



# ID Management, Security Management, Enterprise Risk Management

ISSS Luzerner Tagung 2008

Frank Heinzmann, Zurich Financial Services

# Agenda

- Wie kann man den Nutzen existierender ID Management Lösungen auf den Gesamtkontext des Risikomanagements übertragen?
- Wie kann man die Berichterstattung vereinheitlichen und konsolidieren?
- Wer macht dies bereits heute und wie?
- Was wird vom Revisor eigentlich geprüft und als konform abgesehnet? Security? Risk Management?
- Welche “Evidence” muss vorgewiesen werden?

# Wie kann man den Nutzen existierender ID Management Lösungen auf den Gesamtkontext des Risikomanagements übertragen?

## Ein Beispiel....

- Stellen Sie sich einen Autoreifen vor
- Dieser Reifen hat praktisch kein Profil mehr
- Welche Risiken und Konsequenzen kommen Ihnen in den Sinn?
- Wie sieht die Situation jetzt aus?



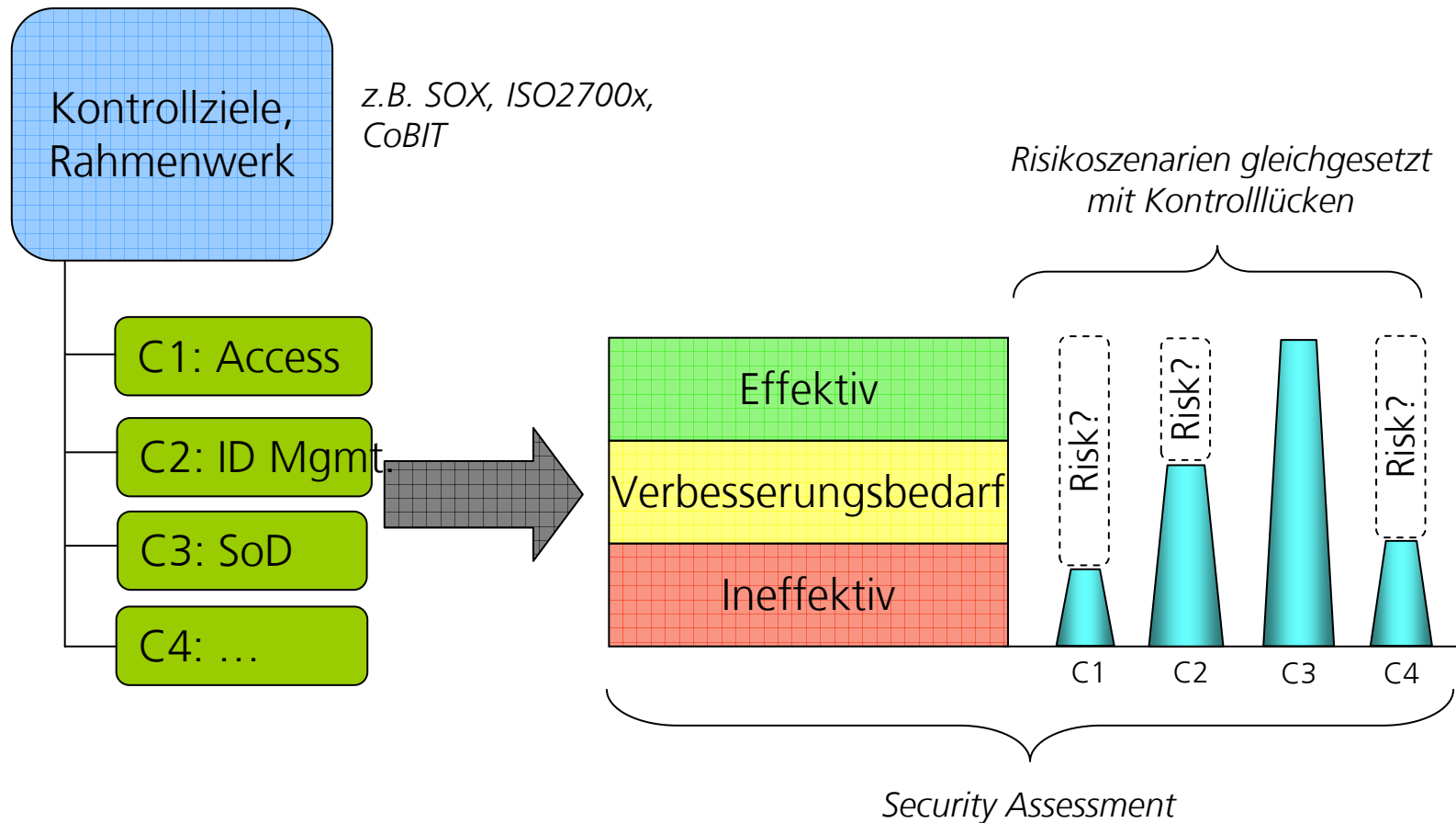
**Wenn wir von (Security) Risiko Management reden, müssen wir sicherstellen, dass wir uns im gegebenen Gesamtkontext bewegen und keine falschen Annahmen treffen!**

