Studium der Wirtschaftswissenschaften an der Gerhard-Mercator-Universität in Duisburg. Bestellt als Wirtschaftsprüfer und Steuerberater. Weitere Qualifikationen: „Certified Information Systems Auditor“ (CISA), „Certified Information Security Manager“ (CISM) und „Certified in Risk and Information Systems Control (CRISC)“. Von 1996 bis 2016 beschäftigt bei einer mittelständischen Wirtschaftsprüfungsgesellschaft. Seit 2017 bei BANSBACH tätig als Leiter des Bereichs IT-Revision und verantwortlich für IT-Prüfung und IT-Beratung.

Jens Pfeifer

Partner bei der BANSBACH GmbH Wirtschaftsprüfungsgesellschaft Steuerberatungsgesellschaft

Compliance Conference
STUTTGART

3. Compliance Conference Stuttgart

Der Informationskongress für den Mittelstand

Schwerpunktthema: Digitalisierung und Datenschutz –
Risiko oder Chance für die Compliance

15. Mai 2018

Haus der Wirtschaft
Bertha-Benz-Saal

BRP

BANSBACH
Das ganze Spektrum

OPPENLÄNDER
RECHTSANWÄLTE

Eine Veranstaltung der Stuttgarter Zeitung Werbevermarktung GmbH

Digitalisierung von Prozessen - Digitalisierung von Compliance

Agenda

- Was ist Compliance?
- Was ist relevant für Compliance?
- Wie kann man Compliance umsetzen?
- Praxisbeispiel: Eingangsrechnungen
- Wer ist verantwortlich für Compliance?
- "Goldene Regeln"

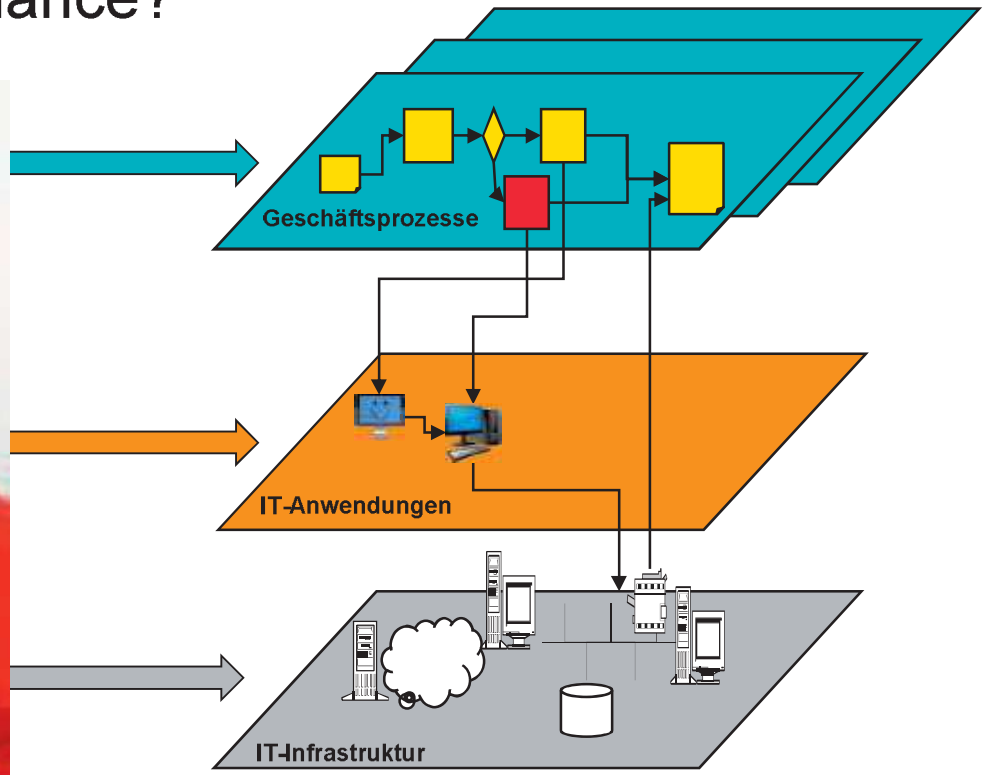
Digitalisierung von Prozessen - Digitalisierung von Compliance

Was ist Compliance?

