Wie man Multi-Compliance in die Bereitstellung von IT-Services integriert

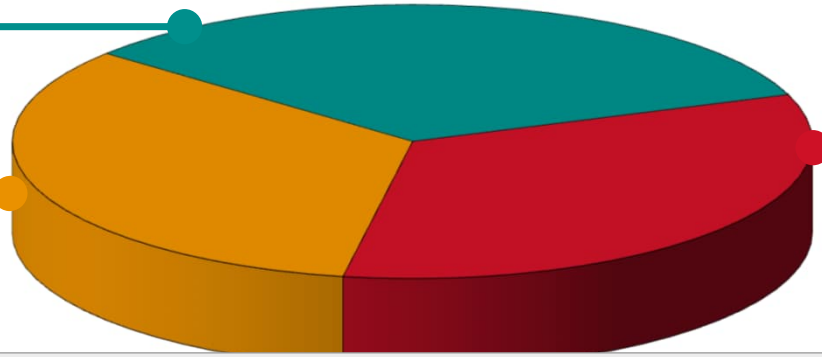
Security Forum 2026
Brandenburg an der Havel

Prof. Dr. Eberhard von Faber

Grundanforderungen und Steuerungslogik: GRC

Governance

Effektive Führung und Kontrolle
- Richtlinien und System für Steuerung/Kontrolle
- Unternehmensorganisation und -prozesse



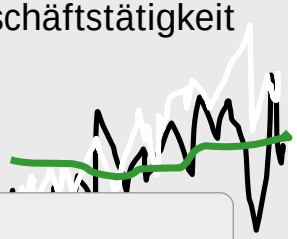
Compliance

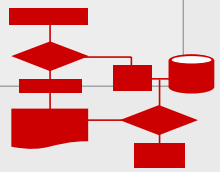
Einhaltung interner und externer Normen
- Identifikation von Richtlinien, Gesetzen, vertraglichen Anforderungen usw.
- Durchsetzung und Kontrolle

Risk Mgmt.

Umfassendes Risikomanagement
- Identifikation und Bewertung
- Reaktion und Kontrolle

A) Umfeld und Märkte, Geschäftstätigkeit





B) IT-Sicherheit:
- business processes
- information, data
- applications
- systems, networks

Security-Compliance

Welche Übereinstimmung? Warum notwendig?

- Ursprung
  - Gesetze / Verordnungen
    - welches Land? EU?
    - welchen Anwendungsbereich?
  - Best Practice / Industriestandard,
  - Branche,
  - eigene Organisation
- Wessen Anforderungen? Wessen Aufgabe?
  - IT-Dienstleister,
  - Anwenderorganisation (Kunde),
  - beide?
- Unterschiedliche Sprache und Detailtiefe!
- Ein IT-Dienstleister, viele Kunden?

