DIIR Deutsches Institut für Interne Revision e.V.

IT-Tagung 2012

IT-Sicherheitsorganisationen zwischen internen und externen Anforderungen

Kontrollaufgaben im IT-Security-Kontext

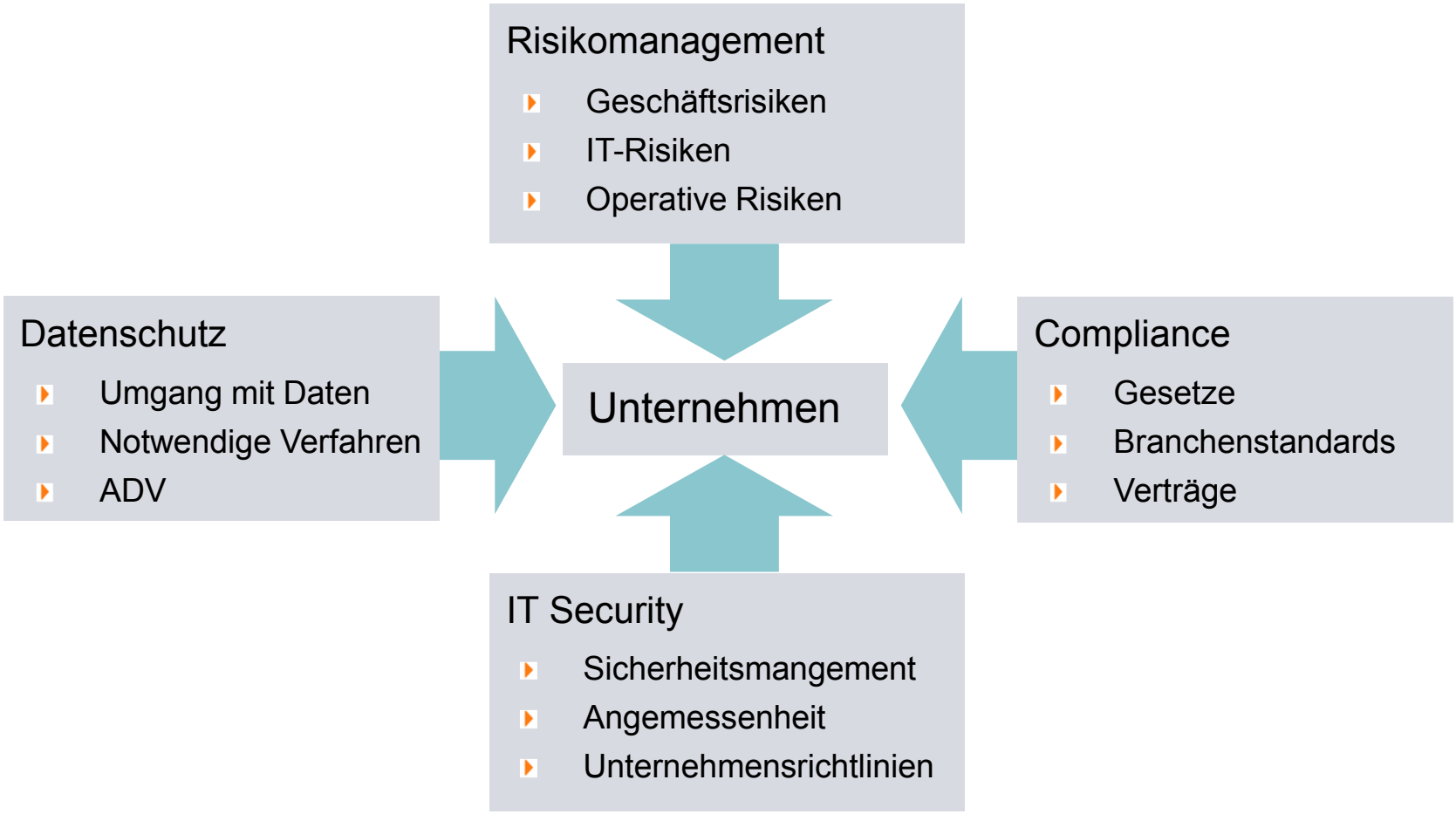
Agenda

- Aufgaben einer IT-Sicherheitsorganisation
- Zusammenspiel IT-Security, IT-Compliance, Datenschutz, IT-Risikomanagement
- Aufgabenteilung und Synergieeffekte
- Umgang mit externen Providern
- Wert und Grenzen von Zertifizierungen
- Beispiele aus der Praxis