# Risk Management – Kunst oder Wissenschaft?

- Fragt man 10 Physiker um eine Definition von Masse, Beschleunigung oder Geschwindigkeit, erhält man 10 mal die gleiche Antwort
- Fragt man 10 Banker um eine Definition von Soll und Haben, wird man ebenfalls 10 sehr ähnliche Antworten erhalten
- Fragt man 10 Risikomanager um eine Definition von Risiko, Auslöser oder Konsequenz, wird man 10 sehr unterschiedliche Interpretationen erhalten!

**Risiko Management wird immer subjektiv sein und bleiben. Dies ist insbesondere bei der Übersetzung von ID Management Risiken in Unternehmensrisiken der Fall.**

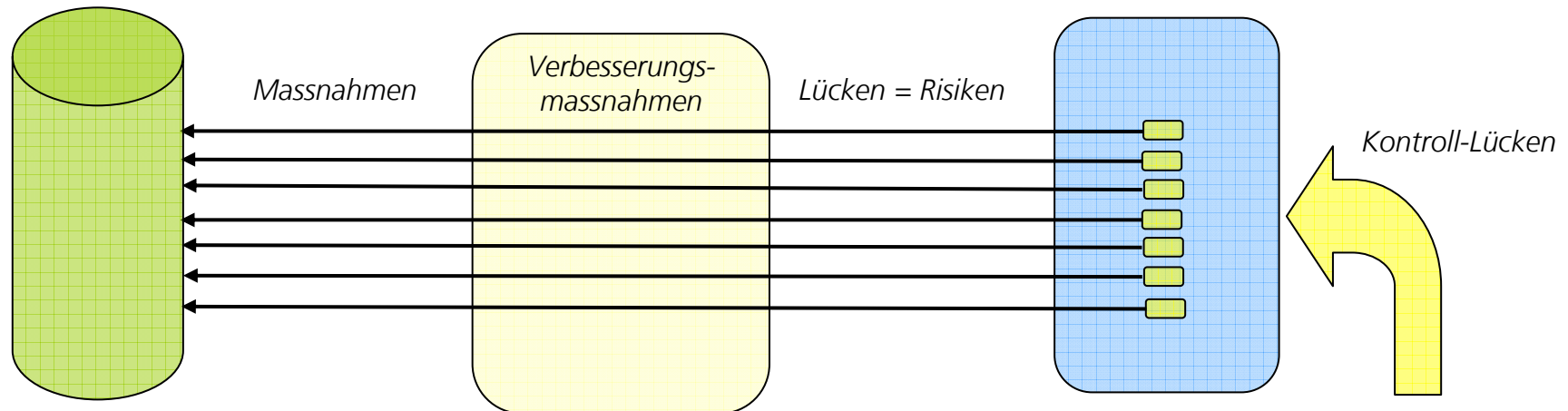
# Securitymanagement vs. Risikomanagement



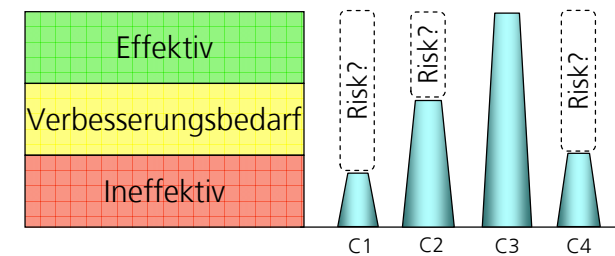
**Wieviele Risiken haben wir jetzt hier? Vier? Zwei? Gar Keine?**

