisungen

3 Begriffe

4 Informationssicherheits-Managementsystem
- 4.1 Allgemeine Anforderungen
- 4.2 Festlegung und Verwaltung des ISMS
- 4.3 Dokumentationsanforderungen

5 Verantwortung des Managements
- 5.1 Verpflichtung des Managements
- 5.2 Management von Ressourcen

6 Interne ISMS-Audits

7 Managementbewertung des ISMS
- 7.1 Allgemeines
- 7.2 Eingaben für die Bewertung
- 7.3 Ergebnisse der Bewertung

8 Verbesserung des ISMS
- 8.1 Ständige Verbesserung
- 8.2 Korrekturmaßnahmen
- 8.3 Vorbeugemaßnahmen

Anhang A (normativ) - Maßnahmenziele und Maßnahmen

Zentrale Komponenten eines ISMS nach ISO/IEC 27001

Das Zusammenspiel der Komponenten macht das System aus!

Ständige Verbesserung

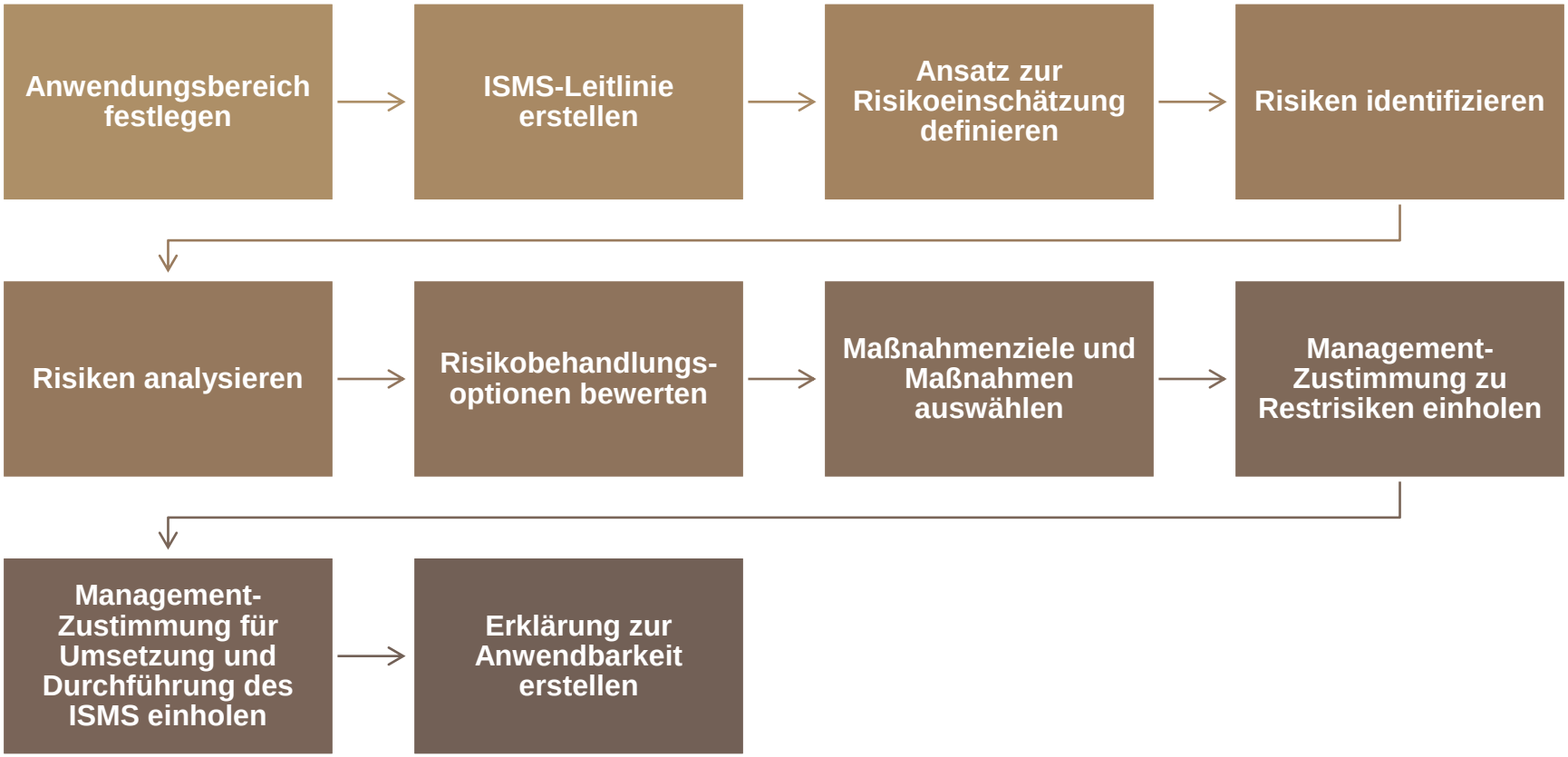
Instandhalten und Verbessern des ISMS
- Korrekturmaßnahmen
- Verbesserungen
- …

