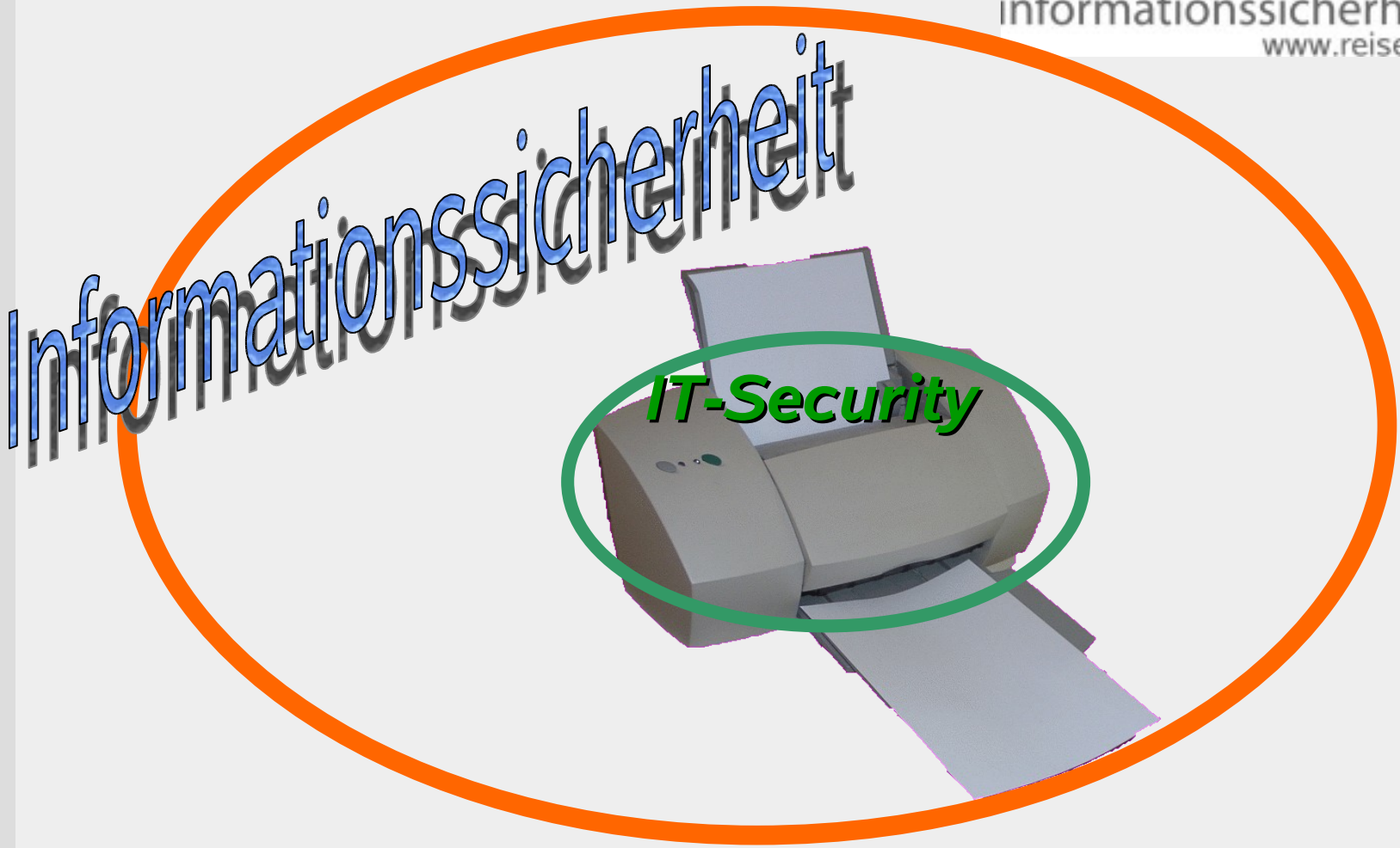
reiser informationssicherheit
www.reiser.at



Standards: Geißel oder Chance - am Beispiel Informationssicherheit

Typischer Status IT

- Technisch gut (nach bestem Wissen und Gewissen)
- Dokumentation schwach bis nicht vorhanden
- Single Head of failure
- “Betriebshandbücher” in Form von Schummelzettel
- Gelebte, nicht dokumentierte Prozesse
- Keine Nachvollziehbarkeit und keine Kontrolle

