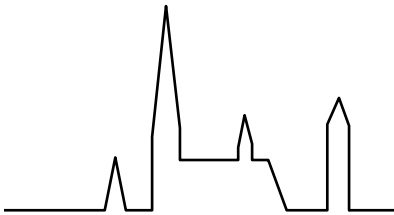
IT - Eine Lösung für Compliance?

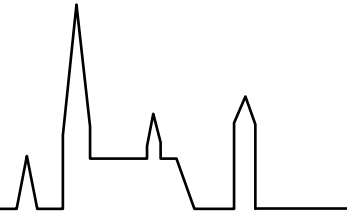


Dr. Stefan Sackmann

Institut für Informatik und Gesellschaft – Telematik
Albert-Ludwigs-Universität Freiburg
http://www.telematik.uni-freiburg.de/

Festkolloquium „Neueste Entwicklungen in der Informationstechnologie“
28. November 2008

Agenda



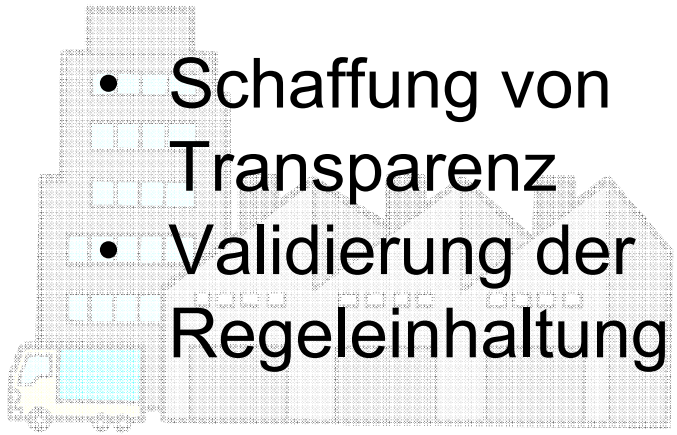
- Compliance: Validierung von Regeln
- Automatisierungsparadigmen „by design“ versus „by detection“
- Freiburger Ansatz
  - Trennung Geschäftsprozess- und Kontrollmodelle
  - Regelbasierter Ansatz
  - Integration Risikomanagement
- Fazit

Compliance – Transparenz und Validierung

- Gesetze
- Regularien
- Standards
- Richtlinien
- Governance
- Verträge
- …

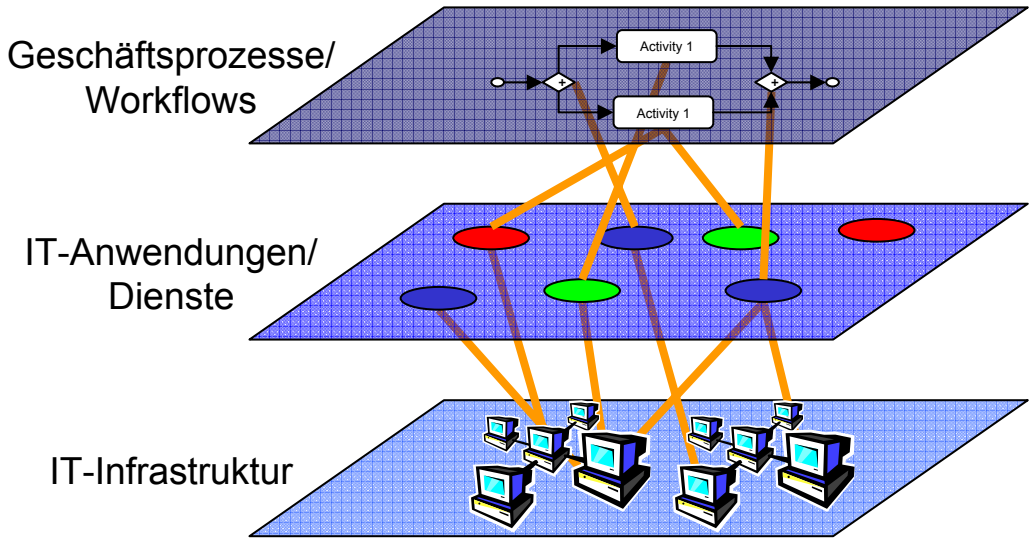
- Schaffung von Transparenz
- Validierung der Regeleinhaltung

