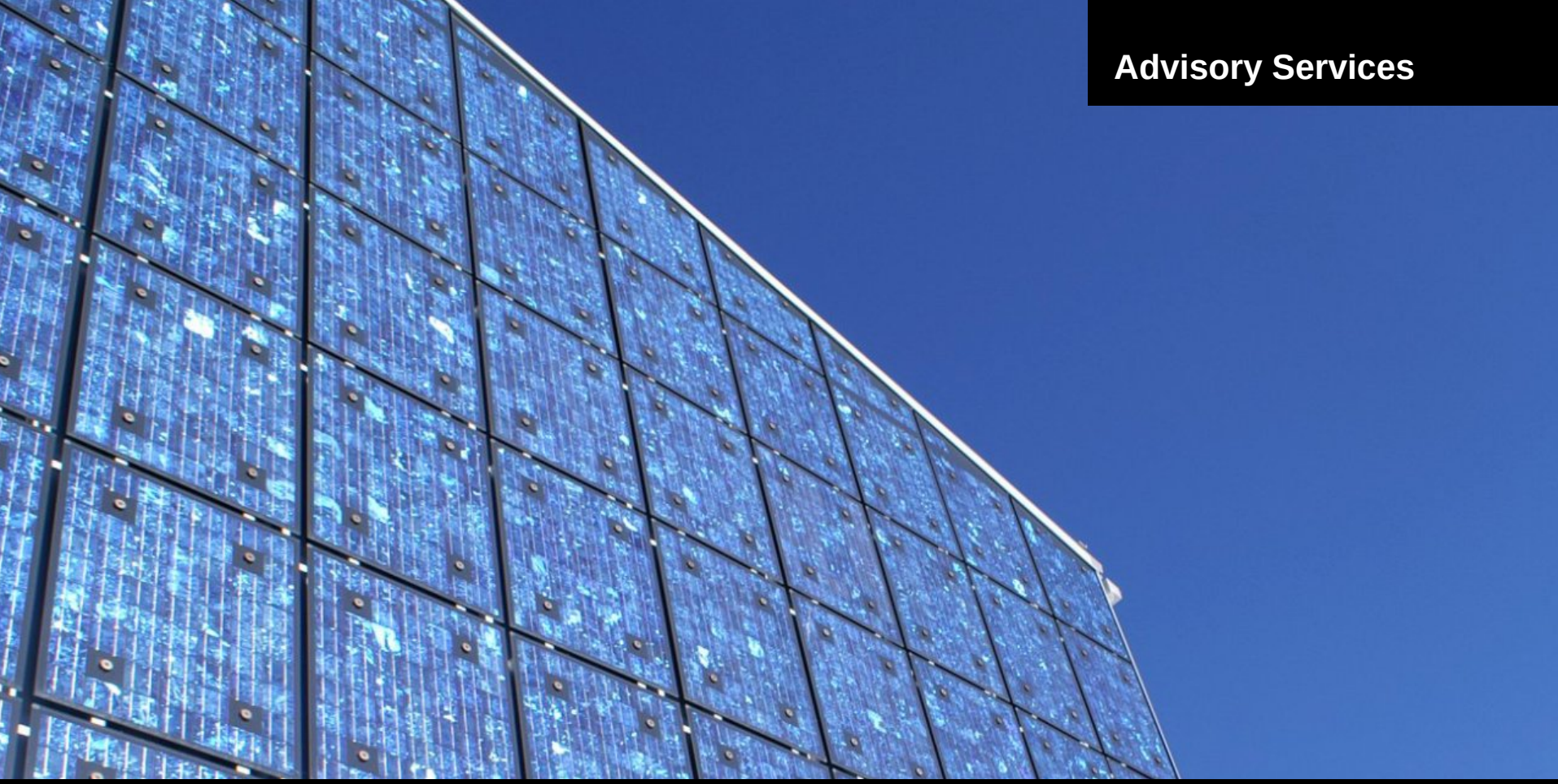


Advisory Services

ERNST & YOUNG

Quality In Everything We Do

IT in der Wirtschaftsprüfung

IT-Compliance-Tagung, DSRI / Oldenburg, 16. März 2007

Im Überblick

1 Ausgangssituation

2 IT-Prüfungen im Rahmen der externen Revision

3 IT-Kontrollen und Risikoeinschätzung

4 Fazit

Im Überblick

1 Ausgangssituation

2 IT-Prüfungen im Rahmen der externen Revision

3 IT-Kontrollen und Risikoeinschätzung

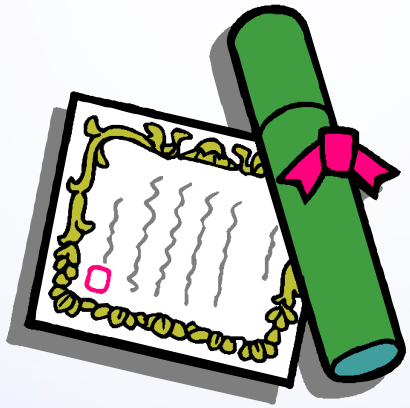
4 Fazit

Ausgangssituation

Gegenstand einer Jahresabschlussprüfung

„Die Prüfung ist so anzulegen, dass Unrichtigkeiten und Verstöße (…), die sich auf die Darstellung des sich nach § 264 Abs. 2 ergebenden Bildes der Vermögens-, Finanz- und Ertragslage des Unternehmens ***wesentlich*** *auswirken, bei* ***gewissenhafter*** *Berufsausübung erkannt werden.“*