Multi-Compliance = es sind diverse Kataloge einzuhalten

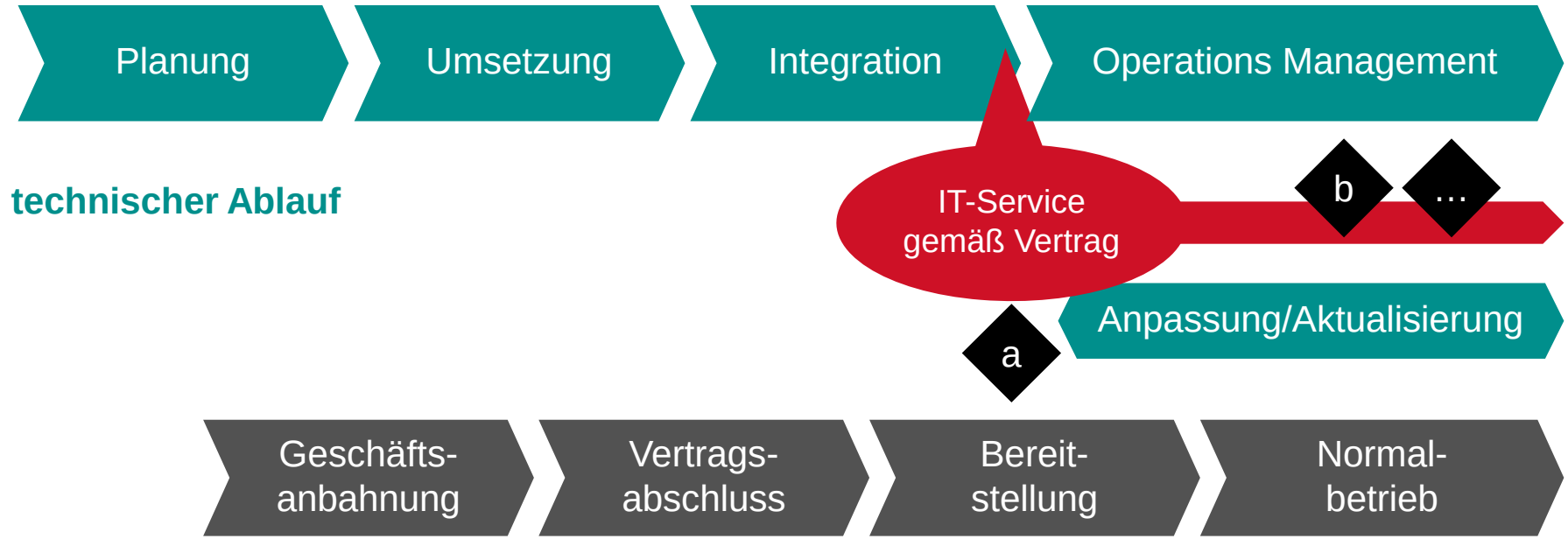
Zwei Ansätze, die nicht funktionieren – ... und zwei Lösungen.

1. Alle Anforderungskataloge den Entwicklern „zur Einhaltung“ übergeben.

2. IT-Services entwickeln, dann die Compliance prüfen und ggf. nachsteuern.

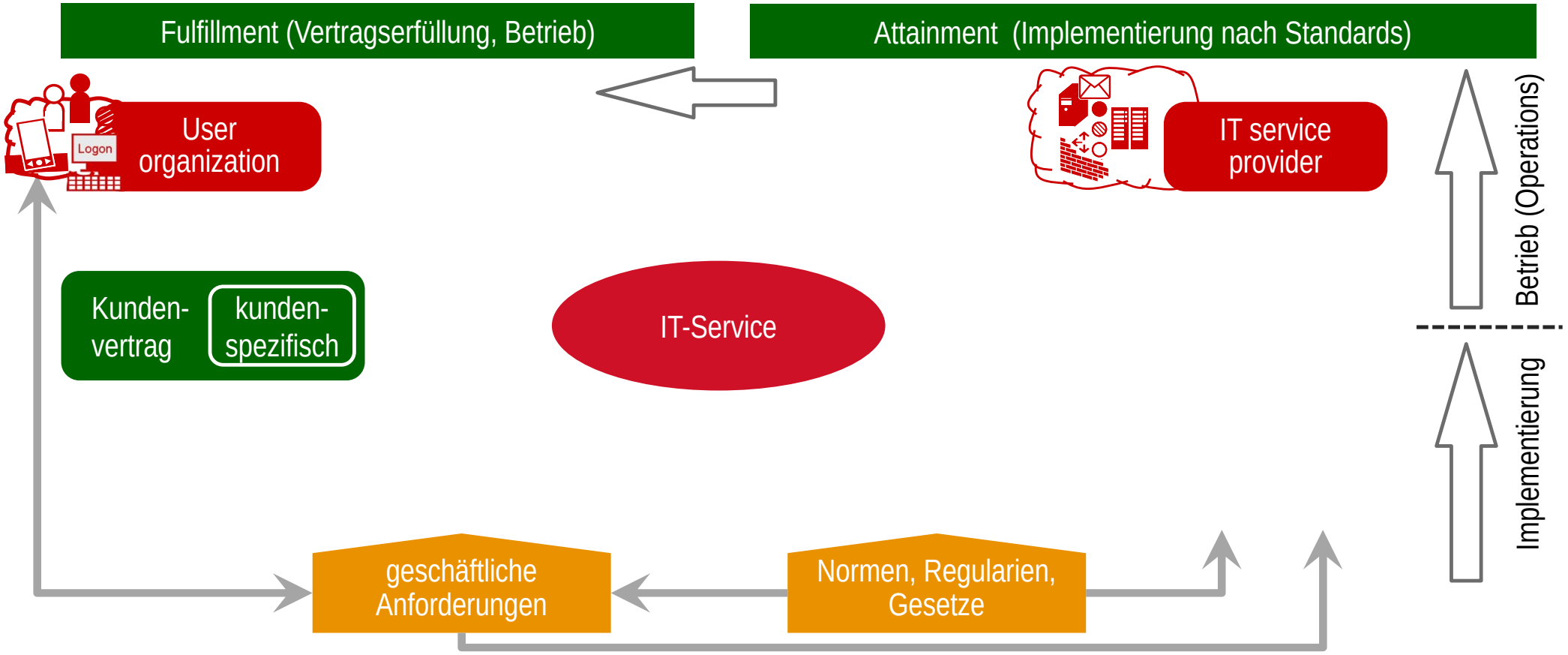
Zwei weitere Probleme - ... zwei weitere Lösungen.