Aufgaben einer IT-Sicherheitsorganisation

- „Informationssicherheitsmanagement“
- Erstellung von Policies und Richtlinien
- Analyse von Schutzbedarfen und IT-Risiken
- Sicherstellung eines angemessenen IT-Sicherheitsniveaus
- Sicherstellen der Einhaltung von Vorgaben
- Durchgängigkeit und Vergleichbarkeit des Sicherheitsniveaus

Unternehmensanforderungen



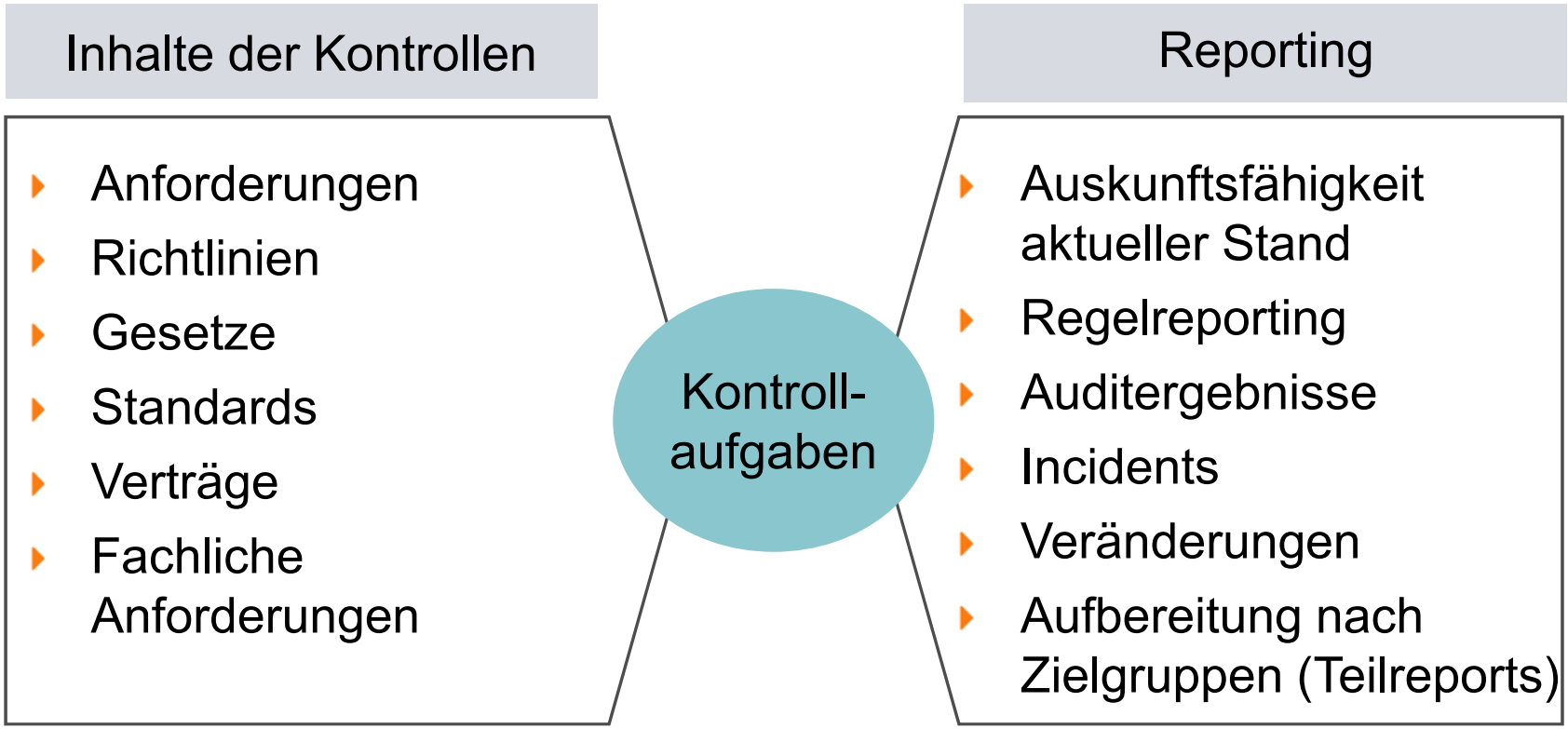
Bedeutung im IT-Sicherheits-Kontext

Risikomanagement	IT-Risiken Risikoanalysen Reporting des Risikos
Datenschutz	Vertraulichkeit, Integrität, Nachvollziehbarkeit Rollen und Rechte, Angemessenheit Relevant in Betrieb und Entwicklung
Compliance	Bedeutung der Anforderungen auf IT Kontinuität über Changes hinweg Häufig Lösch- und Aufbewahrungsthemen

