

Prüfung von digitalen Geschäftsmodellen

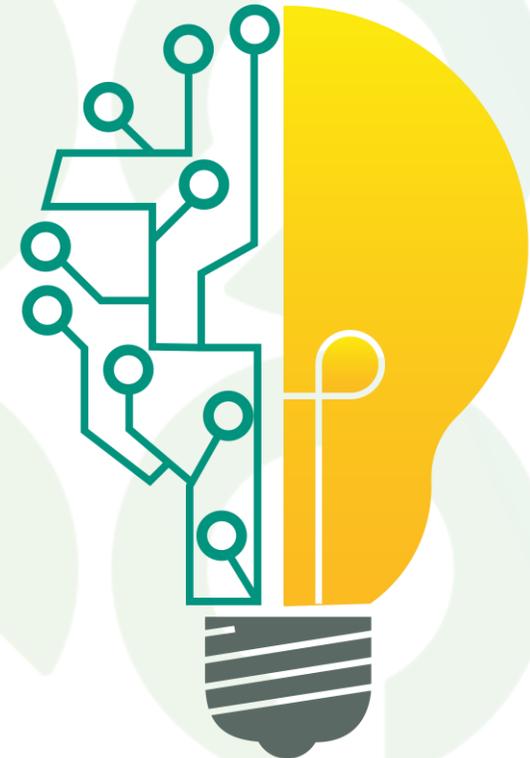
ISACA Barcamp, Workshop 1
Ralf Herter, BASF
Stefanie Schmidt, DZ BANK AG

2. Juni 2022

Digitalisierung und digitale Geschäftsmodelle

Warum ist das Thema Digitalisierung wichtig?

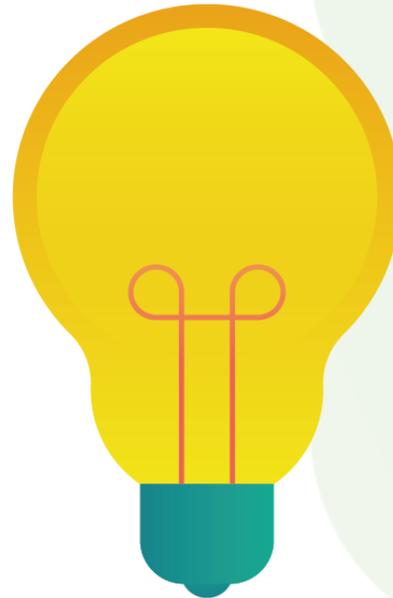
- Corona treibt die Digitalisierung voran (– aber nicht alle Unternehmen können mithalten)
- Digitalisierte Unternehmen kommen besser durch die Krise
- Jeder Vierte sieht sich als Vorreiter bei der Digitalisierung
- Unternehmen ergreifen eine Vielzahl konkreter Digitalisierungsmaßnahmen
- Digitalisierungs-Hemmnisse: Geld und fehlende Lösungen verzögern die Digitalisierung