Festlegen des ISMS
- Definition Anwendungsbereich
- ISMS-Leitlinie erstellen
- Risiken einschätzen
- …

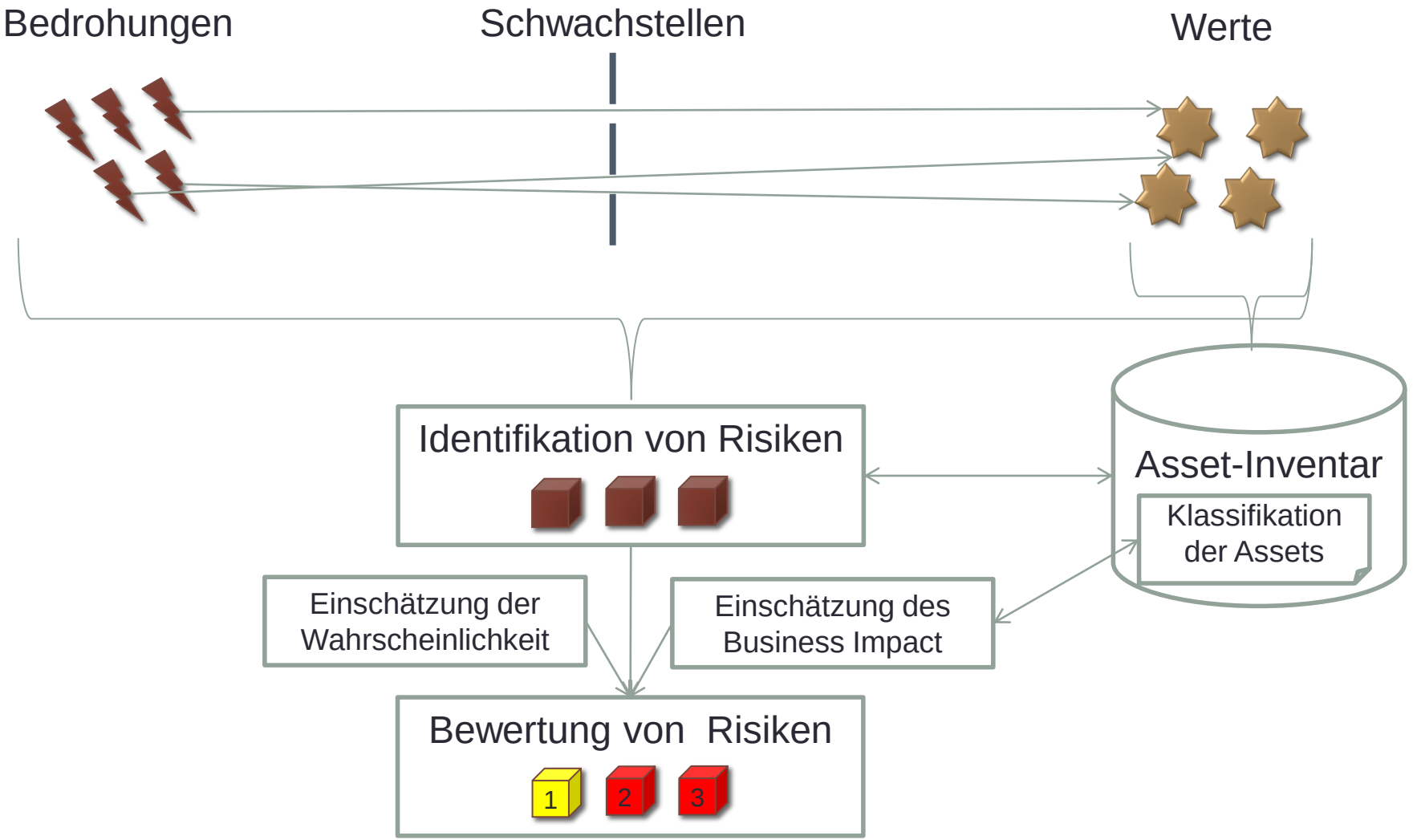
Überwachen und Überprüfen des ISMS
- ISMS-Audits
- Managementbewertungen
- …