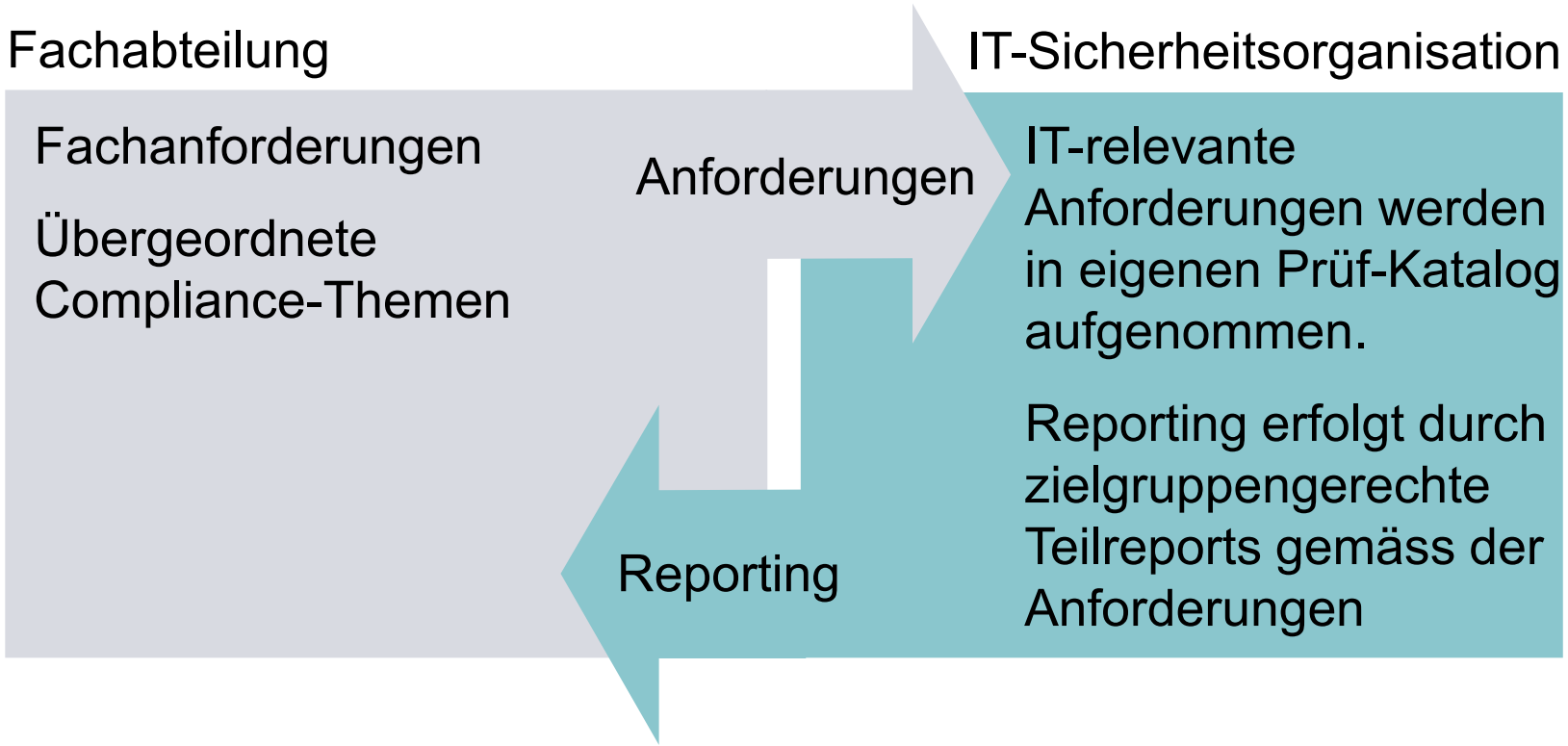
Bündelung von Aufgaben

- Vermeidung doppelter Arbeiten
- Konzentration auf Kernkompetenzen
- Sicherstellen notwendiger Informationsflüsse
- Bessere Qualität
- Gemeinsame Stärke