3. IT-Service wird angepasst und aktualisiert ... Betriebsphase abdecken (technischer Ablauf)

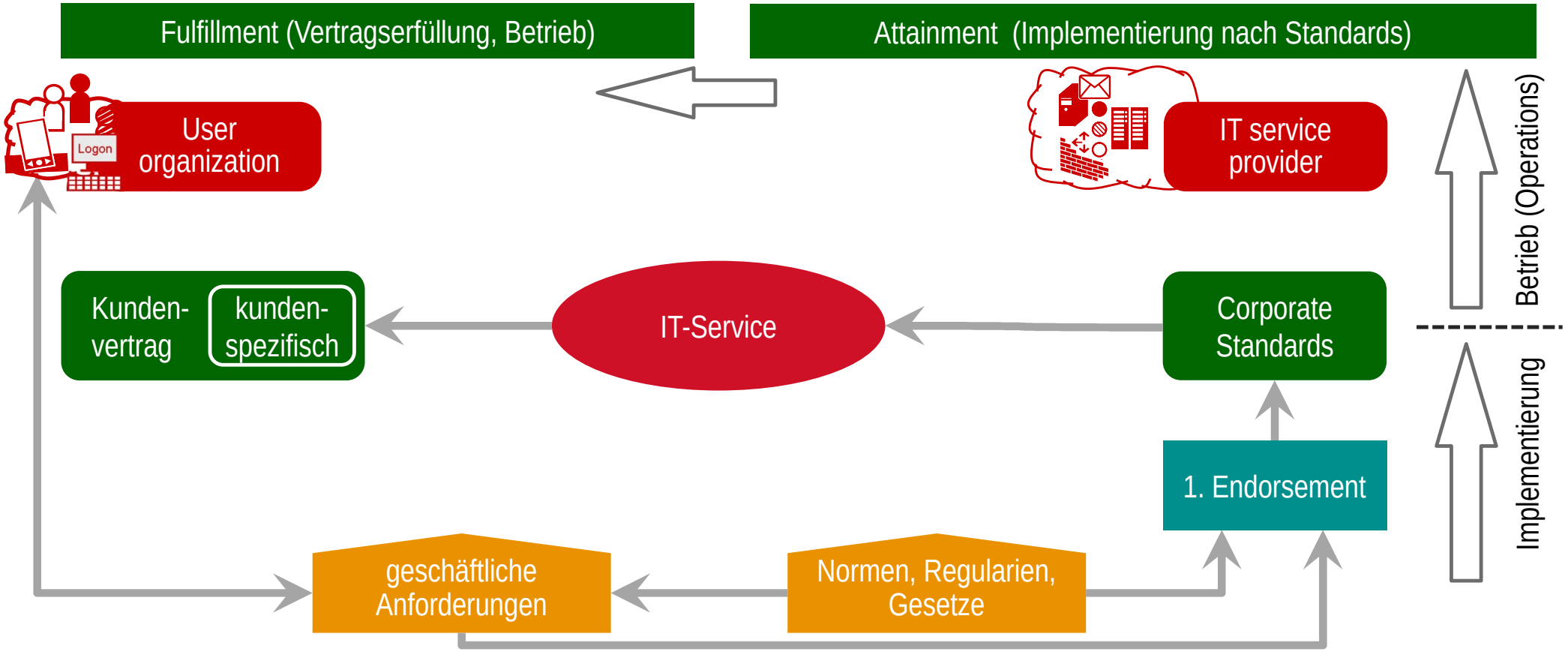


4. Zusagen und Verträge eingehalten? ... beides einbeziehen! (geschäftlicher Ablauf)