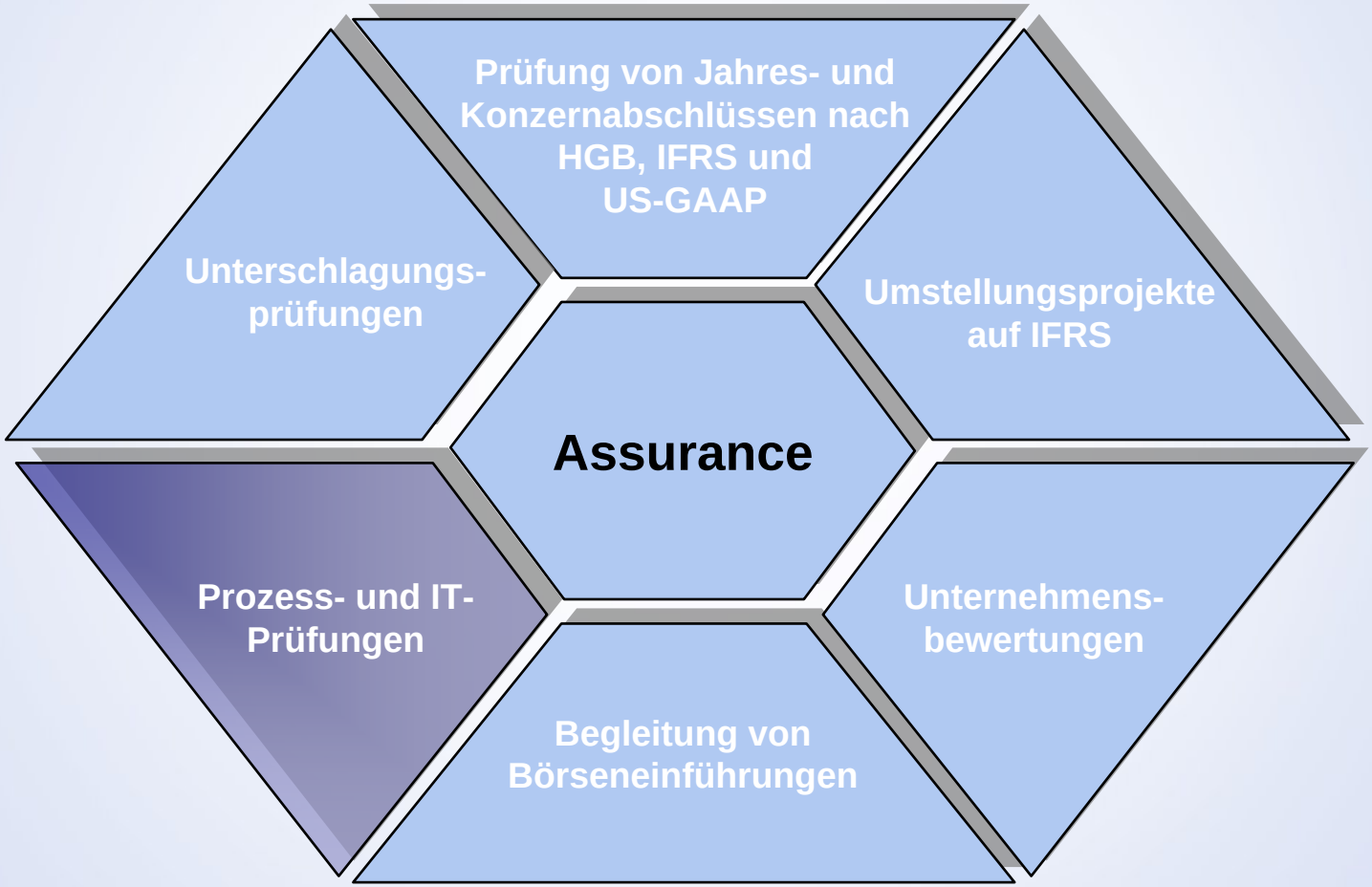
(§ 317 Abs. 1 S. 3 HGB)



Testat
(IDW PS 400)

Ausgangssituation

Breites Aufgabenspektrum in der Wirtschaftsprüfung (Assurance)



Ausgangssituation

Das moderne Berufsbild des Wirtschaftsprüfers

IN	OUT
• Effizienz durch risiko-orientiertes Prüfen • Teamplayer • Berater des Mandanten • Internationalität	• Hakenmacher • Belegprüfung ohne Risikobewusstsein • kein Verständnis für das Geschäft des Mandanten • Aktenwälzer