Typischer Status Unternehmen

- Prozesse höchstens bei Finanz und Controlling
- fast keine Rollenbeschreibungen und nur formale Job-Descriptions
- Geheimhaltung nur DSG auf Papier
- Sicherheit ist physische Sicherheit
- Keine Vorgaben an IT
- Keine Vertraulichkeitsklassen bei Information

Typische Vorfälle

- Passwort unter Mouse-Pad
- Mehrere Personen einen user
- Mehr SW-Installationen als Lizenzen
- Kein Überblick, welche SW installiert ist weil jeder selbst installiert
- Spam et. al. wird selbst weitergeschickt
- Sensible Infos bei Drucker
- Sensible Infos ungesichert auf Laptop (der verschwindet)

Typische Vorfälle ff

- Sensible Infos auf unbesetzten Schreibtischen mit nicht gesperrten Screen
- Jeder (auch fremde) kann in alle Büros
- Notausgänge werden offen gehalten
- Sensible Diskussionen und Telefonate in Öffentlichkeit
- Bereitwillige Auskunft an jedermann, ohne irgendeine Kontrolle
- ...

Viele Baustellen

- Allgemeine Firmenkultur / Bewusstsein
- Was ist zu schützen, und wie sehr
- Physische Sicherheit
- Firmenweite Prozesse
- IT organisatorisch
- ...

ISO 27001[(1)] als Beispiel

- Es gibt auch andere Standards
  - EuroSOX, SOX
  - Basel II
  - Cobit
  - ITIL
  - gesunder Menschenverstand

[(1)] steht hier für BS7799, ISO17799, ÖNorm A 7799, ISO27001, ISO27002, ...