# Regelfall: Kontroll-Lücke = Risiko

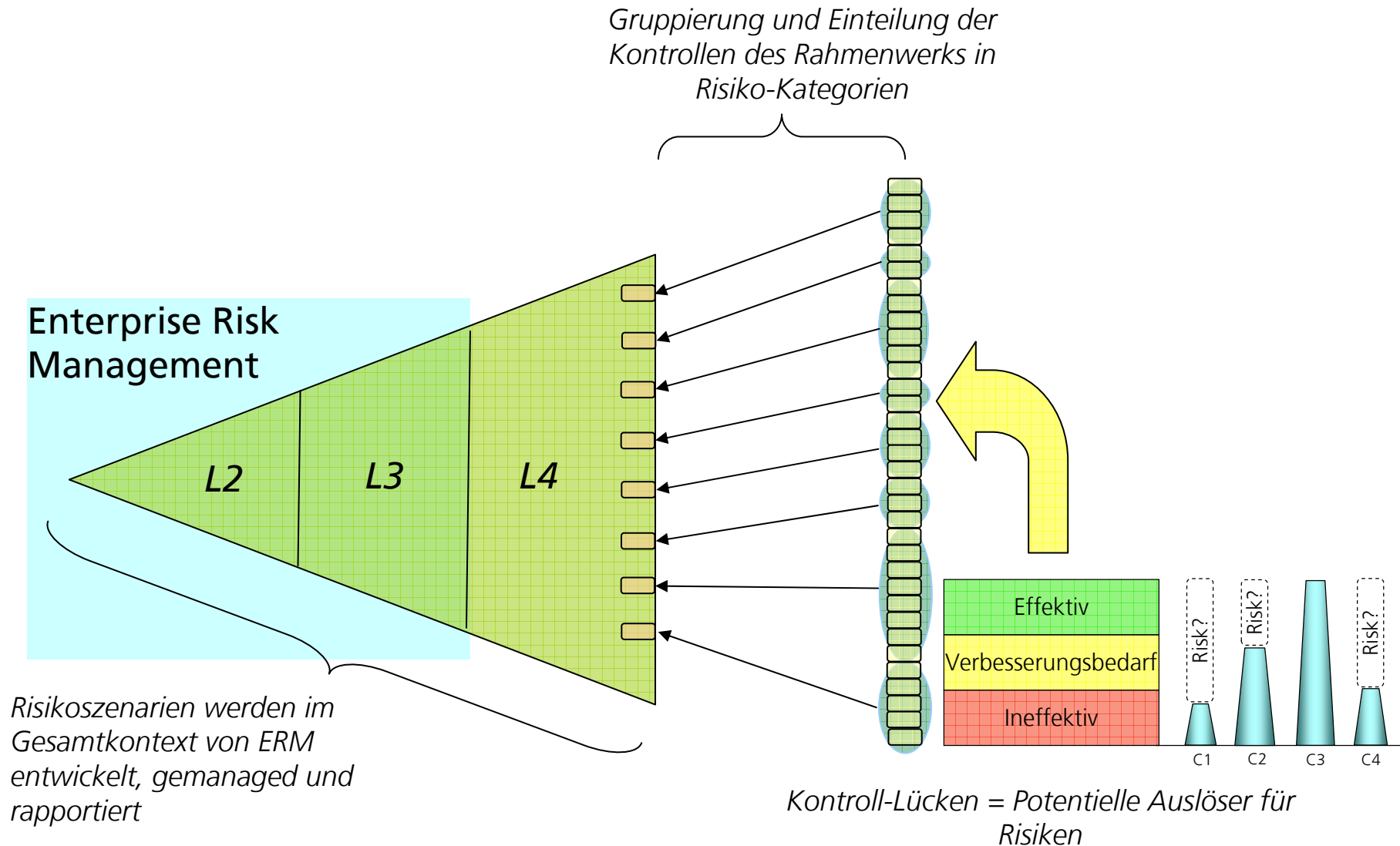
Risiko Register und  
Berichterstattung



- Risikobeurteilung erfolgt einzig aufgrund Vorhandensein oder Nicht-Vorhandensein von Kontrollen (in ERP Systemen)
- Konsolidierung und Aggregation von Risiken auf Unternehmensstufe nicht möglich
- Zu viele zu technische „Risiken“ für ein effektives Management und Reporting