Einflüsse auf Kontrollaufgaben



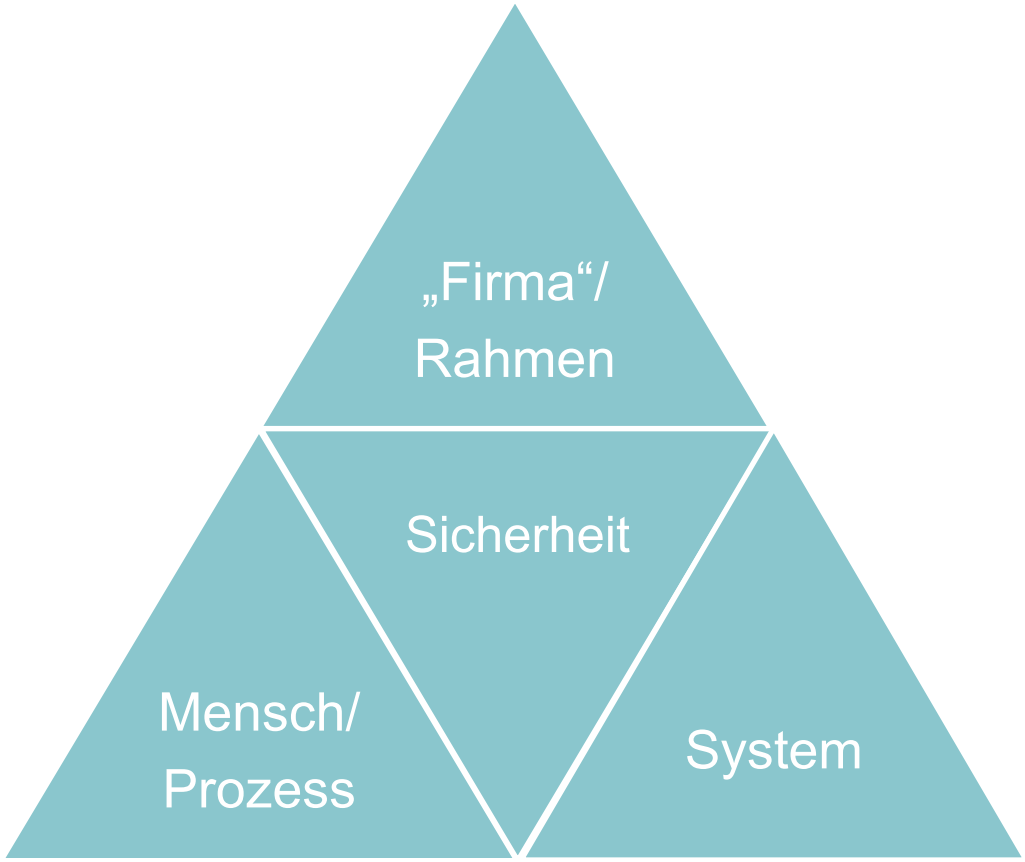
Interaktion zwischen Abteilungen



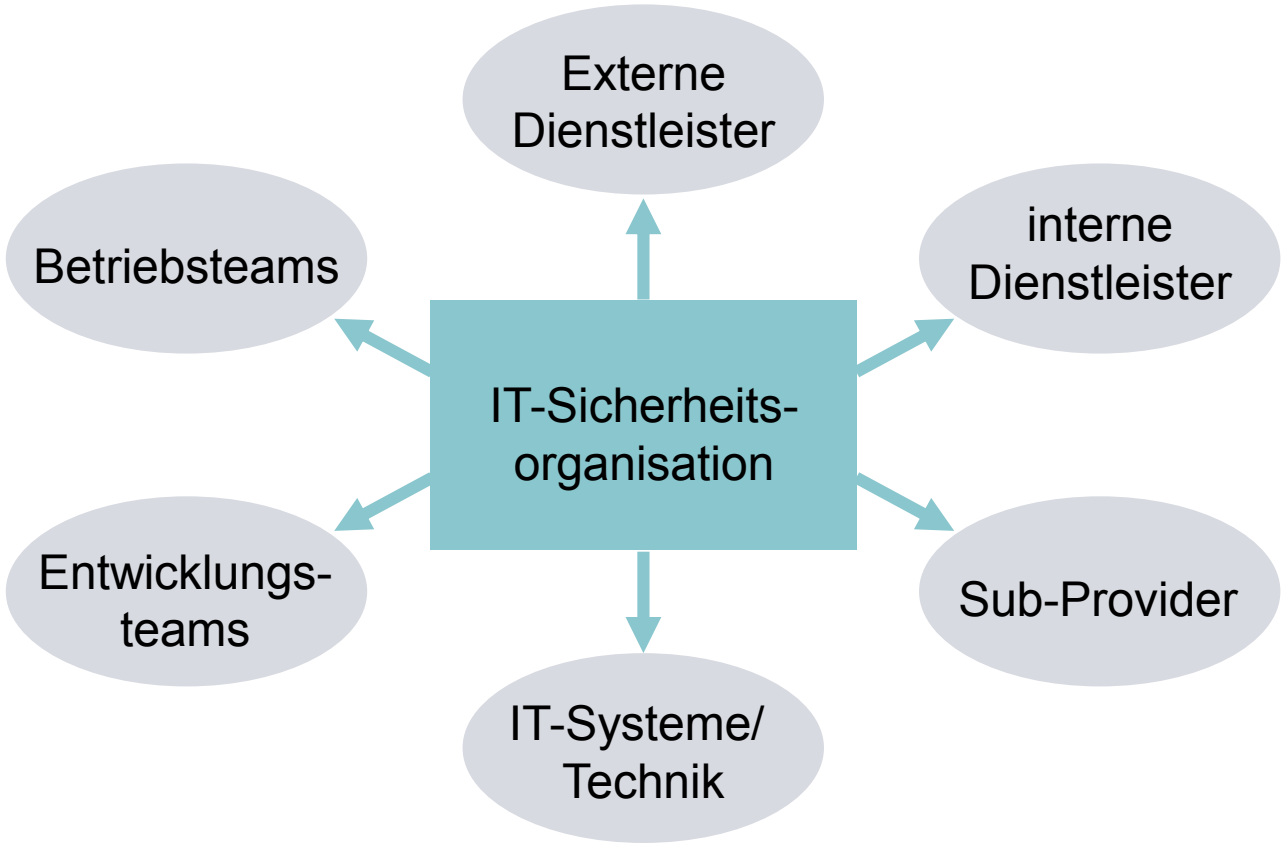
Kontrollprozesse/ Arten von Kontrollen

- Aufgaben im “operativen” Geschäft
  - Bewahrung Übersicht aktueller Stand
  - Antragsprozesse und Freigaben
  - Security-Monitoring
    - ⇒ Kontinuierlicher Prozess
- Audits
  - Stichproben
  - Ist-Aufnahme
  - Vergleich zu Soll-Zustand
    - ⇒ Point-in-Time Prüfung