Digitalisierung und digitale Geschäftsmodelle

Der Begriff Digitalisierung

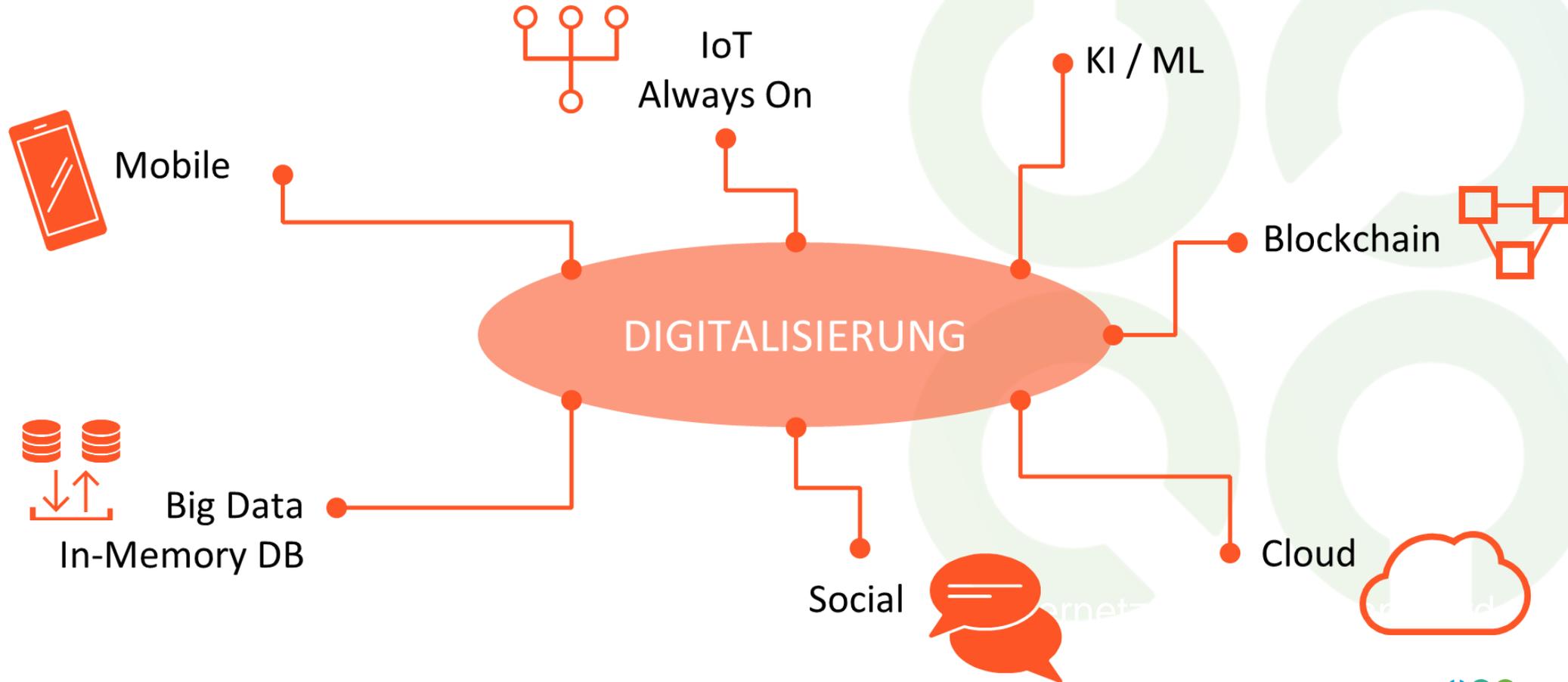
Digitalisierung bezeichnet allgemein die Veränderungen von Prozessen, Objekten und Ereignissen, die bei einer zunehmenden Nutzung digitaler Geräte erfolgt. Im engeren Sinne ist dies die Erstellung digitaler Repräsentationen von physischen Objekten, Ereignissen oder analogen



Im weiteren (und heute meist üblichen) Sinn steht der Begriff insgesamt für den Wandel hin zu IT-gestützten und automatisierten Prozessen mittels Informations- und Kommunikationstechnik.