Ausgangssituation
Externe Revision und IT

- **Integrierte Informationssysteme** in allen Bereichen des Unternehmens
- Erwartung des prüfungspflichtigen Unternehmens in Bezug auf **technologische Risiken** ist zu adressieren
- Aufnahme und Analyse komplexer IT Systeme ist erforderlich
- Einsatz von IT-Prüfung bei Vorliegen von
  - **erheblicher Nutzung** von Technologie
  - **starker Veränderungen** von Technologien oder Prozessen (immer kürzere Produktlebenszyklen)

Ausgangssituation

Steigende Komplexität der IT-Systeme

- IT entwickelt sich zusehends zum **„Nervensystem“** der Unternehmung
- **Integrierte ERP-Systeme** verlagern die Erfassung rechnungslegungs-relevanter Daten in operative Bereiche außerhalb der Buchführung
- Zunehmende **Vernetzung** entlang der Wertschöpfungskette bringt neue Prozesslogiken
- Isolierte Betrachtung des Teilsystems Buchhaltung muss einer **ganzheitliche**n **Betrachtung** aller rechnungslegungsrelevanten Bestandteile des IT-Systems / der IT-Systeme weichen
- Komplexität bedingt spezifische **IT-Risiken**

Ausgangssituation
Begriffsdefinition IT-Prüfungsrisiko

- Die im Zusammenhang mit der konkreten Ausgestaltung des IT-Systems einhergehenden Risiken werden als **IT-Fehlerrisiken** bezeichnet
- **Inhärentes Risiko** = Wahrscheinlichkeit für das Auftreten wesentlicher Fehler in der Rechnungslegung, ungeachtet bestehender Kontrollen
- Risikoindikatoren für **inhärente IT-Risiken**:
  - Abhängigkeit (von IT-Anwendungen und Infrastruktur)
  - Änderungen (z.B. größerer IT-Einführungsprojekte)
  - Know-how und Ressourcen (z.B. aktuelles Fachwissen)
  - Geschäftliche Ausrichtung (z.B. unternehmensadäquate IT-Strategie)
- **Kontrollrisiko** = Wahrscheinlichkeit, dass wesentliche Fehler durch das Interne Kontrollsystem (IKS) nicht verhindert oder aufgedeckt werden.

Ausgangssituation
Begriffsdefinition IT-Prüfungsrisiko

- IT-Audit Risk „Gleichung“ (in Anlehnung AICPA 1987):

$$AR_{IT} = IR_{IT} \times CR_{IT} \times DR_{IT}$$

Bewertung des IT-Umfeldes (z.B. geschäftliche Ausrichtung, IT-Change-Projekte)

Beurteilung von Anwendungskontrollen und allgemeinen IT-Kontrollen

Durchführung von Datenanalysen (z.B. ACL, IDEA)

AR_{IT}: Audit Risk (IT)
IR_{IT}: Inherent Risk (IT)
CR_{IT}: Control Risk (IT)
DR_{IT}: Detection Risk (IT)

Ausgangssituation
Auswirkungen auf die Jahresabschlussprüfung

- Beurteilung der Ordnungsmäßigkeit der Rechnungslegung erfolgt indirekt über
  - die **Ordnungsmäßigkeit** der IT-gestützten Buchführungsprozesse und
  - die **Wirksamkeit** der IT-bezogenen Kontrollen
- **Prüfungssicherheit** und **Prüfungseffizienz** werden durch den Einsatz IT-gestützter Prüfungsprogramme (z.B. ACL, IDEA) erhöht
- Mit wachsender Bedeutung der IT verändern sich auch die notwendigen **Kompetenzen** im Rahmen der Abschlussprüfung. Die Prüfungsteams benötigen **Verständnis / Know-how** für
  - IT-Konzepte
  - IT-bezogene Risiken
  - Wirksame Kontrollen für IT-bezogene Risiken
  - Wirksame Tests IT-bezogener Kontrollen