Compliance – Fokus auf Geschäftsprozesse



- Schaffung von Transparenz
- Validierung der Regeleinhaltung

Modellierungsebenen Geschäftsprozesse



Doppelrolle der Informationssysteme:

- Gegenstand von Compliance
- Werkzeug für Transparenz und Validierung

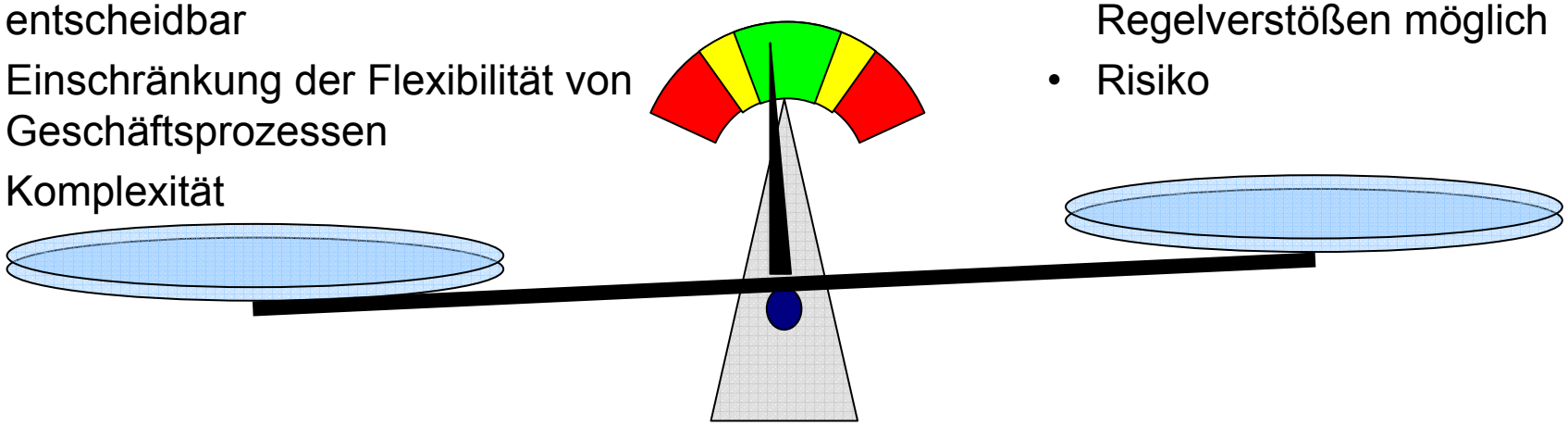
Paradigmen zur Automatisierung von Compliance

Compliance „by design“

- Ziel:
  Vermeidung von Regelverstößen
- Ansätze:
  - Entwurf regelkonformer Prozesse
  - Integration von Kontrollen in Geschäftsprozesse
- Grenzen:
  - Nicht alle Regeln „by design“ entscheidbar
  - Einschränkung der Flexibilität von Geschäftsprozessen
  - Komplexität

Compliance „by detection“

- Ziel:
  Erkennung von Regelverstößen
- Ansätze:
  - Monitoring
  - Auswertung von Log-Files/ Erzeugung von Evidenzen
- Grenzen:
  - Keine Verhinderung von Regelverstößen möglich
  - Risiko