- Institut der Wirtschaftsprüfer in Deutschland e.V.:
  Die Gesamtheit der Grundsätze und Maßnahmen eines Unternehmens zur Einhaltung bestimmter Regeln und damit zur Vermeidung von Regelverstößen.
- Deutschen Corporate Governance Kodex:
  Compliance [ist] die in der Verantwortung des Vorstands liegende Einhaltung der gesetzlichen Bestimmungen und unternehmensinternen Richtlinien.
- Kurz: "Einhalten von Regelungen"

Digitalisierung von Prozessen - Digitalisierung von Compliance

Was ist relevant für Compliance?



BANSBACH
Das ganze Spektrum

Digitalisierung von Prozessen - Digitalisierung von Compliance

Wie kann man Compliance umsetzen? - Vorgehen

- Identifikation von relevanten Regelungen
  - Externe Regelungen (z.B. gesetzliche Vorgaben)?
  - Spezielle externe Regelungen für digitale Unterlagen (z.B. Lesbarkeit)?
  - Interne Regelungen (z.B. Unterschriftenregelungen)?
- Übertragung auf die digitale Welt
  - Welche Regelungen aus der analogen Welt gelten weiter und wie kann ich diese auf die digitale Welt übertragen?
  - Design von Prozessen / Workflows
- Festlegung von Verantwortlichkeiten
  - Wer macht was?

Digitalisierung von Prozessen - Digitalisierung von Compliance

Wie kann man Compliance umsetzen? - Werkzeuge

- IT-Infrastruktur
  - Nutzung von unveränderlichen Speichermedien (z.B. Compliance Festplatten, WORM)
  - Sicherung von Daten gegen Verlust (z.B. Back-up Verfahren)
  - Verschlüsselung von Daten
- IT-Anwendungen
  - Protokollierung von Stammdatenänderungen
  - Logischer Zugriffsschutz (Passworte, Berechtigungen)
  - Eingabekontrollen (z.B. Datumsformate, Gültigkeitsbereiche)
  - Integrierte IT-gestützte Kontrollen verhindern Fehleingaben / Manipulationen (z.B. Warnhinweise bei unplausiblen Eingaben).

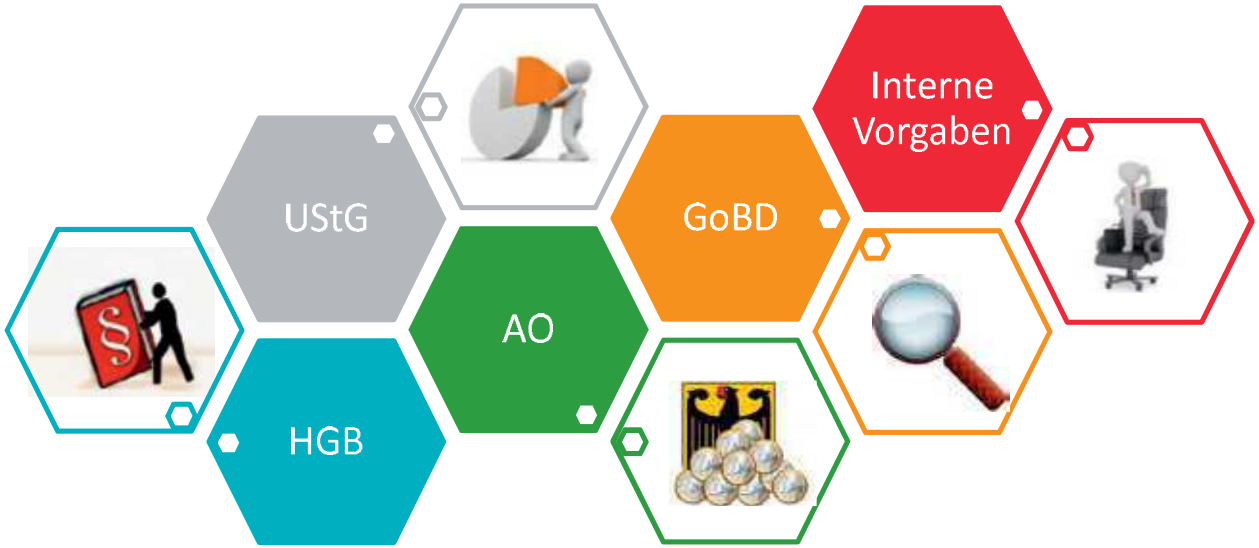
Digitalisierung von Prozessen - Digitalisierung von Compliance