Umsetzung und Durchführung des ISMS
- Risikobehandlung
- Umsetzung von Maßnahmen
- …

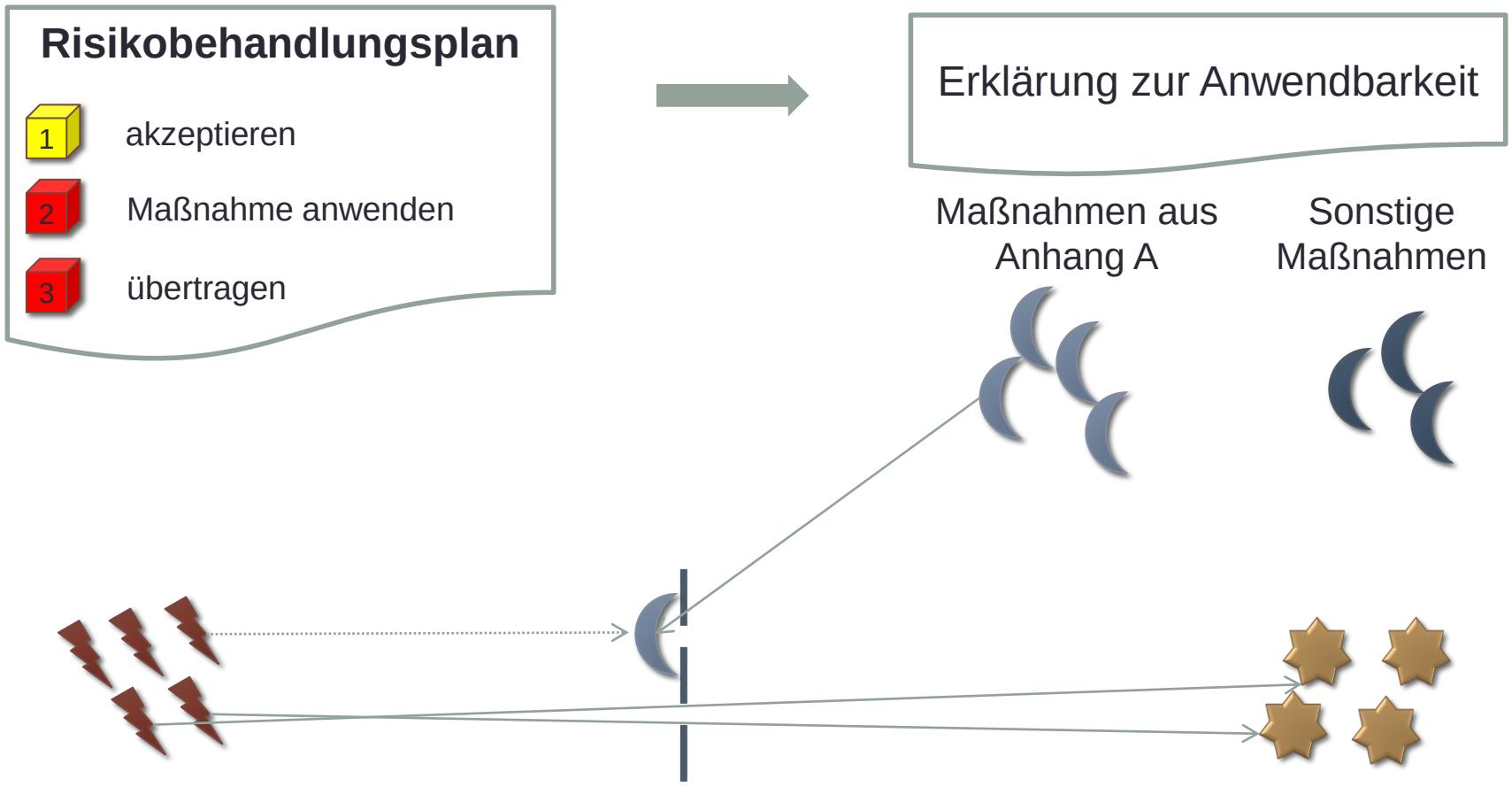
Festlegen / Planen des ISMS



Risikoeinschätzung

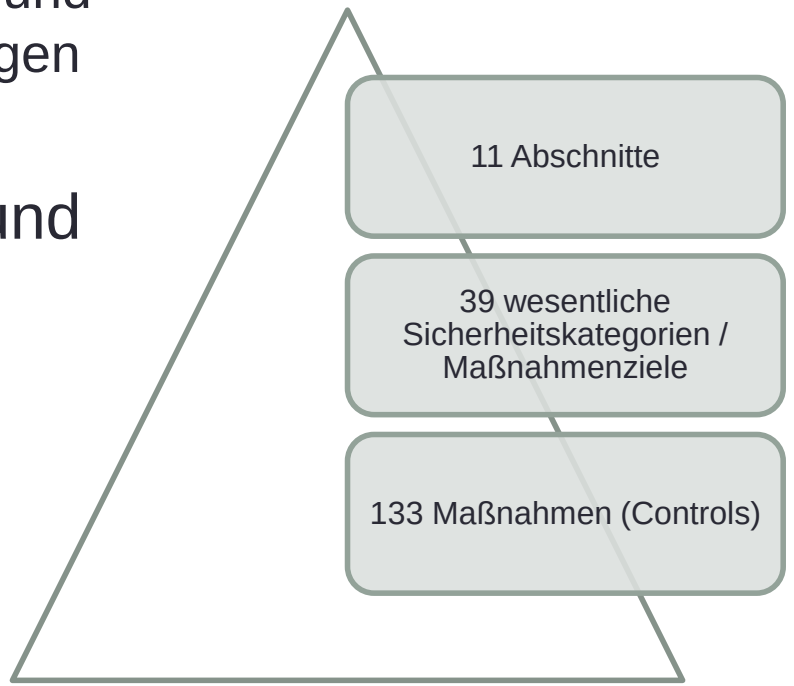


Risikobehandlung



Anhang A: Maßnahmenziele und Maßnahmen

- Katalog von Maßnahmenzielen (Control Objectives) und Maßnahmen (Contols)
- Gegliedert wie Abschnitte 5 bis 15 der ISO/IEC 27002 („Leitfaden“ / „Code of practice“)
  - ISO/IEC 27002 gibt ausführlichere und konkretere Umsetzungsempfehlungen
  - Nummerierung beginnt mit A.5
- Welche Maßnahmen relevant und anwendbar sind, wird in der Erklärung zur Anwendbarkeit (Statement of Applicability) festgelegt.



Abschnitte im Anhang A

<table>
<tr><td colspan="4">A.5 Security policy (1/2) [= 1 Maßnahmenziel / 2 Maßnahmen (Controls)]</td></tr>
<tr><td colspan="4">A.6 Organization of information security (2/11)</td></tr>
<tr><td colspan="4">A.7 Asset management (2/5)</td></tr>
<tr><td>A.8
Human resources security (3/9)</td><td>A.9
Physical & environmental security (2/13)</td><td>A.10
Communications & operations management (10/32)</td><td rowspan="2">A.12
Information systems acquisition, development & maintenance (6/16)</td></tr>
<tr><td colspan="3">A.11 Access control (7/25)</td></tr>
<tr><td colspan="4">A.13 Information security incident management (2/5)</td></tr>
<tr><td colspan="4">A.14 Business continuity management (1/5)</td></tr>
<tr><td colspan="4">A.15 Compliance (3/10)</td></tr>
</table>

vgl. ISO/IEC 27001, S. 21-39

ISO/IEC 27001, Anhang A 11.3.1

A.11 Zugangskontrolle

(…)

A.11.3 Benutzerverantwortung

Ziel:

Verhinderung von unbefugtem Benutzerzugriff, Kompromittierung und Diebstahl von Informationen und informationsverarbeitenden Einrichtungen.