Im Überblick

1 Ausgangssituation

2 IT-Prüfungen im Rahmen der externen Revision

3 IT-Kontrollen und Risikoeinschätzung

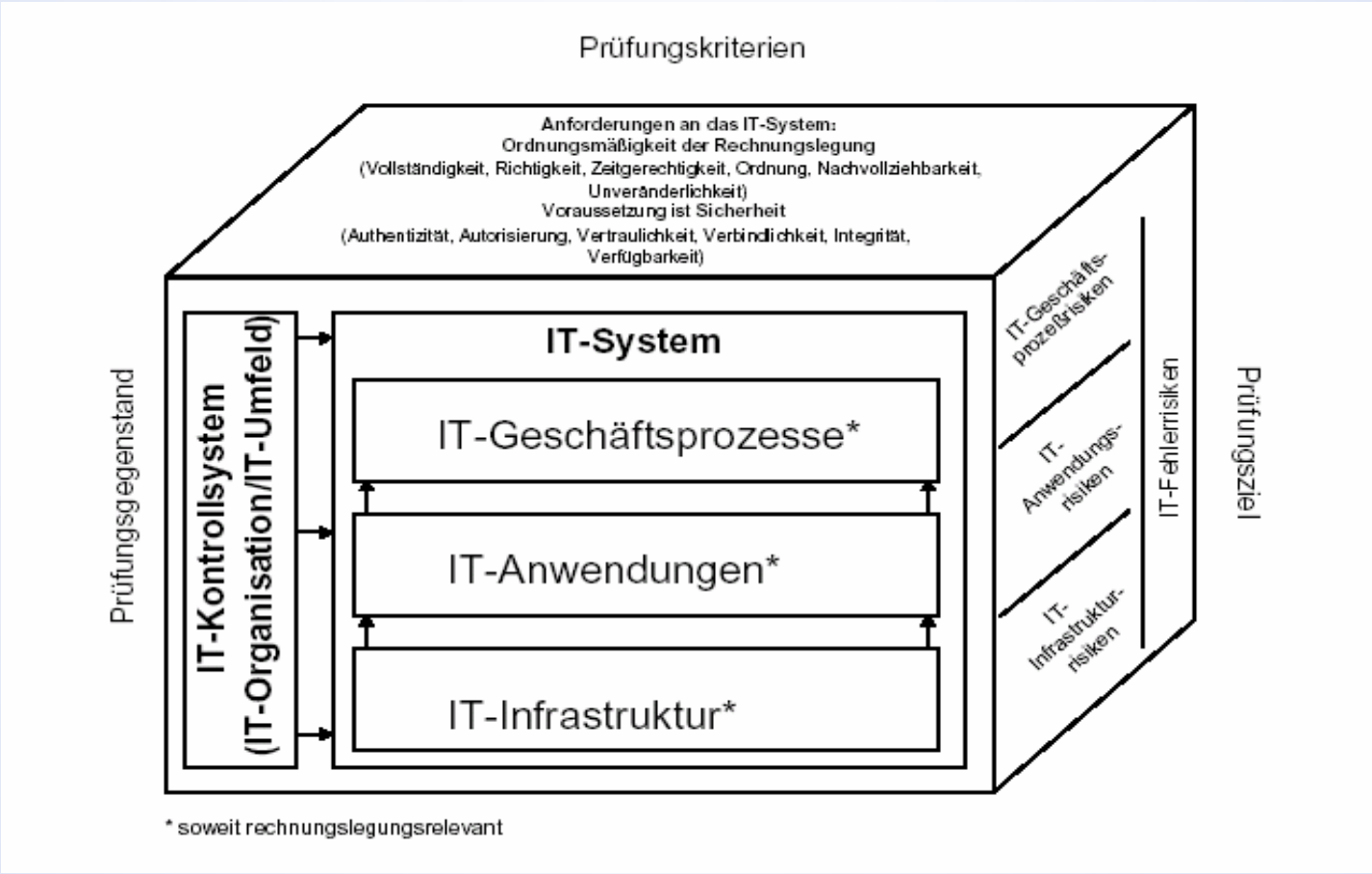
4 Fazit

IT-Prüfungen im Rahmen der externen Revision
Ziele und Umfang von IT-Prüfungen

- Die IT-Systemprüfung stellt einen **Teilausschnitt** aus der Prüfung des **internen Kontrollsystems** dar und wird nach den allgemeinen Grundsätzen für die Prüfung des IKS geplant und durchgeführt
- Ziel der IT-Systemprüfung ist die **Beurteilung der IT-Fehlerrisiken**, d. h. des Risikos wesentlicher Fehler in IT-Systemen, soweit diese **rechnungslegungsrelevant** sind
- Prüfungsgegenstand sind die Prüfungsgebiete **IT-Infrastruktur**, **IT-Anwendungen** und **IT-gestützte Geschäftsprozesse** einschließlich des **IT-Umfeldes** und der **IT-Organisation**
- Art und Umfang der IT-Systemprüfungen bestimmen sich auch aus der **Wesentlichkeit** des IT-Systems für die **Rechnungslegung**

IT-Prüfungen im Rahmen der externen Revision

Ziele und Umfang von IT-Prüfungen

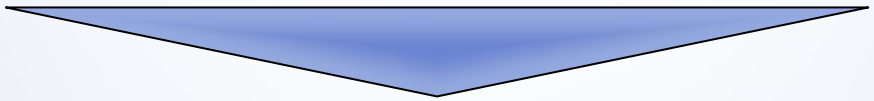


Quelle: IDW PS 330

IT-Prüfungen im Rahmen der externen Revision

Rolle des IT-Prüfers in der Jahresabschlussprüfung

- Identifikation der **relevanten** IT-**Systeme** und **Informationsflüsse**
- Identifikation **systemseitig** bestehender **Risiken**
- Definition von geeigneten **Prüfungs- bzw. Testverfahren**
- Durchführung von **datenanalytischen** Prüfungshandlungen
- Beurteilung der **Wirksamkeit** systemseitig existierender **Kontrollen**