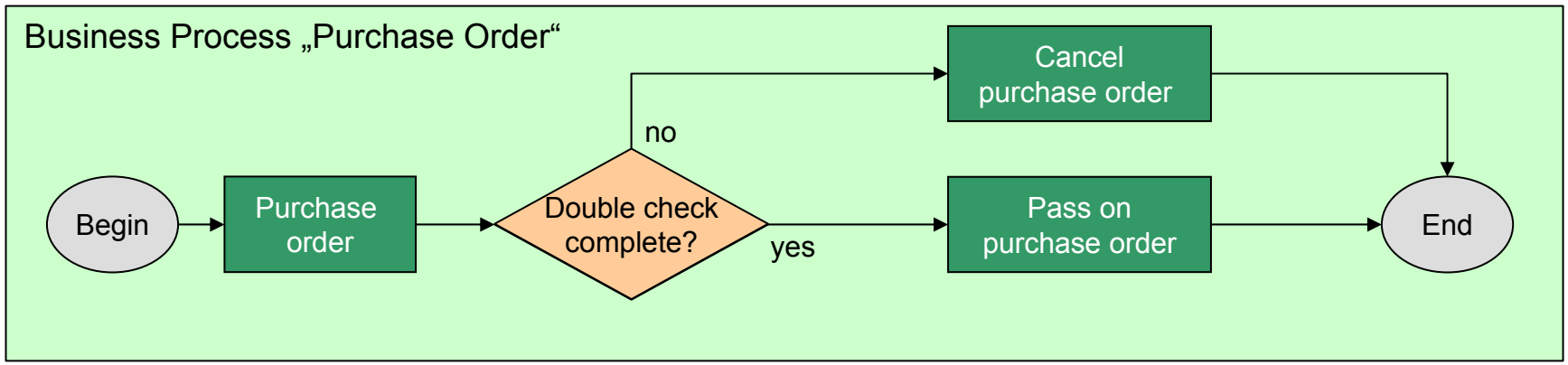


Allgemeiner, methodischer Ansatz erforderlich