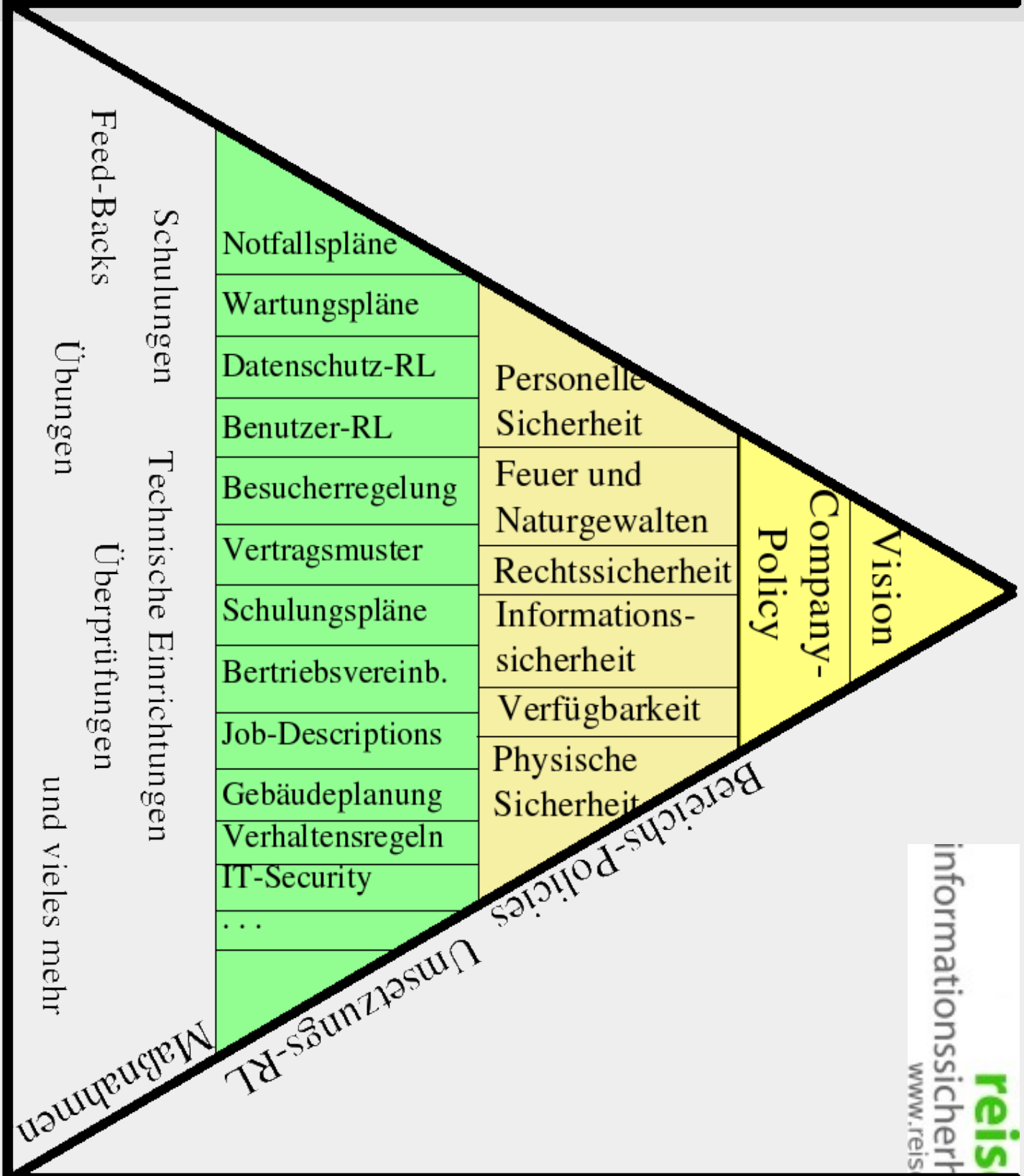
Themen von ISO17799

- Sicherheitspolitik
- Organisation der Sicherheit
- Klassifizierung und Kontrolle der Vermögenswerte
- Personelle Sicherheit
- Physische und umgebungsbezogene Sicherheit

Themen von ISO17799

- Management der Kommunikation und des Betriebs
- Zugriffskontrollen
- Systementwicklung und –wartung
- Betriebliches Kontinuitätsmanagement
- Einhaltung der Verpflichtungen
- Incident Management