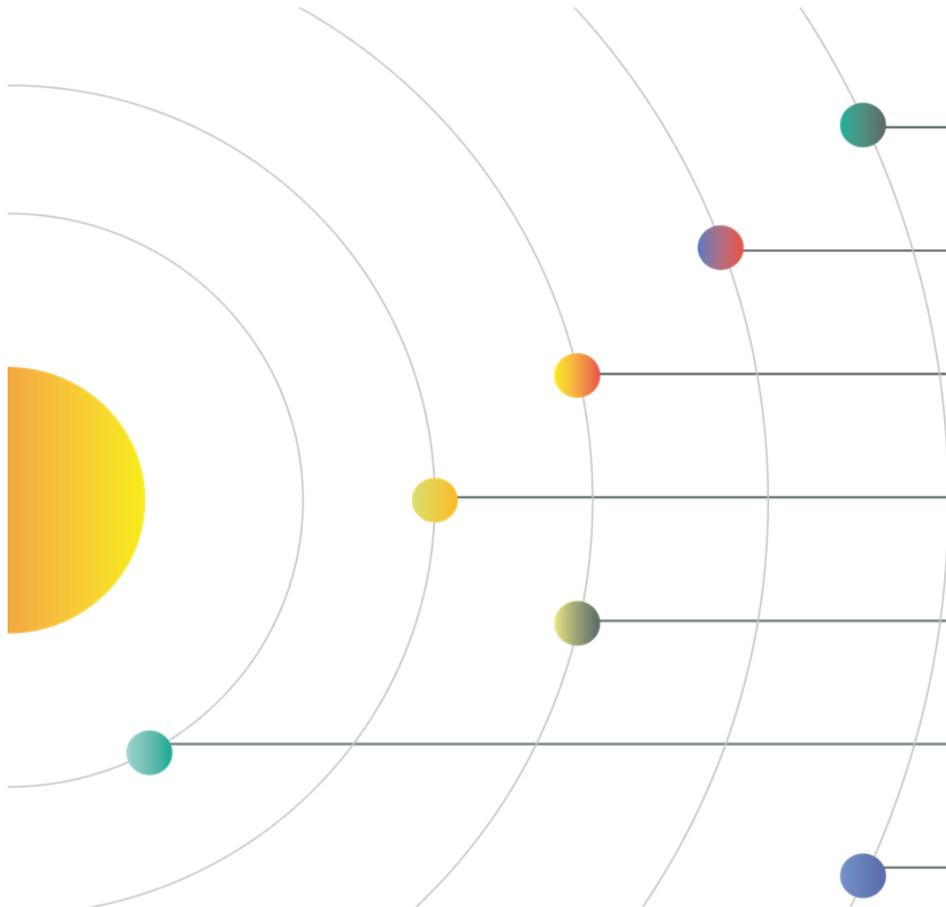
Digitalisierung und digitale Geschäftsmodelle

Sieben Technologietrends der Digitalisierung



Vorschlag für die Diskussion

Welche Handlungsfelder möchtet Ihr vertiefen ?



- Neue Technologien werden eingesetzt und müssen verstanden werden.
- Prozesse laufen automatisiert und digital ab und verändern das Prüfungsverfahren.
- Prozesse sind zum Teil unternehmensübergreifend mit Schnittstellen zu Lieferanten und / oder Kunden.
- Die richtige Funktion von Schnittstellen und die Verarbeitung von Transaktionsdaten ist wesentlich.
- Die Ordnungsmäßigkeit und Sicherheit der IT-Prozesse und Systeme ist kritisch.
- Die fachlichen und methodischen Anforderungen an die Fach- und IT-Revision ändern sich.
- Automatisierte Prüfungstechniken können genutzt werden (CCM, Online Audits).

Diskussion zur Begriffsklärung

Frage der Risikobeurteilung – Existiert das Risiko tatsächlich?

Wie gehen wir damit um?

- Risikobetrachtung – welche Technologie wird eingesetzt.
- Kenntnisse der Technologie sind erforderlich
- Differenzierung nach Standort on-prem oder in der Cloud
- Betrachtung des Technologiestacks kann sich aus einem Mix von on-prem und XaaS Schichten ergeben, erhöht die Komplexität, differenzierte Anforderungen an IT-Governance
- on-prem ist es transparenter; bei XaaS komme ich nicht leicht an die Informationen heran.
- XaaS-Anbieter wie einen IT-Dienstleister prüfen (prinzipiell)
- auf Prüfungsberichte des XaaS zurückgreifen
- kein „blindes“ Vertrauen in den IT-Dienstleister; Schwierigkeit zu validieren

Thema Umsatzrealisierung

- Wie kann ich das validieren? Wonach wird der Anbieter bezahlt? Ggf. Anzahl „clicks“. tatsächliches Bankguthaben ist nicht gleich Umsatzrealisierung => Wie also messen?

automatisierte Prüfungstechniken

Erfahrungen?