A.11.3.1: Passwortverwendung

Maßnahme:

Benutzer müssen aufgefordert werden, guten Sicherheitspraktiken bei der Auswahl und der Anwendung von Passwörtern zu folgen.

ISO/IEC 27002, Abschnitt 11.3.1

A.11 Zugangskontrolle

(…)

A.11.3 Benutzerverantwortung

Ziel: Verhindern von unbefugtem Benutzerzugriff, Kompromittierung und Diebstahl von Informationen und informationsverarbeitenden Einrichtungen.

Die Mitarbeit der rechtmäßigen Benutzer (…)

A.11.3.1: Passwortverwendung

Maßnahme:

Benutzer sollten aufgefordert werden, guten Sicherheitspraktiken in der Auswahl und der Anwendung von Passwörtern zu folgen.

Anleitung zur Umsetzung:

Allen Benutzern sollte angeraten sein:

a) Passwörter geheim zu halten;

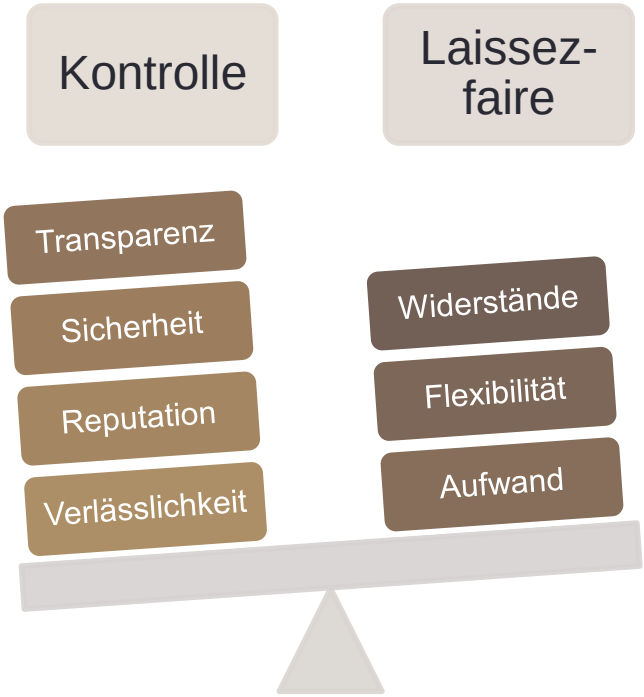
b) es zu vermeiden Passwörter aufzuzeichnen (z. B. auf Papier, in einer Datei oder auf einem Handheld), solange diese nicht sicher gespeichert werden und die Methode des Speicherns genehmigt worden ist;

c) Passwörter zu ändern wann immer es einen Hinweis darauf gibt, dass die Passwörter oder das System kompromittiert wurden;

(…)