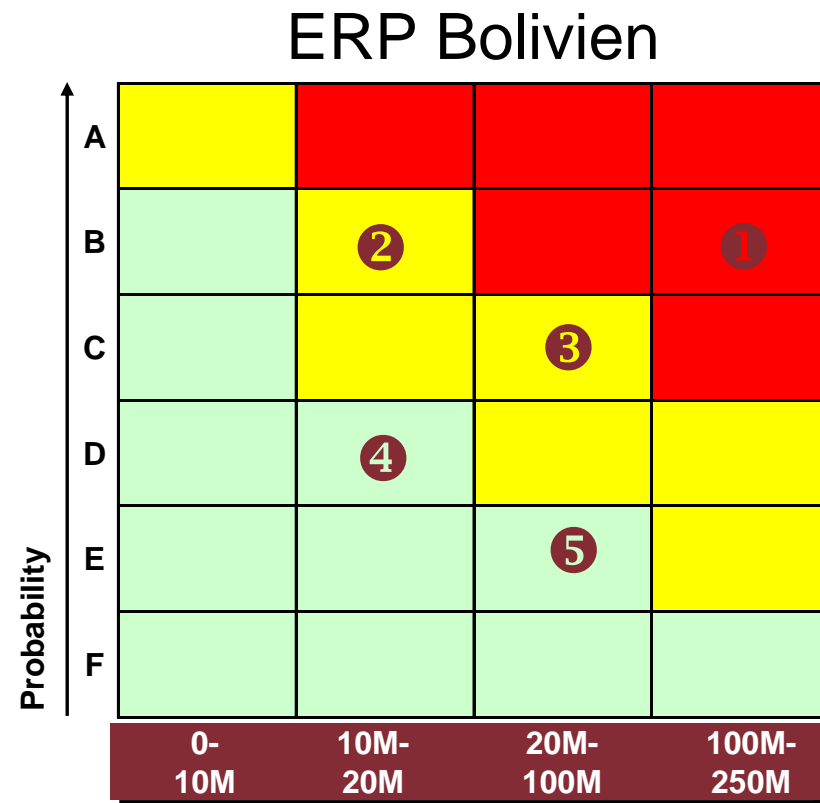
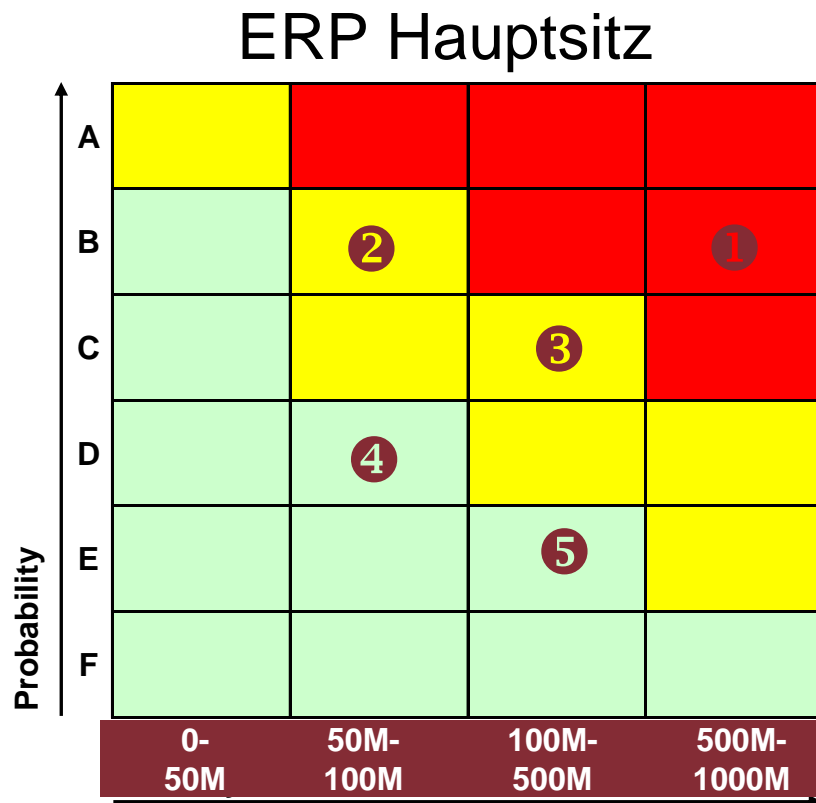