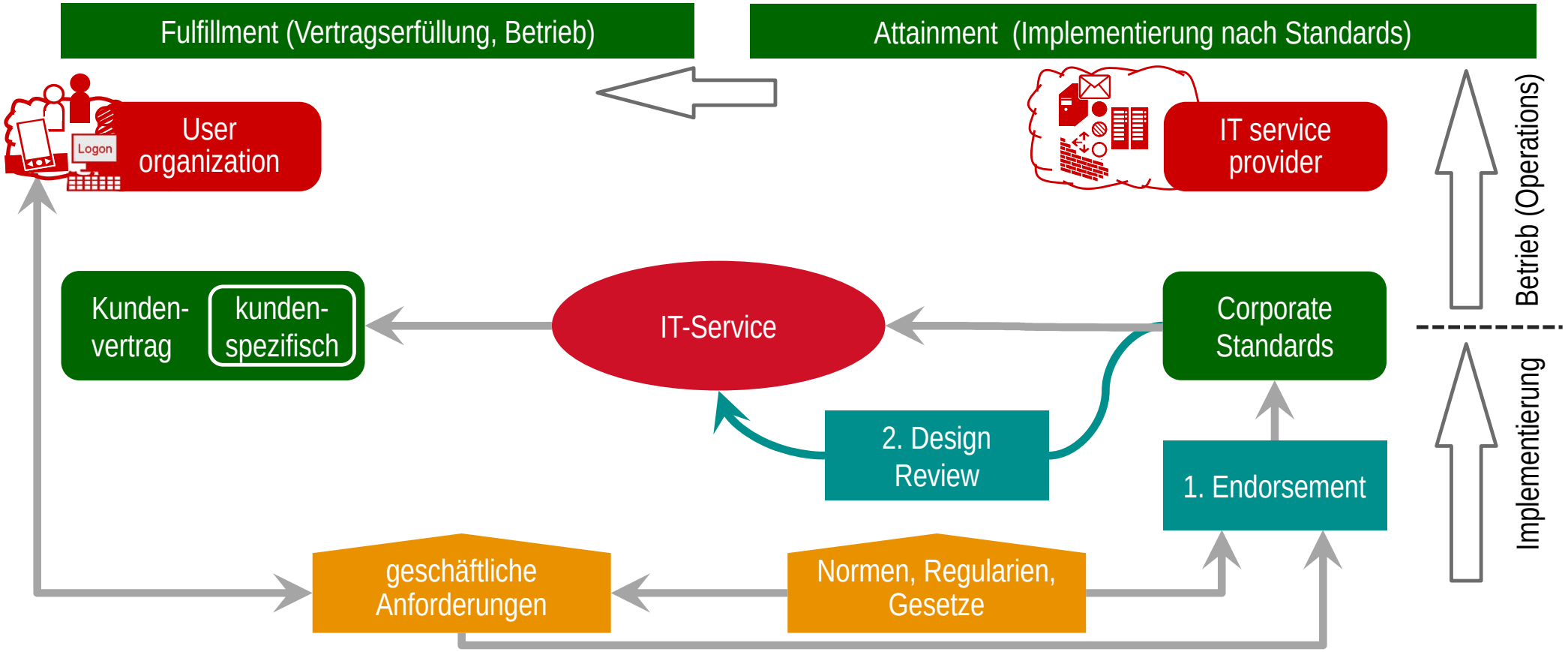
Compliance-System: 0. Genereller Plot



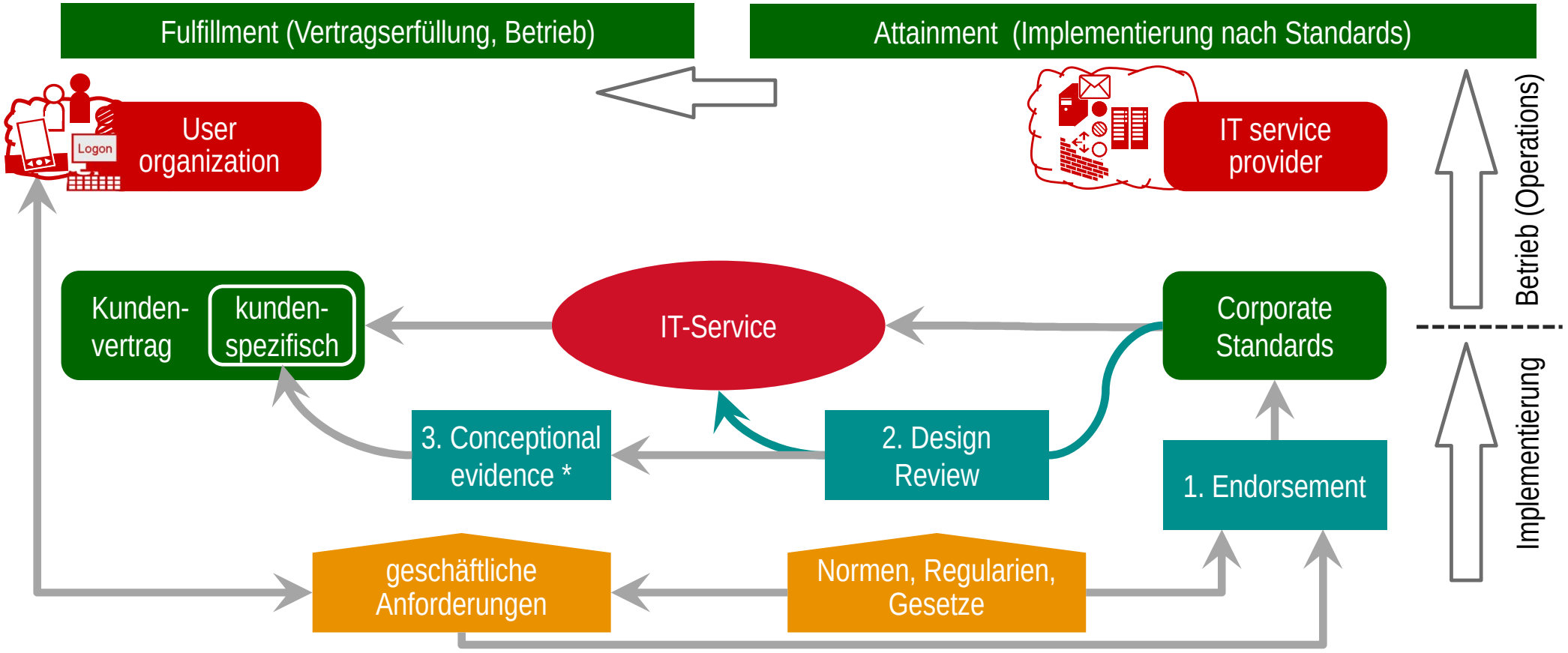
Compliance-System: 1. Endorsement; interne Standards mit Optionen