- Cloud Prüfung bei AWS: von AWS gezeigt bekommen, was für Techniken zum Einsatz kommen und was alles möglich wäre
 - Vielfalt an Analysemöglichkeiten durch AWS angeboten; Nutzung dieser neuen Angebote
 - Ist das vertrauenswürdig? zusätzliche Absicherungsmöglichkeiten einsetzen für die Validierung der Prüfergebnisse.
 - externer WP prüft die Controls und veröffentlicht Ergebnisse in einem Report (e.g. SOX Report)
 - gezielte Nachfragen möglich
- RPA – nutzbar?
 - gleichartige Kontrollen und Nachweise mit einem Processmining koppeln – Auffälligkeiten?
 - Test-of-One reicht dann aus und reduziert die Grundgesamt; funktioniert bei SAP LOG
 - Kamunda Process Engine, Service Now und SAP; wo LOGS zur Verfügung stehen (e-2-e Sicht herstellen)
- CCM – automatisiertes Vorgehen => Übergabe an den operativen Betrieb
- Aufbau von Technologieansätzen mit Hilfe von Tools aus dem PaaS-Stack

neue Technologien / automatisierte Prozesse

Wie finde ich heraus, ob die Technik den Prozess auch tatsächlich unterstützt?

- Whitebox-Ansatz – arbeitet das Werkzeug an sich korrekt?
 - Voraussetzung ausreichend Transparenz
- Blackbox-Ansatz – kommt das richtige Ergebnis heraus, dann hat das Tool richtig gearbeitet
- von der Fachlichkeit kommend, mit dem Prozess starten
 - Sind die Vorgaben angemessen?
- vom ursprünglichen Ziel kommend – Metriken, wie zum Beispiel Lead Time
- Welche Strategie wird verfolgt?
- vom Business Case kommend => Mut haben zu sagen, dass sich das Modell vom Business Case her nicht lohnt. „Heiteres Scheitern“
 - Analyse von Proof-of-Concepts?
 - Was hat die Entscheidung getriggert? Waren alle wesentlichen Ansprechpartner, alle Lines involviert?

Es gibt einen ISACA Ansatz zu integrated Audit Verfahren. Erfahrungsansätze aus der Praxis?

- Integration in das Endprodukt? Protokolle im Endprodukt
- Datenschutz – revisionsfähige Reports eines Audit Trails
- oftmals fehlt es an der Anforderung hierzu

Berücksichtigung von Cyber-Risiken

Berücksichtigung von Cyber-Risiken im Kontext von Digitalisierungslösungen

- Prüffeld unter Security Aspekten analysieren

oder

- eine reine ISMS Prüfung

oder

- Prüfung des Betriebsführungskonzepts

oder

- Prüfung einer bestimmten Sicherheitstechnologie, z.B. Firewalls
- Prüfung der organisatorischen Struktur, insbesondere Rollenverständnis

Einsatz von „datenschutz- oder betriebskritischen“ KI-Analyse Tools zur Threat Detection und –Prävention

Problem der Fachexpertise als IT-Revisor – Einsatz von SME

- Wie geht der Prüfer mit dem Prüferisiko um?
- Es ist unsere Pflicht die Themen anzusprechen; nach Grundlagen zu fragen und dann an Experten abzugeben.

Umgang mit Widerständen im Fachbereich

- funktioniert über Awareness Erzeugung bei der Geschäftsführung, weil haftend
- kann zu Einschränkungen im Testat führen

Unsere Kontaktdaten



Stefanie Schmidt

DZ BANK AG

Konzern-Revision

IT Infrastruktur

M +49 151 15942024

<mailto:stefanie.schmidt@dzbank.de>



Ralf Herter

BASF Digital Solutions GmbH

Datenschutzbeauftragter

M +49 621/ 60-59607

<mailto:ralf.herter@basf.com>



ISACA®

Germany Chapter