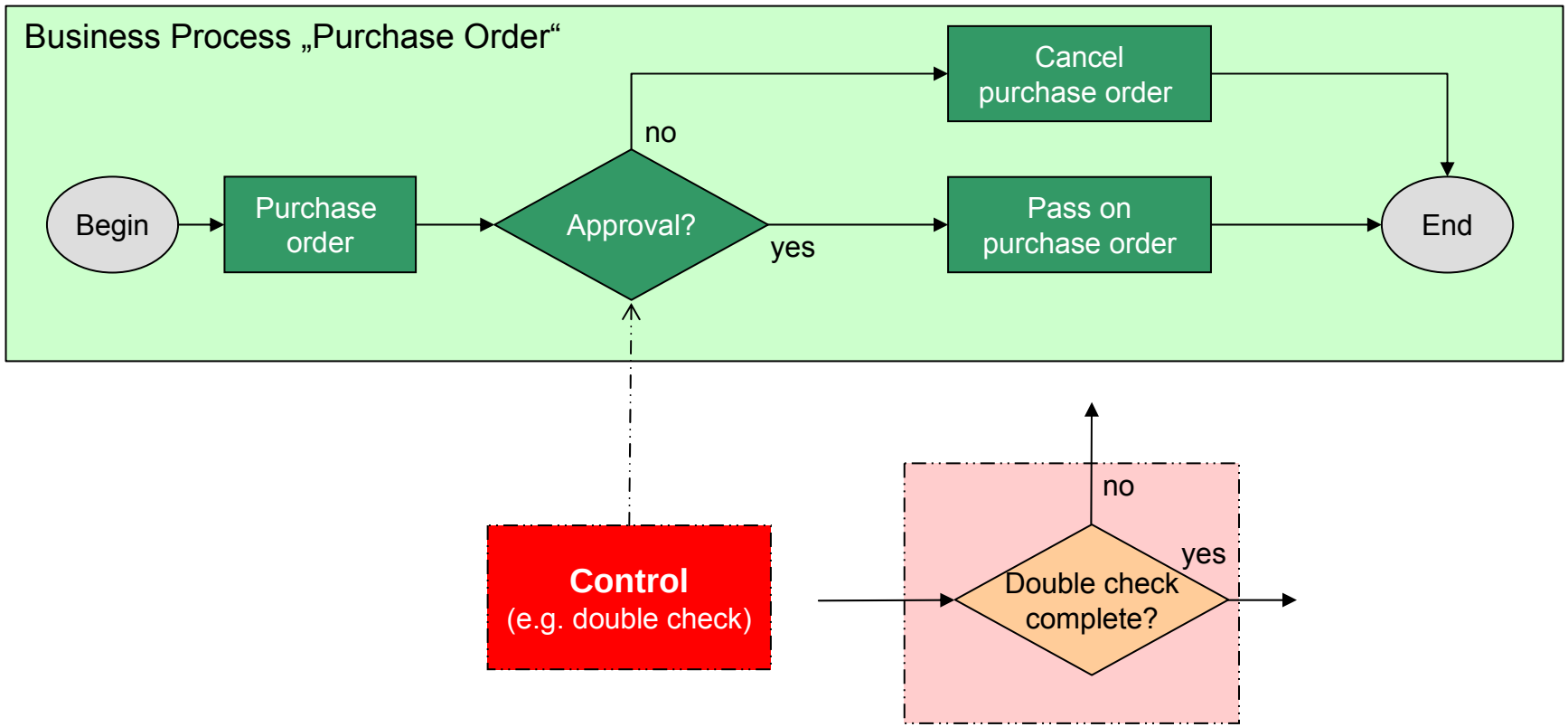
Freiburger Automatisierungsansatz für Compliance