Warum das alles nicht leicht ist…

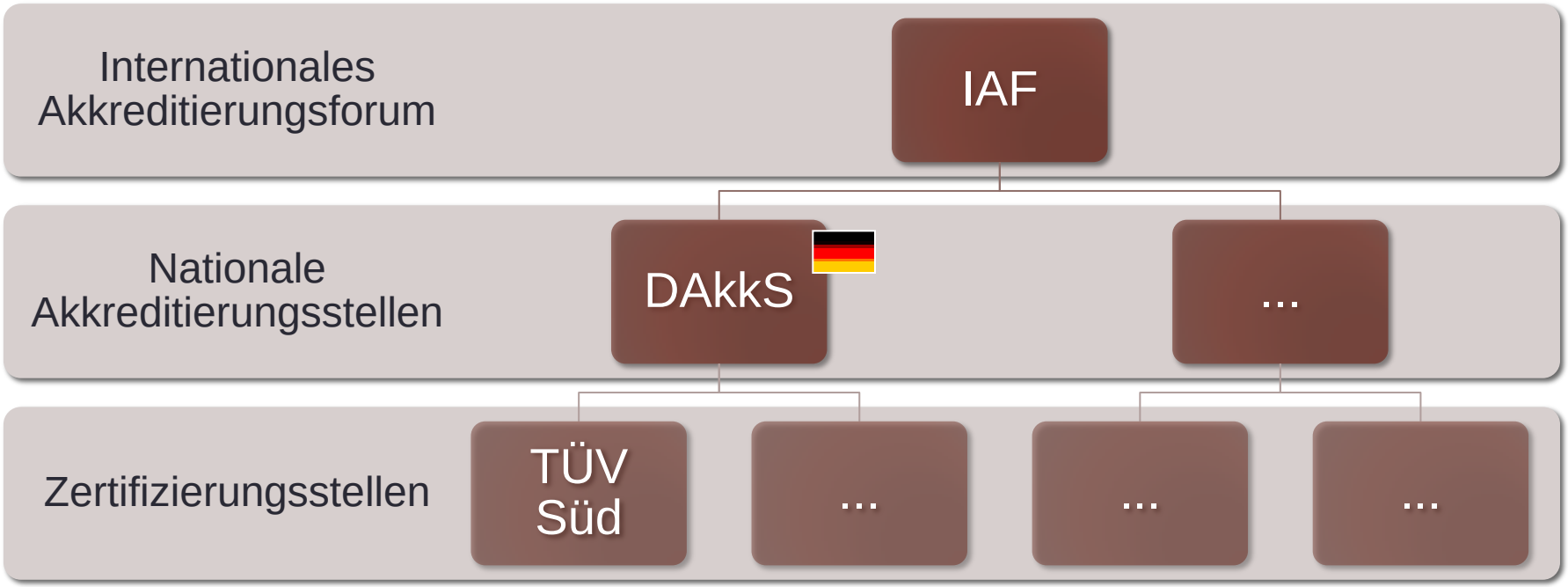
- Sicherheitsmaßnahmen kosten: Geld, Mitarbeiterzeit, Flexibilität, Nerven,…
- Sicherheits-Leitlinie und Risiko-Akzeptanz erfordern konkrete Antworten des Managements auf Fragen, die gerne vermieden werden.
- Einführung eines anspruchsvollen Managementsystems stellt meist, je nach Voraussetzungen, einen *Organizational Change* dar.
- Erfolgsrate von *Organizational Changes:* 30% (J. Kotter).



Was bedeutet „ISO/IEC 27001 Zertifizierung“?

ISMS-Zertifizierung nach ISO/IEC 27001

Organisationen rund um die Zertifizierung



Schritte zur ISMS-Zertifizierung

1. Auswählen einer Zertifizierungsstelle (Certification Body, CB)

Wer auditiert und zertifiziert?