# Idealfall: Aggregation von Lücken zu Risiken



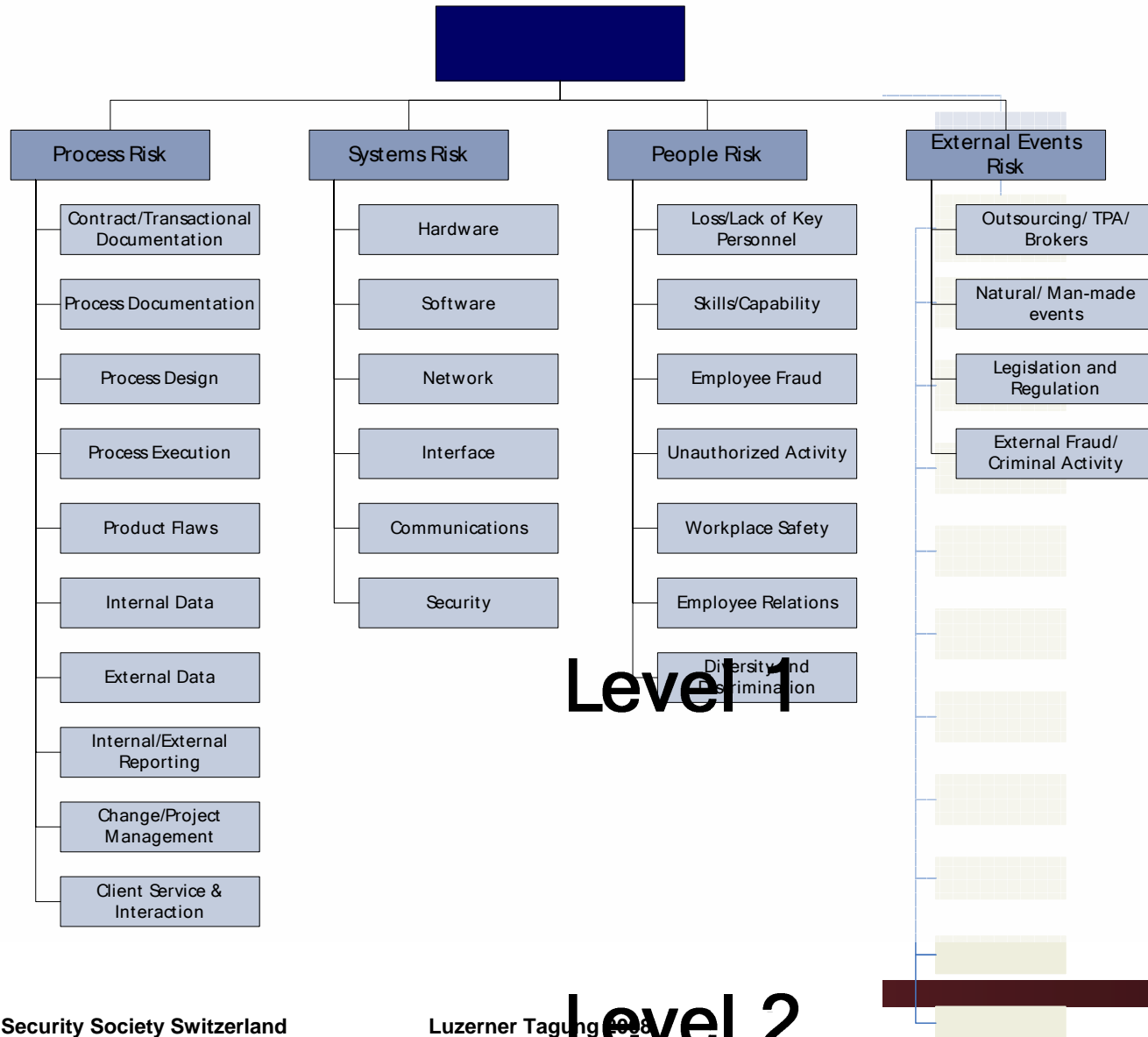
# Wie kann man die Berichterstattung vereinheitlichen und konsolidieren?

# 1. Quantitatives Risikomanagement



**Qualitativ gleichwertig – Aber quantitativ gleich signifikant?**

# 2. Risikokategorien und -hierarchien



# Wer macht dies bereits heute und wie?

## Diskussionsrunde

**Was wird vom Revisor eigentlich geprüft  
und als konform abgeseignet? ID  
Management? Security? Risk  
Management?**

**Welche “Evidence” muss vorgewiesen  
werden?**

# Wann ist ein ERP System „revisionskonform“?

- Wenn es ein ID Management gibt?
- Wenn es ein Security-Rahmenwerk gibt?
- Wenn es ein Kontroll-Rahmenwerk gibt?
- Wenn der Revisor genügend „Beweise“ oder Anhaltspunkte hat, dass die existierenden Kontrollen funktionieren?
- Wenn alle Punkte auf der Checkliste des Revisors abgehakt wurden?
- Wenn das potentielle Risiko im Gesamtkontext des Unternehmens akzeptabel ist? Was ist denn akzeptabel?

# Welche „Evidence“ muss vorgewiesen werden?

- Ein Kontroll-Rahmenwerk?
- Ein Tool zur Umsetzung des Rahmenwerks?
- Die vollständige Implementierung aller Kontrollen?
- Die risiko-basierte Implementierung aller Kontrollen?
- Logfiles und Systemzugriffe?
- Effektivitätstests aller Kontrollen?
- Trainings und Awareness-Kampagnen?
- ...

# Ihre Meinungen und Erfahrungen?

## Diskussionsrunde