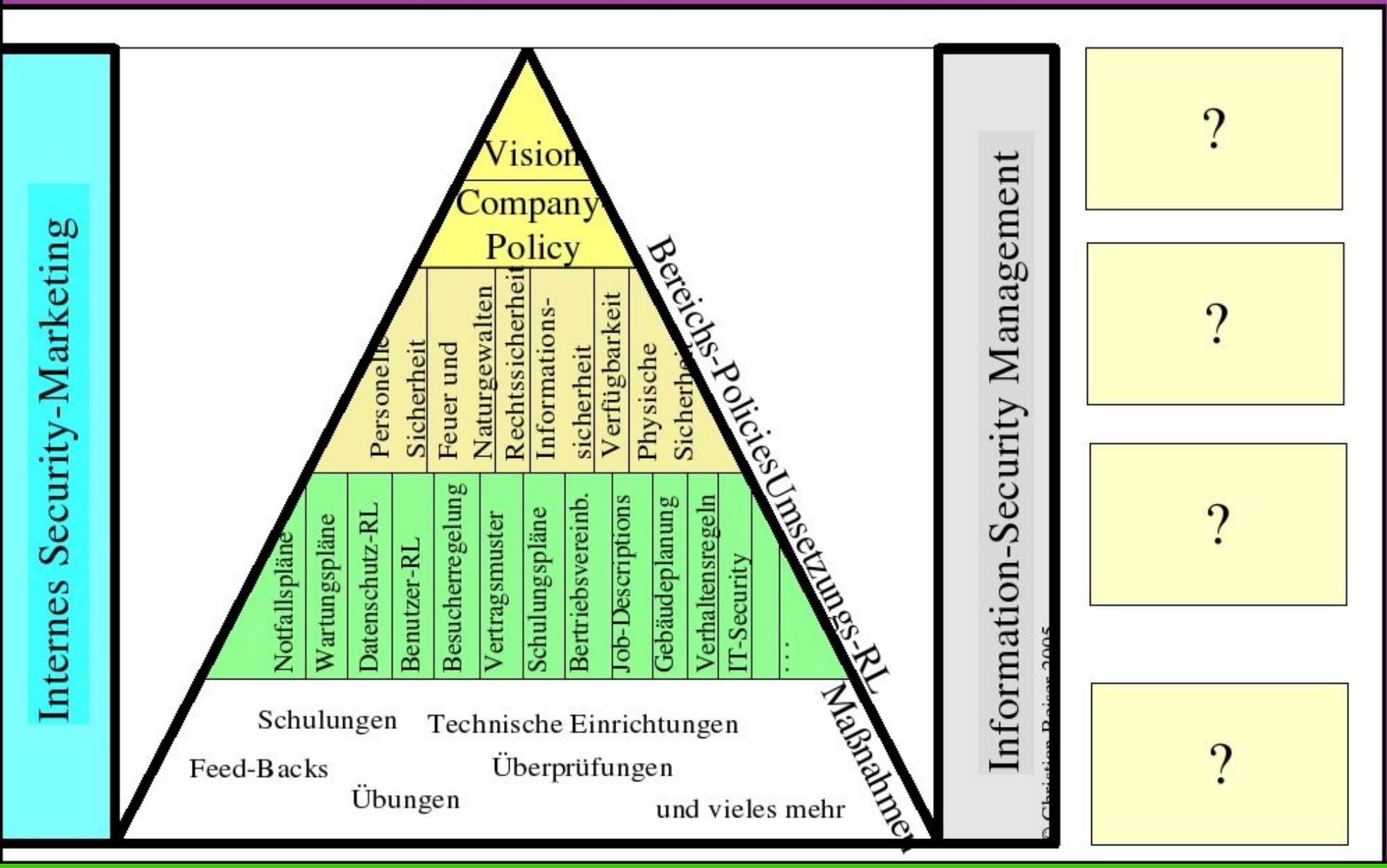
Internes Security-Marketing



Information-Security Management

EuroSOX

COBIT / ITIL / ISO27001



1. Schritt Bestandsaufnahme

reiser informationssicherheit
www.reiser.at

- Welche Dokumente gibt es?
- Welche Prozesse gibt es?
  - gelebt
  - dokumentiert
  - kontrolliert
- Wer arbeitet mit?

- Basis für Projektplan

Mögliche Teilprojekte

- Dokumentation und Dokumente
- Block Erhebungen
  - Informations-Inventarisierung
  - Klassifikation nach Vertraulichkeit und Verfügbarkeit
  - Erhebung der Gefahren und deren Wahrscheinlichkeit
  - Erfassung der zugehörigen Prozesse

Mögliche Teilprojekte ff

- Block Prozesse und Richtlinien für die IT
  - Anforderungen an Computersysteme
  - Erlaubte Datenübertragungen (insbesondere nach außen)
  - Prozesse innerhalb der IT
  - Softwarequalität
- Mitarbeiter-Lifecycle

Mögliche Teilprojekte ff

- Richtlinien für alle Mitarbeiter
  - Benutzerrichtlinie
  - Besucherrichtlinie
  - Geheimhaltungsrichtlinie
- Block Fremdfirmen
  - Outsourcing
  - „Befreundete“ Firmen
- Physische Sicherheit

Mögliche Teilprojekte ff

- ISMS
- Management von IS-Risiken
- Rechtliche Aspekte
- Notfall- und Krisenplanung
  - mit allem, was zu diesem Thema gehört