Erhöhung der Prüfungssicherheit und Prüfungseffizienz

IT-Prüfungen im Rahmen der externen Revision

Vorgaben und Standards

- **Gesetzliche Vorgaben**
  - Handelsgesetzbuch (HGB § 238 ff.) (z. B. Buchführungspflicht, Aufbewahrungspflichten etc.)
  - Abgabenordung (AO § 140 ff.)
  - Grundsätze ordnungsmäßiger DV-gestützter Buchführungssysteme (GoBS)
  - Kontroll- und Transparenzgesetz (KonTraG)
  - Bundesdatenschutzgesetz (BDSG)
  - Grundsätze zum Datenzugriff und zur Prüfbarkeit digitaler Unterlagen (GDPdU)
  - **Sarbanes Oxley Act (SOX), insb. Sect. 404**
  - **8. EU-Richtlinie**

- **Berufsständische und weitere Standards**
  - Standards des Instituts deutscher Wirtschaftsprüfer (IDW)
    - z.B. PS 330, PS 331, PS 880, RS FAIT 1, ERS FAIT 2
  - **International Standards on Auditing (ISA) des International Auditing and Assurance Standards Board (IAASB)**
    - **z.B. ISA 315, 330 (zuvor 400, 401)**
  - IT-Grundschutzhandbuch (IT-GSHB)
  - **ISO 27001 (zuvor: 17799 / BS 7799) Information technology – Code of practice for information security management**
  - **CobiT - Control Objectives for Information and Related Technology**

IT-Prüfungen im Rahmen der externen Revision

Szenarios

Ausgangssituation	Art der Prüfung	Ergebnis
Fehlende qualifizierte Ressourcen in der IT-Innenrevision. Sicherstellung ordnungsgemäßer Einführung / Releasewechsel / Anwendung von IT-Systemen (z. B. SAP).	**IT-Audit / IT-Assurance** Prüfung von IT-Systemen und IT-Dienstleistern nach anerkannten Standards (z. B. SAP Post Implementation Review, Projektbegleitende Revision und SAP- Berechtigungsprüfung).	Qualifizierte Prüfung und Bewertung von IT-Systemen zur Einhaltung der gesetzlichen Vorschriften.
Stand, Bedeutung und Integrationsfähigkeit der Informationstechnologie ist unbekannt.	**IT-Due Diligence** Beurteilung und Bewertung von IT-Anwendungen, Infrastrukturen, usw.	Sicherheit bei der Einschätzung der IT-Risiken durch neutrale und umfassende Bewertung.
Sicherstellung der regulatorischen und gesetzlichen Anforderungen von Softwareprodukten.	**Softwarezertifizierung** Qualifizierte Prüfung und Bewertung von Softwareprodukten nach anerkannten Standards.	Förderung der Marktstellung durch zertifizierte Softwareprodukte gemäß gesetzlicher Vorschriften.