Facetten der Sicherheit



Betrachtungsgegenstände bei Kontrollen



Inhalte von Kontrollen (Audits) - Unternehmen

Prüfung von

- Vertragliche Themen
  - Auswahl und Einbindung Subdienstleister
  - Verträge mit Subdienstleistern
  - …
- Rahmenbedingungen
  - Physische Sicherheit
  - Sicherheitspolicies
  - Mitarbeiterauswahl und Schulung
  - Einhaltung Verträge
  - …

Inhalte von Kontrollen (Audits) - Prozesse

Prüfung von

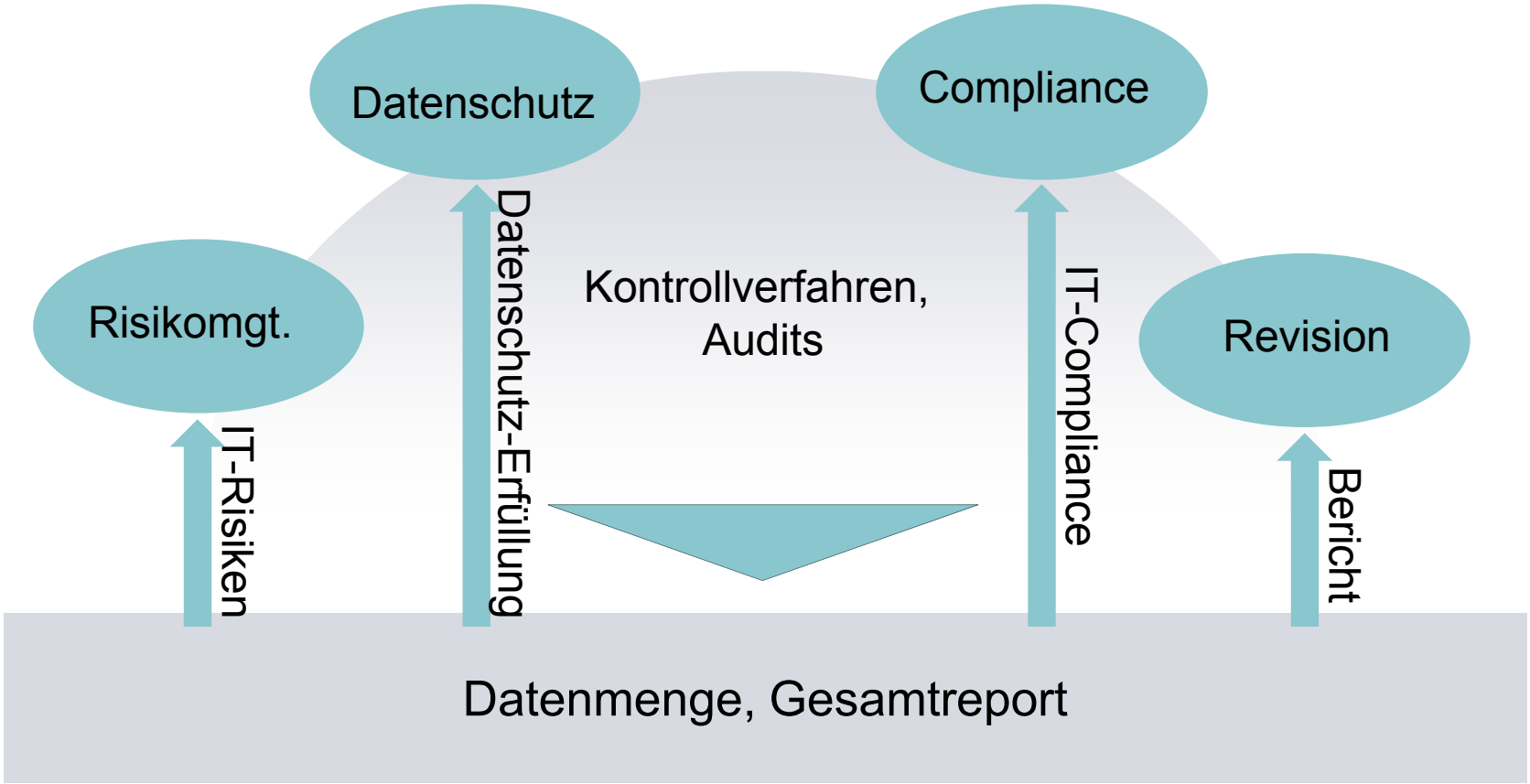
- Fachlichen Themen
  - Arbeitsprozessen
  - Dokumentationen
  - Prozesstreue
  - Kenntnis von Anforderungen und Richtlinien
  - Nachvollziehbarkeit der Arbeiten