- Trennung Geschäftsprozess- und Kontrollmodelle
- Regelbasierter Ansatz
- Integration Risikomanagement

Trennung Geschäftsprozess- und Kontrollmodelle

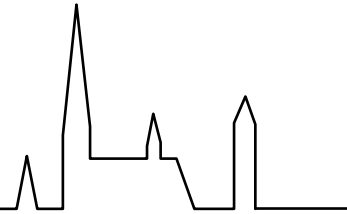


Trennung Geschäftsprozess- und Kontrollmodelle



- zentraler Ansatz und Wiederverwendung von Kontrollen
- Zielkonflikte sind nicht „by design“ zu lösen.
- Erhaltung der Flexibilität von Geschäftsprozessen

Regelbasierter Ansatz

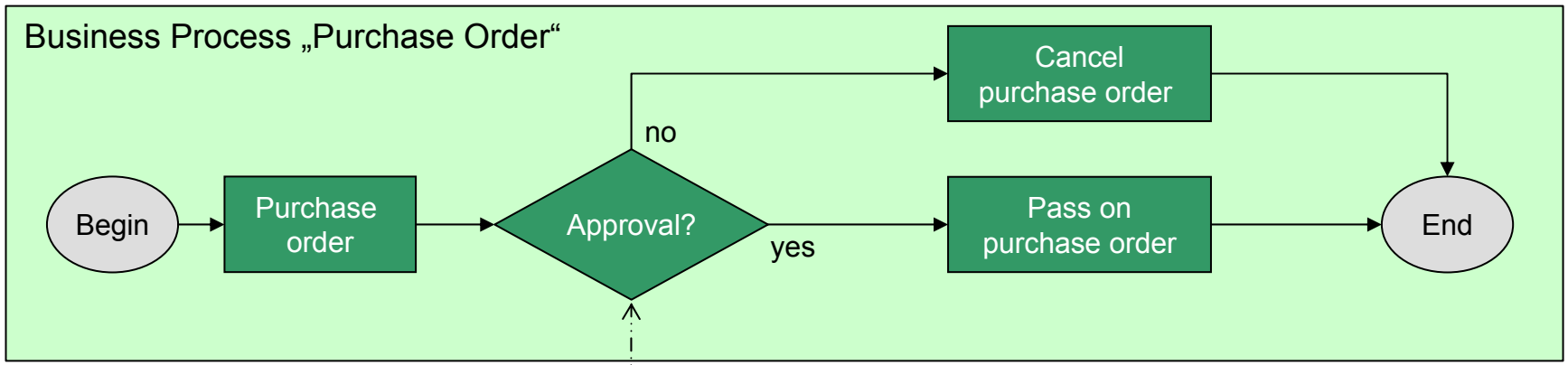


- Compliance- und Geschäftsregeln: gleiches Prinzip

- „Policies“ als Schnittstelle zwischen Gesetz und IT-System
  - Übersetzung von Kontrollzielen in formale Policy-Regeln
  - Eigenschaften der Policy-Sprache bestimmen Automatisierbarkeit

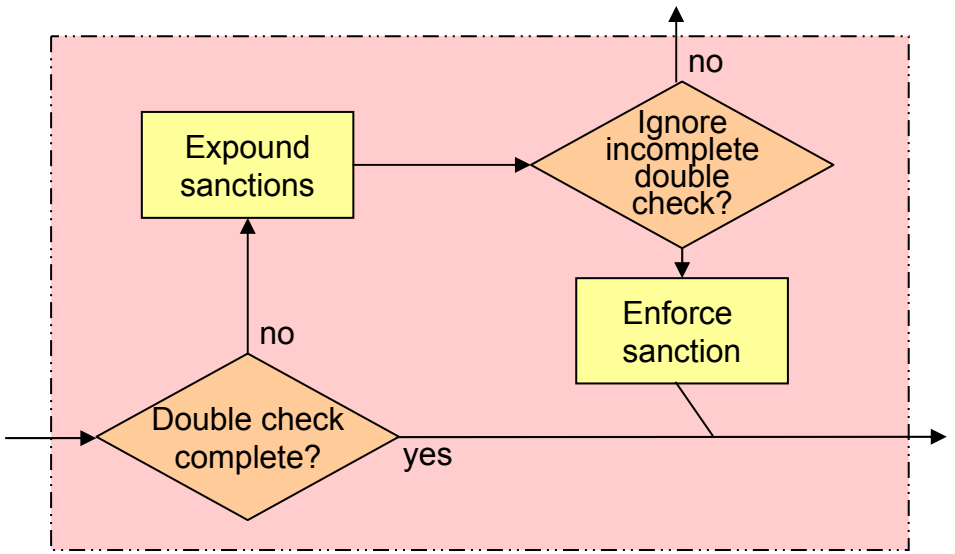
- Aufgabe der IT:
  - Gewährleistung der Regeldurchsetzung
    - „Provisions“: Zugriffskontrolle
  - Erkennung von Regelverletzungen
    - „Obligations“: Nutzungskontrolle
    - Durchführung von Reaktionen/ Erzeugung von Evidenzen