Im Überblick

1 Ausgangssituation

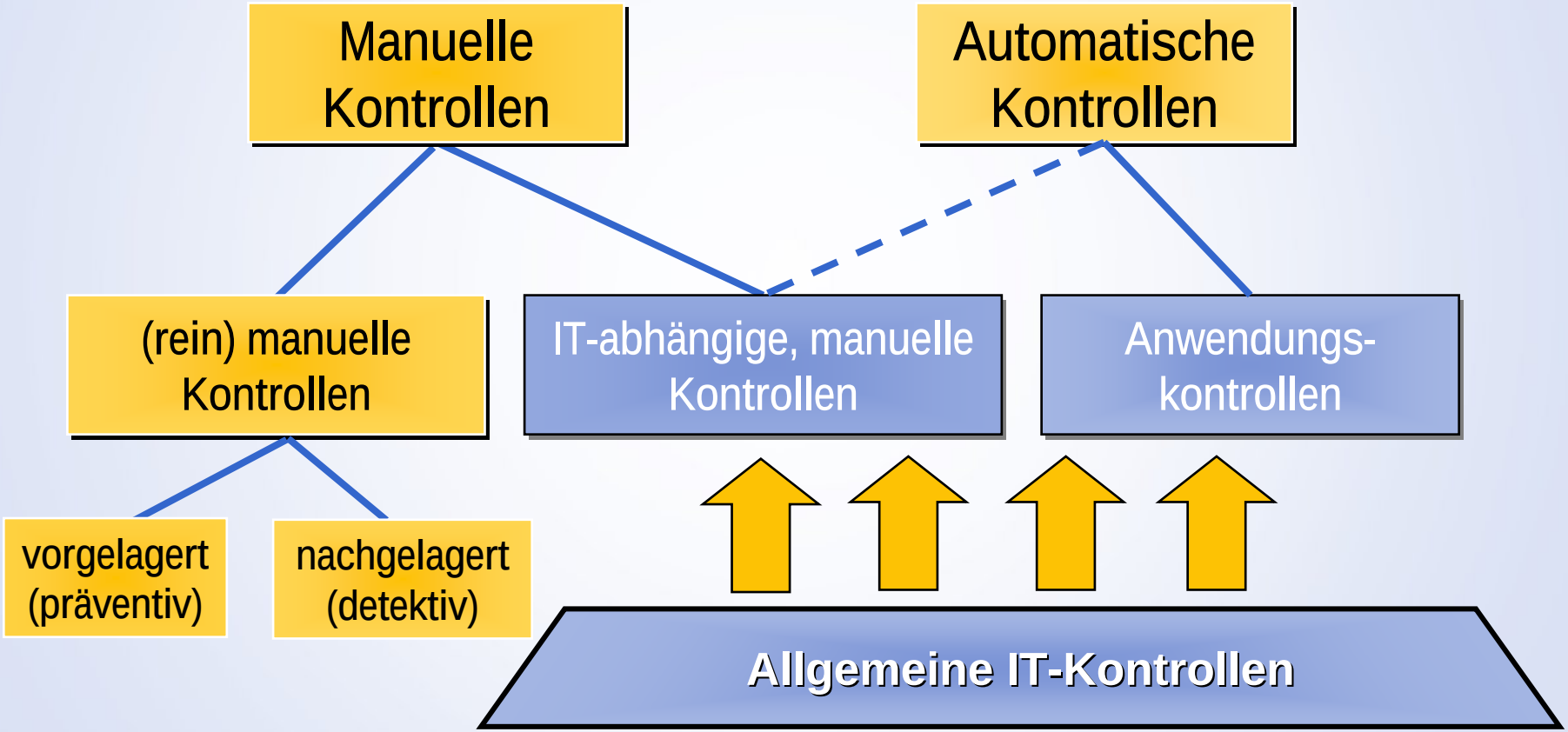
2 IT-Prüfungen im Rahmen der externen Revision

3 IT-Kontrollen und Risikoeinschätzung

4 Fazit

IT-Kontrollen und Risikoeinschätzung

Klassifizierung von Kontrollen



IT-Kontrollen und Risikoeinschätzung

Klassifizierung von IT-Kontrollen

Allgemeine Kontrollen:

- schaffen eine sichere Basis für IT-Prozesse und damit verbundene Kontrollen
- werden außerhalb der Anwendungen durchgeführt
  (Beispiel: physische Sicherheit, 3-Systeme Umgebung, Dokumentation, etc.)

Anwendungskontrollen:

- sichern die Korrektheit der Bearbeitung einzelner finanzieller oder nicht-finanzieller Transaktionen
- werden innerhalb der Anwendungen durchgeführt
  (z.B. Eingabe- oder Berechtigungskontrollen, Berechnungen, etc.)

IT-Kontrollen und Risikoeinschätzung

Allgemeine IT-Kontrollen – ausgewählte Inhalte

- Organisation, Funktionstrennung (Programmierung/ Betrieb, etc.), IT-Strategie
- Hardware und Netzwerke
  (Architektur, Produkte, Kompatibilität, Medienbrüche = Fehlerquelle)
- Software, Applikationen, Sicherheitstools (z.B. Firewall)
- Programmier- und Testverfahren
- Dokumentationsverfahren
- Physischer Zugangsschutz und Betriebsbereitschaft
- Logischer Zugangsschutz
- Datensicherungs- und Wiederanlaufverfahren
- Notfallkonzept