Inhalte von Kontrollen (Audits) – System-Audits

Prüfung von

- IT-Systemen
- Konzepten
- Systemeinstellungen/Konfigurationen
- Schutzbedarf und Risiken
- Zweckbindung und Datenarten

Zielgruppengerechtes Reporting



Unterschiede interne/externe Dienstleister

- Verträge
- Rahmenbedingungen: Arbeitsbedingungen, Richtlinien
- Strukturen, Ziele
- Ansprechpartner und Kontaktmöglichkeiten
- Eskalationswege
- Offenlegung von Informationen und Dokumenten
- Durchgriffsmöglichkeiten

Rückgriff auf Zertifizierungen

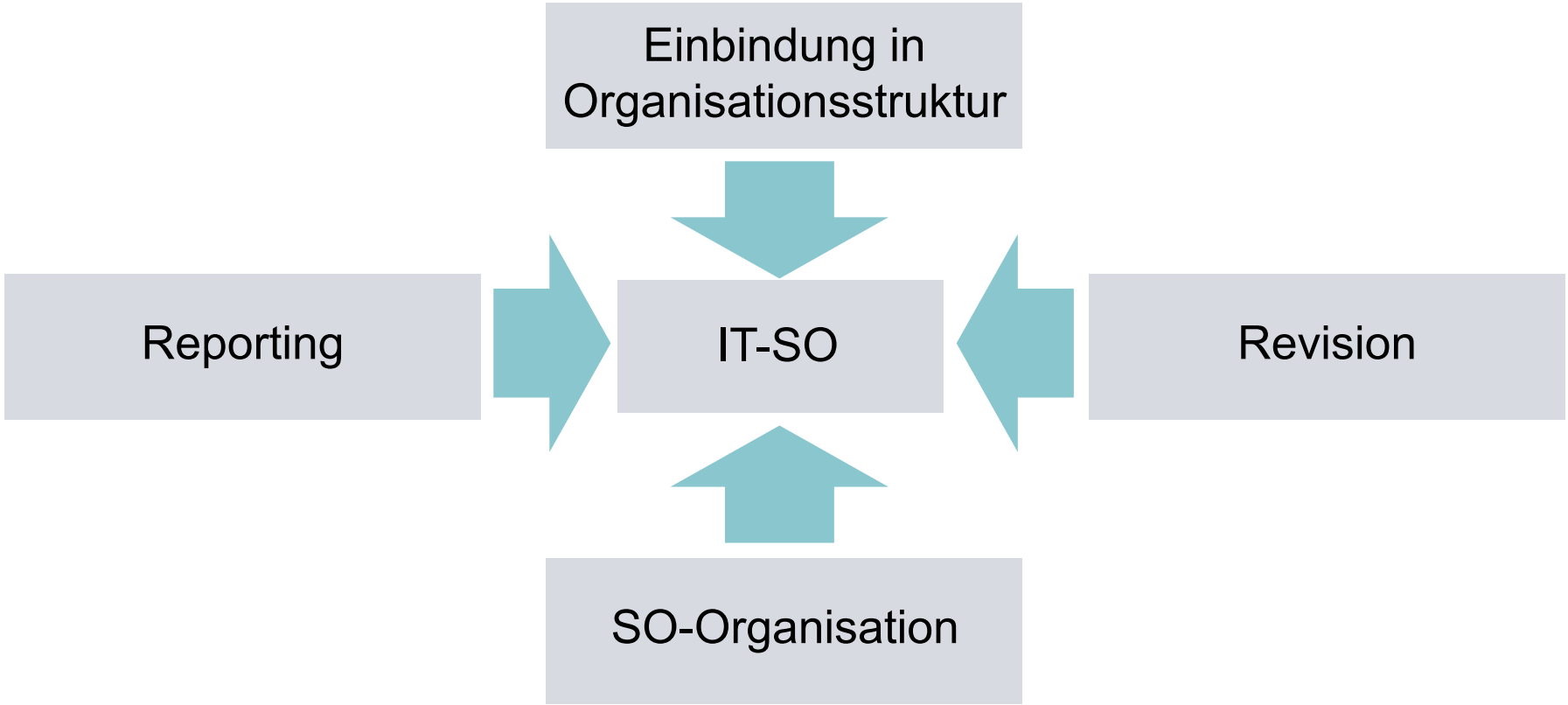
Chancen

- Minimierung des Kontrollaufwands
- Ggf. umfassendere Prüfung als bei Eigenkontrollen
- Standardisierte Verfahren und Anforderungen

Grenzen

- Vorsicht beim Scope! Was genau wurde Zertifiziert?
- Sagt Zertifikat inhaltlich das gewünschte aus?
- Ergeben sich die nötigen Informationen für das eigene Reporting aus dem Zertifikat bzw. Bericht?

„Kontrolle des Kontrolleurs“



Erfahrungen - Fallstricke in der Praxis

- Gleichartige Aufgaben liegen in unterschiedlichen Abteilungen
  - Mangelnde Kommunikation
  - Doppelte Arbeiten
  - Verärgerung der Kontrollierten
- “Scheinbilder” für Audits