Wie kann man Compliance umsetzen? - Werkzeuge

- Geschäftsprozesse
  - Berechtigungskonzepte (Wer darf was?)
  - Freigabe durch eine andere Person bei manuellen Erfassungen (Vier-Augen-Prinzip)
  - Verarbeitungskontrollen bei Schnittstellen zwischen IT-Systemen (z.B. Summenabgleich, Hash-Codes)
  - Konsistenzprüfungen zwischen verschiedenen Datenbeständen
  - Regelungen zum Fehlermanagement
- Dokumentationen
  - Beschreibung von Kontrollen mit Weisungscharakter
  - Führen und Aufbewahren von Kontrollnachweisen
- Schulungen / Sensibilisierungen

Digitalisierung von Prozessen - Digitalisierung von Compliance

Praxisbeispiel Eingangsrechnungen: Relevante Vorgaben



Digitalisierung von Prozessen - Digitalisierung von Compliance

Praxisbeispiel Eingangsrechnungen: Mögliche Interne Kontrollen

- Freigaberegelungen,
- Informationspflichten,
- Kontierungsvermerke,
- Dokumentation,
- Lieferantenbewertung,
- Rückverfolgbarkeit,
- etc.

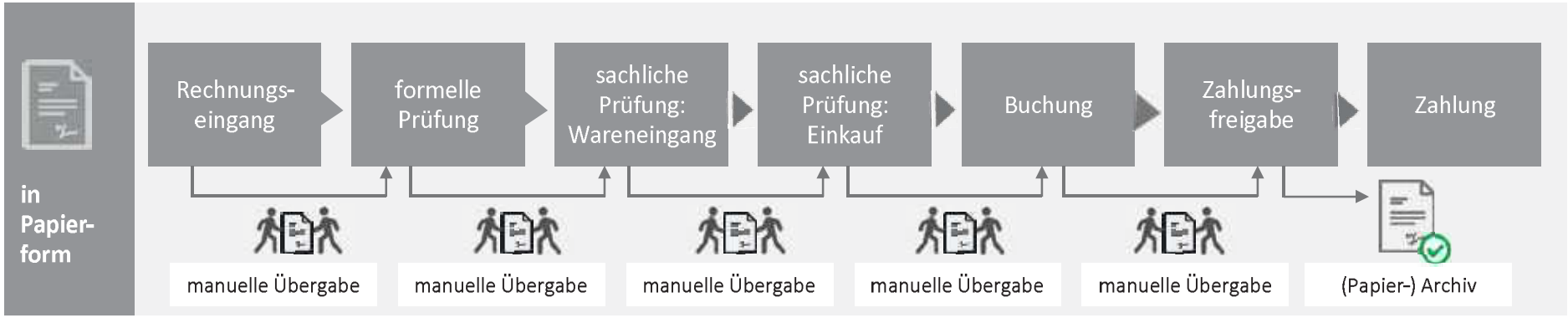
Digitalisierung von Prozessen - Digitalisierung von Compliance