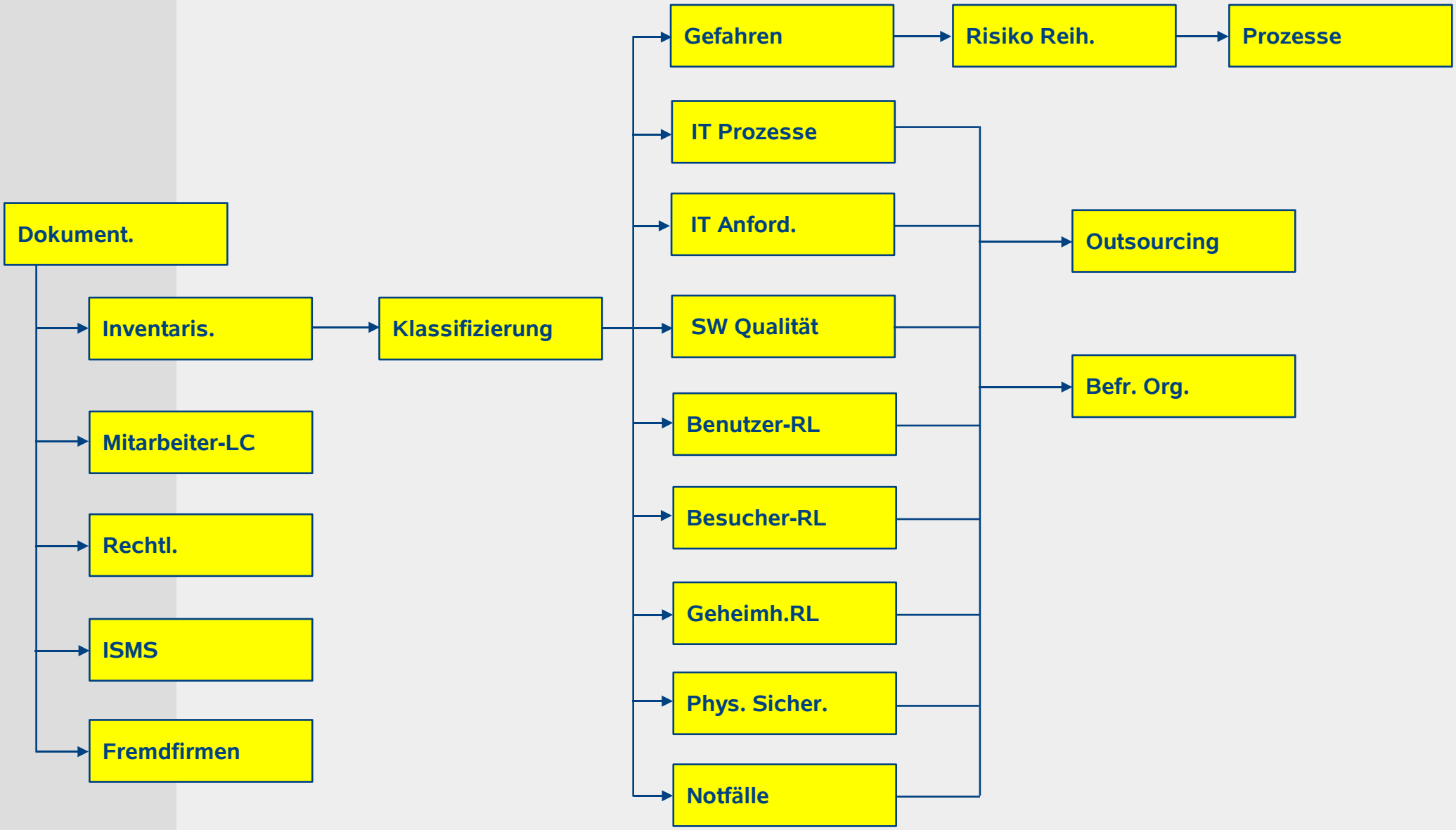
Begleitende Aufgaben

- Projektmarketing und Schulungen
- Einbindung des Betriebsrats
- Konsistenz-Prüfungen
- Self-Assessment
- Pre-Audit
- Zertifizierung
- Projektmanagement

ISMS

- Damit es danach weiter lebt
- Rollen / Gremien definieren
- Risiko-Board
- Laufende Kontrolle / Messen
  - Werden die Vorgaben eingehalten?
  - Wirken die Vorgaben?
  - Müssen die Vorgaben angepasst werden?
- Die Rolle des Kerberos

Abhängigkeiten



Mögliche Vorgangsweisen

- Trotz Abhängigkeiten kann viel parallel durchgeführt werden
- Vorbereitung -> WS -> Protokoll -> Review -> Fertiges Dokument -> Implementation
- Coaching von Mitarbeitern, die ihren Teil selbst machen
- ...
- Wie auch immer, die Betroffenen müssen beteiligt sein.

Aufwand

- Sehr unterschiedlich
- Abhängig von Ausgangssituation, Ziel und Komplexität
- Durchlaufzeit 8 bis 24 Monate
- Von 150 PT aufwärts, bei sinnvoller Implementierung

Auswahl des Beraters

- Kann er mit den Menschen und der Kultur Ihres Unternehmens umgehen?
- Passt er sich an Ihr Unternehmen an? Nicht umgekehrt!!!
- Nachhaltigkeit durch möglichst geringe Änderungen in Abläufen und Kultur
- Erfahrung in Informations-Sicherheit
- Kompatibel zu unterschiedlichen Personengruppen

Ziel

Wir heben die Informations-Sicherheit und bekommen so nebenbei dafür auch ein Zertifikat!

Danke für Ihre Aufmerksamkeit

Dr. Christian Reiser
Experte für Informationssicherheit
Christian@Reiser.at
www.Reiser.at

Tel: +43 664 2148540
+43 780 Reiser
Fax: +43 2262 64460