- Einführung von “Sonderlocken” zur Erfüllung der Anforderungen, Standardprozesse nicht ausreichend
- Ohne flächengreifende Kontrollstrukturen keine Entwicklung von ausreichenden Standardlösungen

Erfahrungen – Positive Entwicklungen

- Einführen von Kontrollprozessen führt zu Verbesserung des Sicherheitsniveaus in allen Bereichen
- „Papierkonzepte“ werden entdeckt und praxistauglich gemacht
- Neue Konzepte werden gleich geeignet entwickelt
- Akzeptanz durch Vermeidung doppelter Arbeit
- Schärfung Bewusstsein bei Dienstleistern und Management (Auditberichte!)
- Möglichkeit zur Aufdeckung von Verbesserungspotential
- Gemeinsam ist man stärker! (Gleiche Anforderungen aus mehreren Bereichen)

Anekdoten aus der Praxis

- Dienstleisteraudit - §11 Verträge mit Sublieferanten wurden am Tag vor Audit unterschrieben
- “Sagen Sie und doch, was wir da reinschreiben müssen, damit es ok ist”
- “Ihre Härtungsvorschriften machen alles so kompliziert” – Anforderungen ergaben sich aus den eigenen Richtlinien des entsprechenden Dienstleisters …

Fragen?

- Kontakt:

Marion Steiner
Marion.Steiner@isw-online.de

IT-Security@Work GmbH (ISW)
Robert-Koch-Str. 41
55129 Mainz
Tel.: 06131 88056-60
Fax: 06131 88056-69
Web: www.isw-online.de