Regelbasierter Ansatz

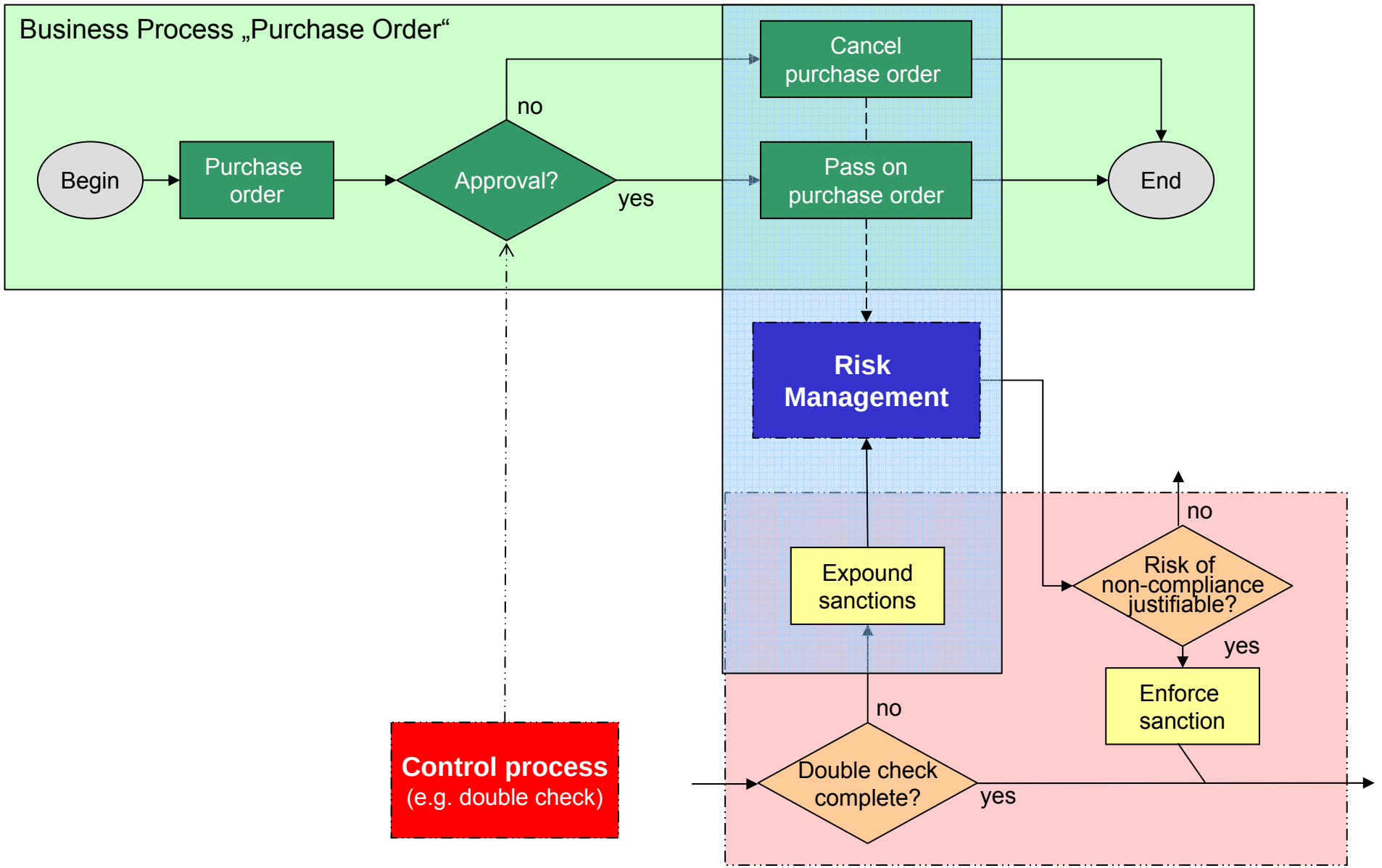


Beispielregel in ExPDT:
(E1, PassOn, Order, forPurchase),
not(checkedBy(E1,E2) ∧ (E1≠E2)),
(⊥, notify)

Control process
(e.g. double check)



Integration Risikomanagement



Fazit

1. Compliance und Risikomanagement ist ein zentrales Thema an der Schnittstelle Wirtschaft und Technik.

2. Automatisierung von Compliance und flexible Geschäftsprozesse können eine gemeinsame Basis haben.
   - Automatisierte Geschäftsprozesse erfordern automatisierte Compliance
   - Chance liegt in regelbasiertem Prozessmanagement
   - IT muss gewährleisten, dass…
     - „by design“: Verbote eingehalten werden,
     - „by detection“: Regelverstöße entdeckt und sanktionierbar werden.

3. Integriertes Risikomanagement bietet eine Entscheidungsbasis für die Lösung von Zielkonflikten.