2. Gültigkeitsbereich (Scope) der Zertifizierung festlegen

Scoping Statement

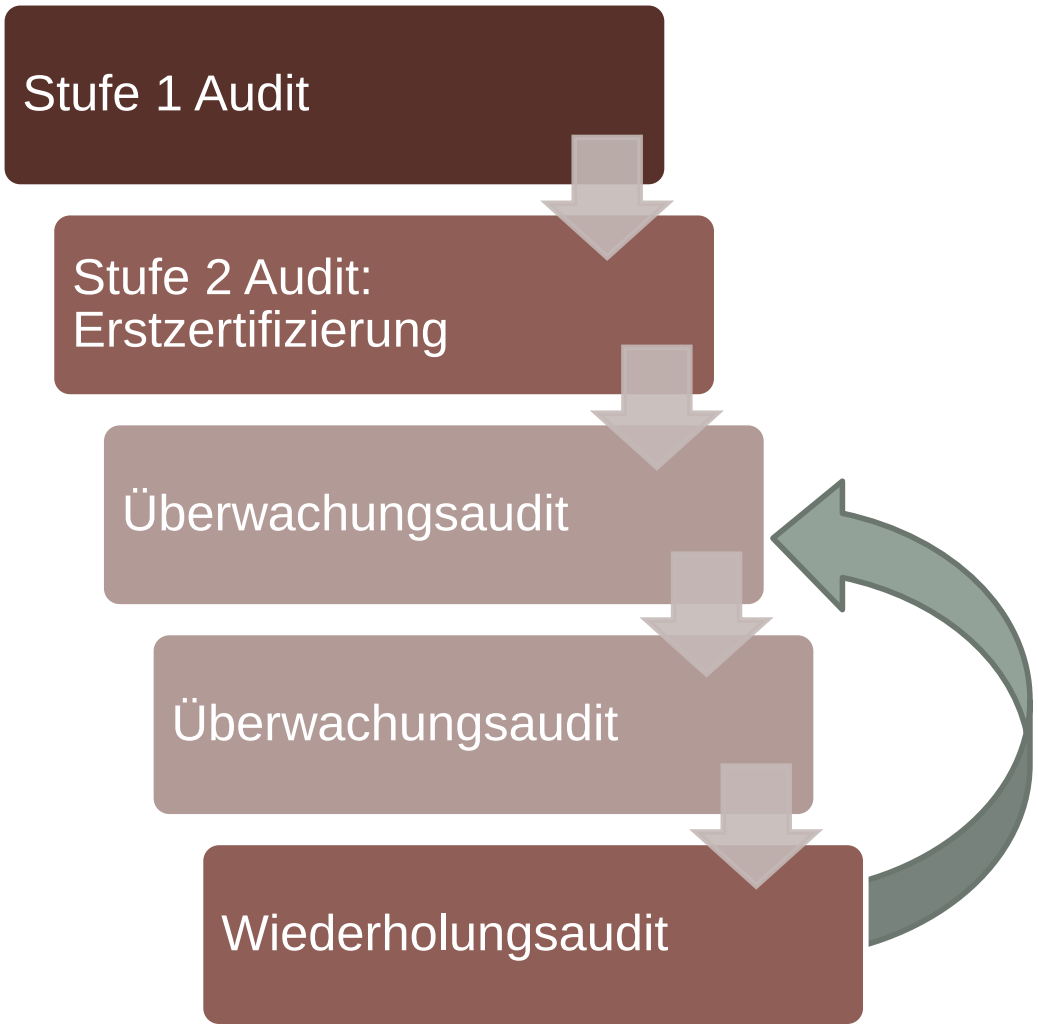
3. Initiales Assessment durchführen

Selbsteinschätzung	oder	Vor-Audit durch den CB

4. Termin für ISO/IEC 27000 Zertifizierungsaudit vereinbaren

(Ab) wann wird auditiert?

Auditablauf



- 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

Auf was man beim Lesen eines Zertifikats achten sollte

- **Was ist der Geltungsbereich?**
  Der Geltungsbereich gibt die Grenzen des Zertifikates an. Der Geltungsbereich kann auf Unternehmensteile oder bestimmte Services eingeschränkt sein. Nicht immer fällt das, was man von einer Firma erwartet, auch unter das Zertifikat.

- **Wurde es von einem akkreditierten Zertifizierer ausgestellt?**
  Nur bei akkreditierten Zertifikaten kann man eine gewisse Qualität als gegeben annehmen.
  Nur akkreditierte Zertifizierer unterliegen einer jährlichen Kontrolle durch eine übergeordnete Stelle.

Personenqualifizierung auf Basis von ISO/IEC 27000

- Unabhängig von der Zertifizierung des ISMS
- Ziel der Zertifizierung von Personen: Unabhängig dokumentierter Nachweis über die fachliche Qualifikation einer Person in einem Wissensgebiet
- Zwei Arten von Zertifikaten für Personen:
  - "Klassisches" Zertifikat (z.B. ISO/IEC 27001 Foundation)
    - Nachweis über das Bestehen einer Prüfung und ggf. Erfüllung weiterer Anforderungen (Kursteilnahme, Practical Assignments)
    - Gültigkeit: unbegrenzt
  - Kompetenzzertifikat (nach ISO/IEC 17024)
    - Nachweis über fachliche Fähigkeiten und deren Anwendung im Rahmen mehrjähriger Berufspraxis sowie über regelmäßige fachliche Fortbildung
    - Gültigkeit: begrenzt (z.B. 3 Jahre), muss regelmäßig erneuert werden

Personenzertifizierung durch TÜV Süd

Weitere Informationen

- Praxisbuch ISO/IEC 27001
  www.iso27000buch.de
  www.hanser.de/978-3-446-43026-6
- Qualifizierungs- und Zertifizierungsprogramm für Personen des TÜV Süd
  tinyurl.com/tuev27k
- BSI Standard 100-1: Managementsysteme für Informationssicherheit
  tinyurl.com/bsi100-1