Compliance-System: 2. Design-Reviews; Umsetzung sicherstellen

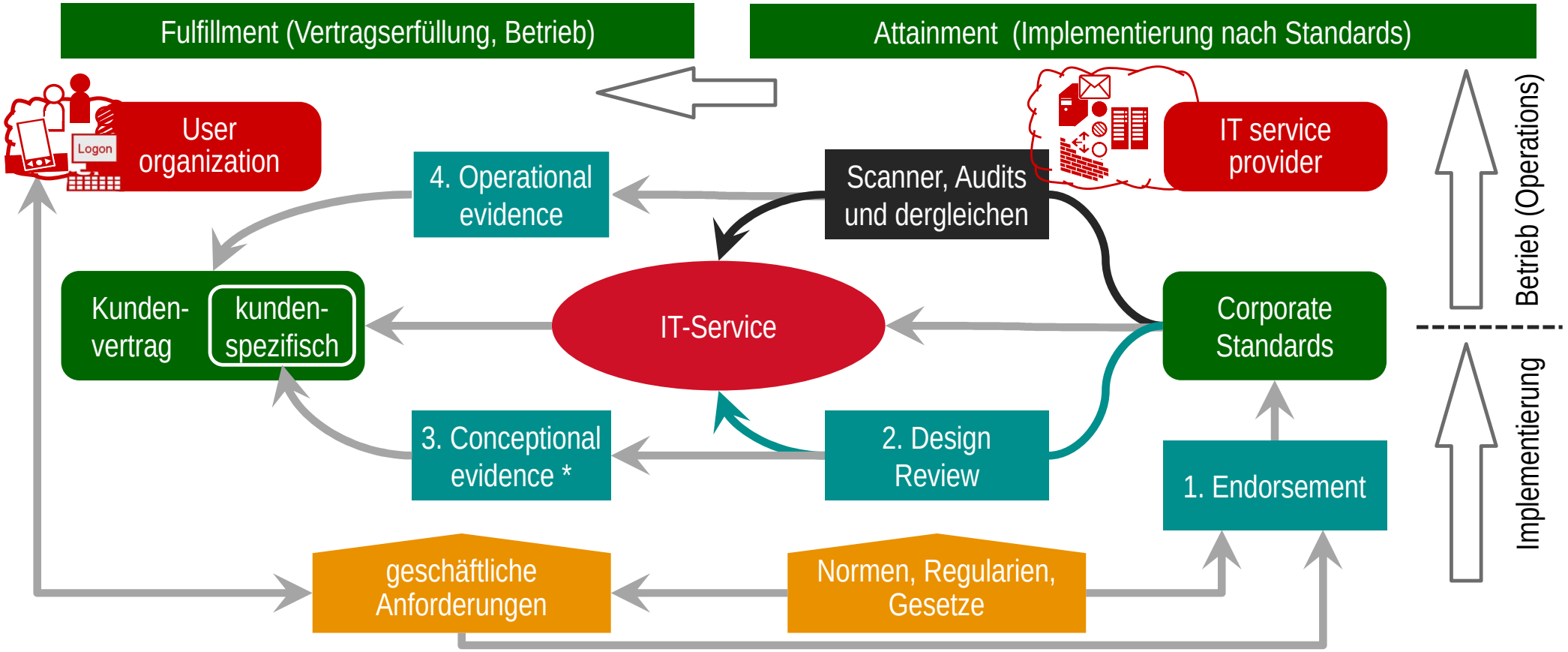


Compliance-System: 3. Einhaltung des Vertrages sicherstellen



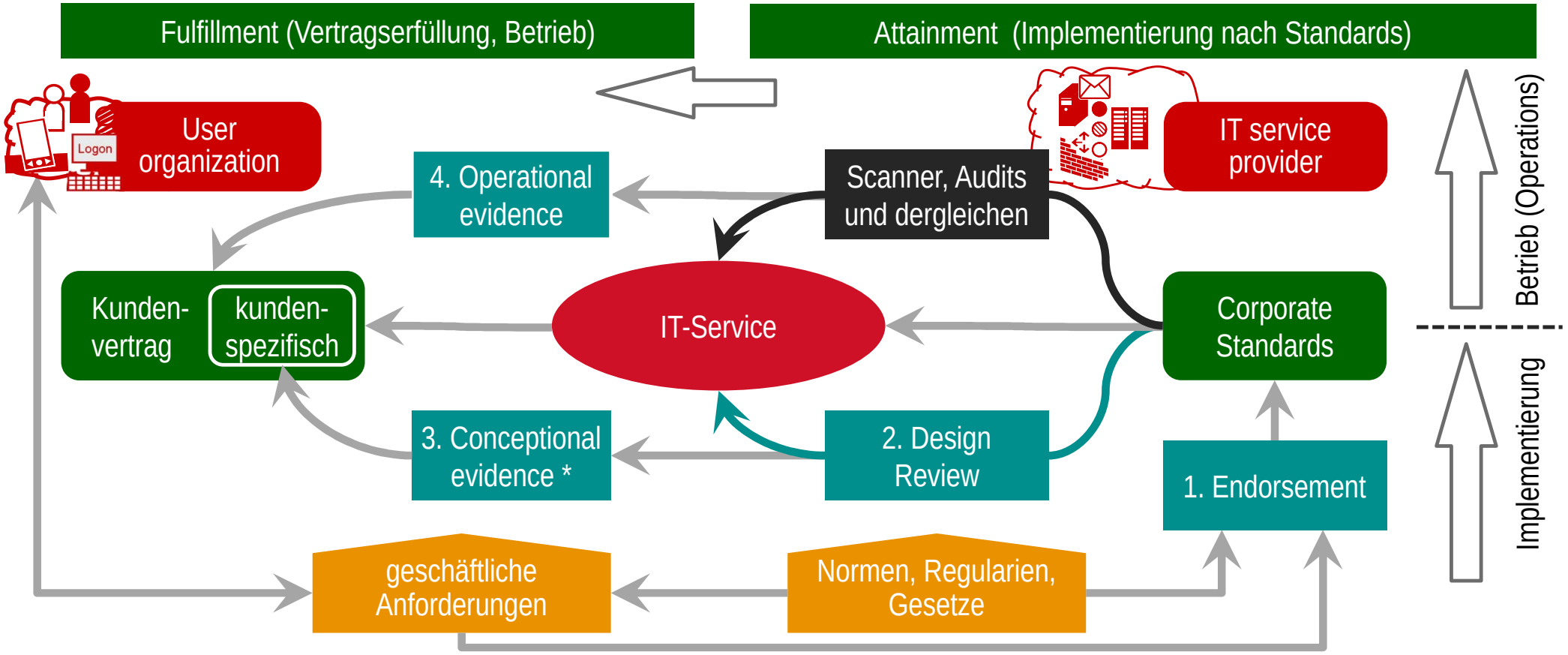
* nur relevant im Falle kundenindividueller Verträge bzw. Vertragsklauseln

Compliance-System: 4. Übereinstimmung im Betrieb sicherstellen



* nur relevant im Falle kundenindividueller Verträge bzw. Vertragsklauseln

Vier Arten von Compliance-Untersuchungen.



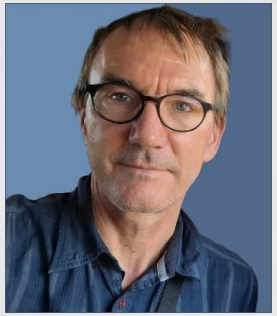
* nur relevant im Falle kundenindividueller Verträge bzw. Vertragsklauseln

Zusammenfassung:

1. Es gibt viele evtl. relevante Anforderungskataloge („Multi-Compliance“). Sie haben unterschiedliche Detailierungsgrade und Anwendungsbereiche.
2. Die Anforderungskataloge müssen (unter Verwendung von Optionen) in eigene, interne Standards des IT-Dienstleisters transformiert werden.
3. Diese umfangreichen Vorarbeiten erfordern ein eigenes System („Endorsement Framework“).
4. Der IT-Dienstleister setzt die eigenen, internen Standards und deren Optionen im Hinblick auf den Kunden, Service und das Einsatzgebiet um.
5. Ein Compliance-Vergleich reicht nicht aus. Es sind bis zu vier Vergleiche entlang des Lebenszyklus eines IT-Service nötig: Endorsement, Design-Review, Conceptional Evidence* und Operational Evidence.

* entfällt bei IT-Services nach vordefinierten AGB

Danke für Ihre Aufmerksamkeit!



Prof. Dr. Eberhard von Faber
Technische Hochschule Brandenburg
Eberhard.vonFaber@th-brandenburg.de

Springer-Vieweg, Wiesbaden 2023, 143 Seiten,
30 farbige Abbildungen, ISBN 978-3-658-41932-5,
https://doi.org/10.1007/978-3-658-41933-2