IT-Kontrollen und Risikoeinschätzung

IT-Anwendungskontrollen – ausgewählte Inhalte

Sicherstellung, dass alle digitalen Transaktionen

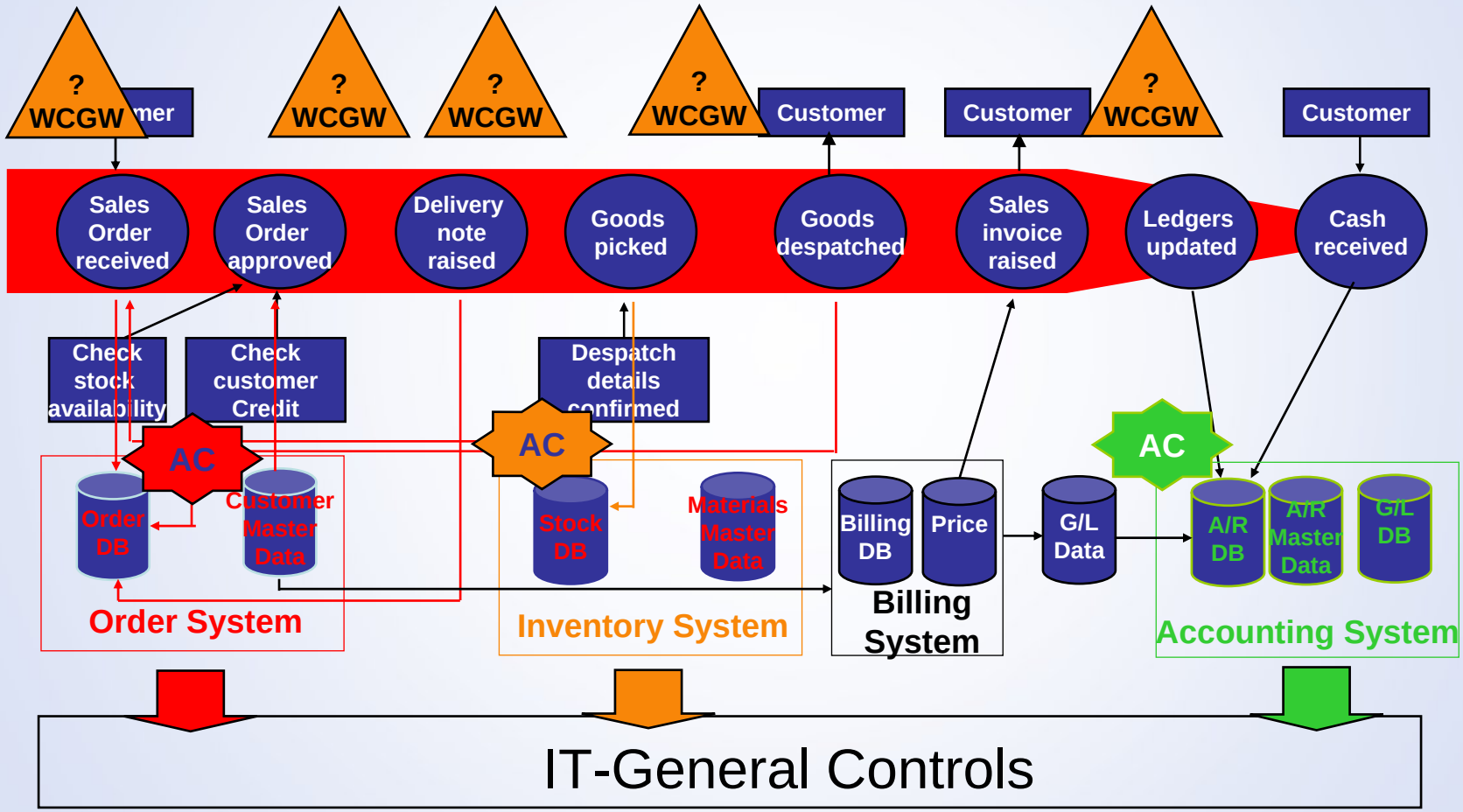
- **gültig**, **berechtigt** und **aufgezeichnet** sind, und
- **vollständig**, **richtig**, und **zeitnah** bearbeitet worden sind

z.B. Kontrollen über:

- Neuanlage, Änderung und Löschung von **Stammdaten** (Berechtigung, Prozess der Genehmigung, periodische Auswertungen, etc.), Beispiele sind Stammdaten für Material, Kreditoren, Debitoren, Konditionen, Konten, etc.
- Neuanlage, Änderung und Löschung von **Bewegungsdaten** (Prozess der Genehmigung, systemseitige Validierungen, etc.), Beispiele sind Bestellungen, Wareneingänge, Rechnungen, etc.
- Systemunterstütze (logische) **Funktionstrennung** zwischen den einzelnen Prozessschritten sowie angemessene **Dokumentation**

IT-Kontrollen und Risikoeinschätzung

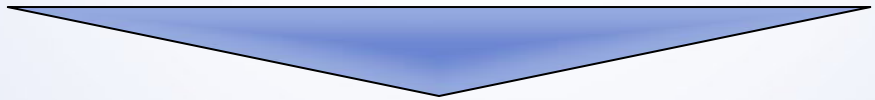
IT-Kontrollen – Beispiel Auftragsabwicklung



IT-Kontrollen und Risikoeinschätzung

Risikoeinschätzung

- Risikoeinschätzung ist Ausdruck des **risikoorientierten Prüfungsansatzes**
- Beurteilung der **IT-Fehlerrisiken** baut auf den **inhärenten Risiken** und den **IT-Kontrollrisiken** auf
- **Kontrollrisiko** wird durch die **allgemeinen IT-Kontrollen** und die **IT- Anwendungskontrollen** determiniert
- Ein **geringes inhärentes Risiko** bzgl. der rechnungslegungsrelevanten Teile der IT in Verbindung mit einem **geringen IT-Kontrollrisiko** führen zu einem **minimalen IT-Fehlerrisiko**



- Ein minimales IT-Fehlerrisiko führt i. a. zu deutlich **reduziertem** substantiellem (sprich: „beleghaftem“) Prüfungsaufwand