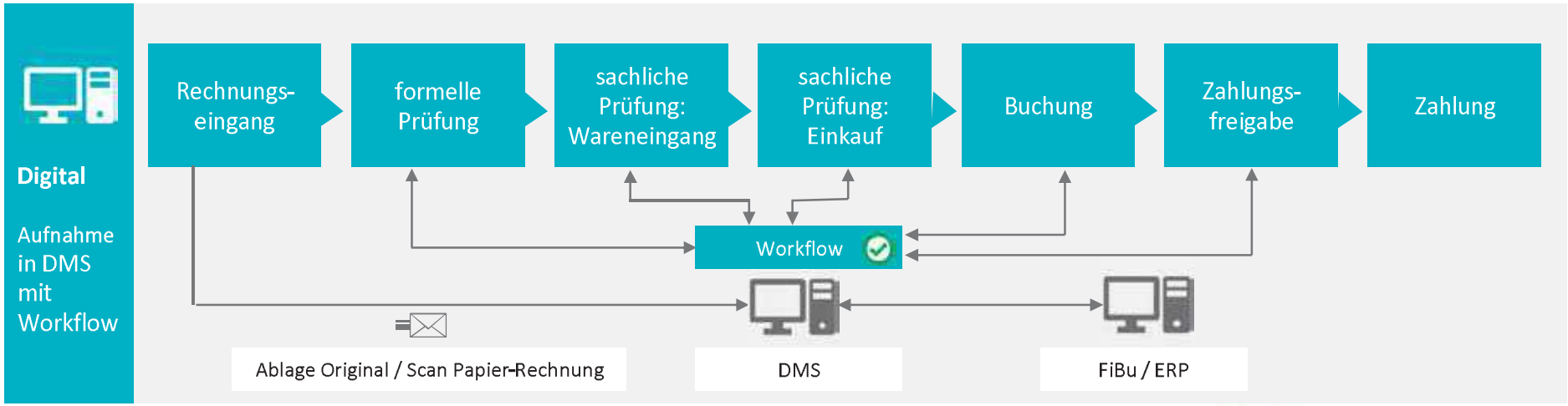
Praxisbeispiel Eingangsrechnungen: Steuerliche Aspekte

- Qualifizierte elektronische Signatur (§ 14 Abs. 3 Nr. 1 UStG),
- Elektronischer Datenaustausch (§ 14 Abs. 3 Nr. 2 UStG) oder
- "Dritter Weg" (§ 14 Abs. 1 UStG)
  - Innerbetriebliches Kontrollverfahren hinsichtlich Echtheit der Herkunft und Unversehrtheit des Inhalts
  - Unverzügliche Lesbarkeit
- Anforderungen der GoBD[1)]
  - Maschinelle Auswertbarkeit: mathematisch-technische Auswertung, Volltextsuche oder Prüfbarkeit auf anderem Wege
  - Revisionssichere Aufbewahrung im Originalformat

1) Grundsätze zur ordnungsmäßigen Führung und Aufbewahrung von Büchern, Aufzeichnungen und Unterlagen in elektronischer Form sowie zum Datenzugriff (GoBD)

Digitalisierung von Prozessen - Digitalisierung von Compliance





BANSBACH
Das ganze Spektrum

Digitalisierung von Prozessen - Digitalisierung von Compliance

Praxisbeispiel Eingangsrechnungen: Verantwortlichkeiten

Operativ	Vorgabe und Überwachung	Nicht verantwortlich
Buchhaltung	Geschäftsführung	Interne Revision
Wareneingang	Compliance Beauftragter	Wirtschaftsprüfer
Einkauf		
Prokurist		

Digitalisierung von Prozessen - Digitalisierung von Compliance

"Fünf goldene Regeln"

1. Identifizieren der Anforderungen und Besonderheiten

2. Definition der Prozesse und der dazugehörigen Kontrollen

3. Anforderungen und Prozess bestimmen die Auswahl der IT-Anwendung. Nicht umgedreht!

4. Berücksichtigen Sie alle Ebenen des IT-Systems (Prozesse, Anwendungen und Infrastruktur)

5. Dokumentieren: Viel, aber nur das Wichtige!

BANSBACH

Digitalisierung von Prozessen - Digitalisierung von Compliance

Haben Sie noch Fragen?

IHR ANSPRECHPARTNER:

Jens Pfeifer
Wirtschaftsprüfer, Steuerberater,
CISA, CISM, CRISC

Gänsheidestraße 68-74
70184 Stuttgart
Telefon: 0711-1646-867
E-Mail: jens.pfeifer@bansbach-gmbh.de