IT-Kontrollen und Risikoeinschätzung

Einfluss der IT-Risiken auf das Gesamtprüfungsrisiko

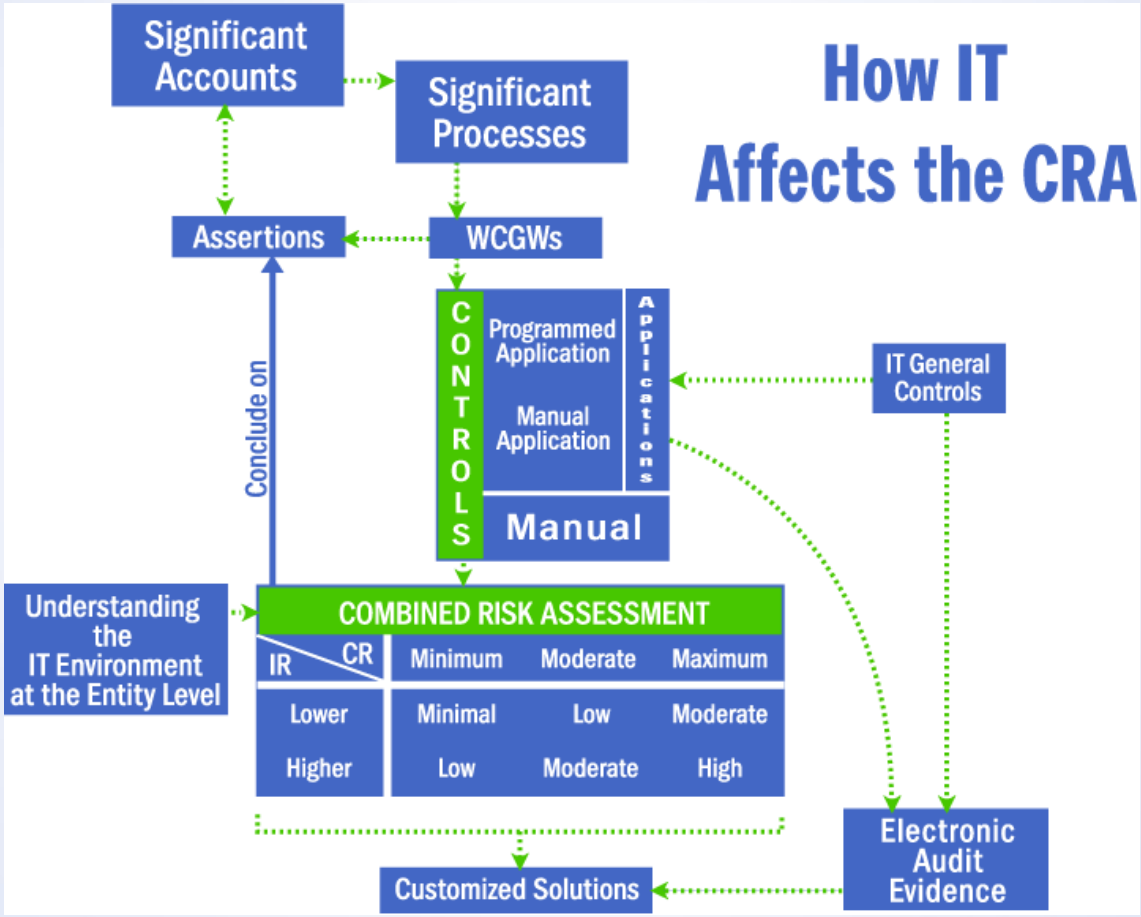


Abb.: EY-Modell zur kombinierten Risikoeinschätzung

Im Überblick

1 Ausgangssituation

2 IT-Prüfungen im Rahmen der externen Revision

3 IT-Kontrollen und Risikoeinschätzung

4 Fazit

Fazit

- Einschätzung des Prüfungsrisikos ohne Beurteilung der rechnungslegungs-relevanten Systeme ist mit zunehmender Komplexität der Unternehmens-prozesse nur schwer möglich bzw. **unmöglich.**
- Die Gewährleistung der Ordnungsmäßigkeit von relevanten Systemen ist ohne Einhaltung von **Sicherheitsgrundsätzen** nicht möglich.
- Der IT-Prüfungsansatz ist eine Ausprägung der **IKS-Prüfung** und erfordert besondere **Expertise**.
- Der Prüfungsansatz muss **risikoorientiert** sein und sich an der Unternehmensorganisation mit seinen Systemen und Prozessen ausrichten.
- Anteil der IT-bezogenen Prüfungshandlungen an den gesamten durchgeführten Prüfungshandlungen kann durchaus **gewichtig** sein.
- IT-Prüfungen leisten einen wesentlichen Beitrag zur **Erhöhung der Prüfungssicherheit** bei gleichzeitiger **Steigerung der Prüfungseffizienz.**

Vielen Dank für Ihre Aufmerksamkeit

Sabry Macher
Senior Manager
Certified Information Systems Auditor
Landschaftstraße 8
30159 Hannover
Tel: 0511 / 8508-17616
Fax: 0181 / 3943-17616
Mobil: 0160 / 939 - 17616
E-Mail: sabry.macher@de.ey.com