

Das neue Framework der ISACA: RiskIT

Werte schaffen und Risiken managen

Alfred Heiter

25. Februar 2010

Vorstellung – Alfred Heiter



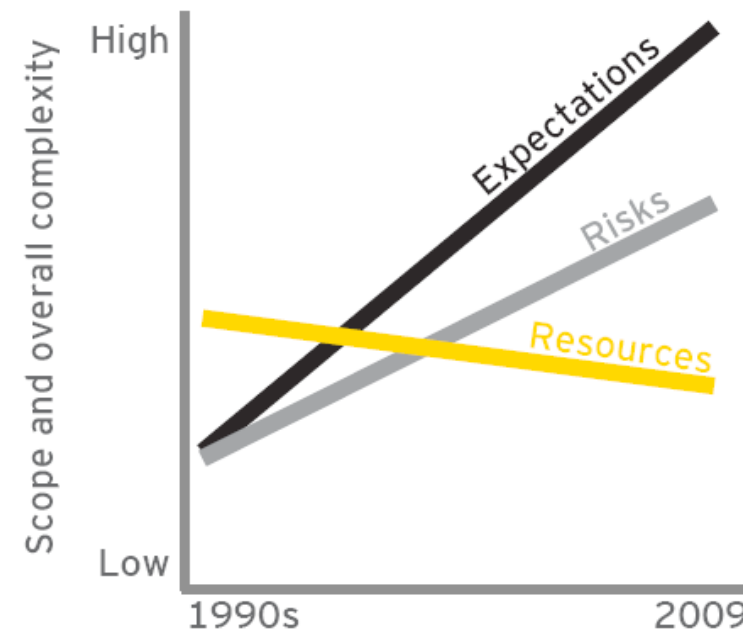
alfred.heiter@at.ey.com

- ▶ Seit 10 Jahren im IT-Prüfungs- und IT-Beratungsgeschäft
- ▶ Senior Manager bei Ernst & Young im Bereich Technology & Security Risks Services
- ▶ Schwerpunkte:
 - ▶ IT Governance, Risk and Compliance
 - ▶ IT Prüfung
 - ▶ IT Security
- ▶ Wirtschaftsprüfer, Steuerberater
- ▶ Certified Information Systems Auditor (CISA)
- ▶ Certified Information Systems Security Professional (CISSP)
- ▶ GIAC Certified Windows Security Administrator (GCWN)
- ▶ Certified in the Governance of Enterprise IT (CGEIT)
- ▶ Mitglied ISACA Austria
- ▶ Mitglied des Fachsenats für Datenverarbeitung der Kammer der Wirtschaftstrehänder

Die Rolle der IT – Trends

- ▶ Zunehmende Risiken
- ▶ Zunehmende Erwartungen

- ▶ bei gleichbleibenden oder abnehmenden Ressourcen (personell und finanziell)



Kernziele der IT

- ▶ Create Value
 - ▶ Wie kann IT dazu beitragen, den Wert des Unternehmens (z.B. Umsatz, Gewinn, Wettbewerbsfähigkeit) zu steigern?

- ▶ Rationalize Costs
 - ▶ Wie kann IT zur Kostensenkung im Unternehmen beitragen?

- ▶ Manage Risks
 - ▶ Wie kann IT dazu beitragen, die Risiken (IT und nicht-IT) im Unternehmen in den Griff zu bekommen?

Risk IT – im Kontext des ISACA Produkt Portfolios

COBIT

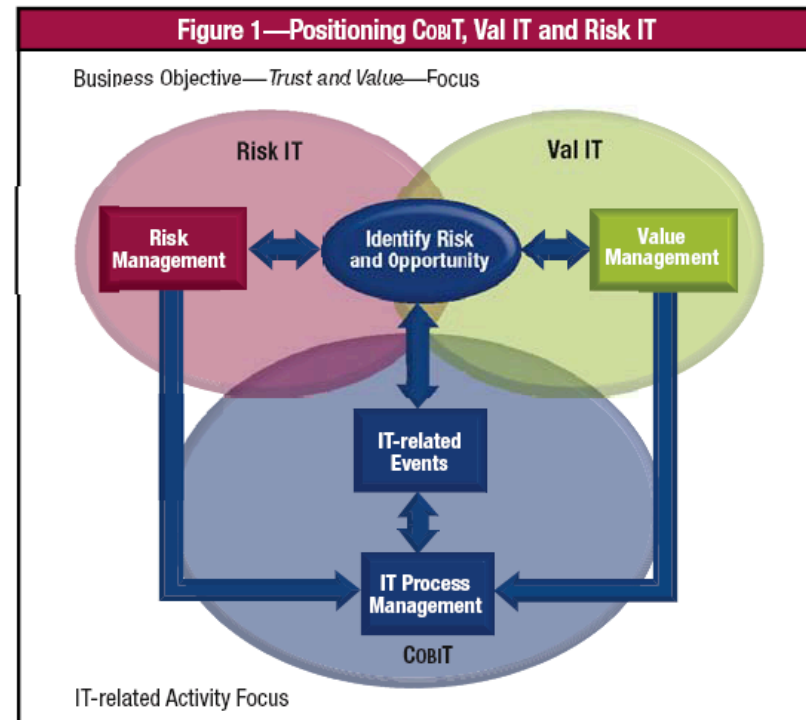
- ▶ Management aller IT-bezogenen Aktivitäten in einem Unternehmen

Val IT

- ▶ Chancen Management

Risk IT

- ▶ IT Risikomanagement



Warum Risk IT?

Andere (IT) Risikomanagement Standards

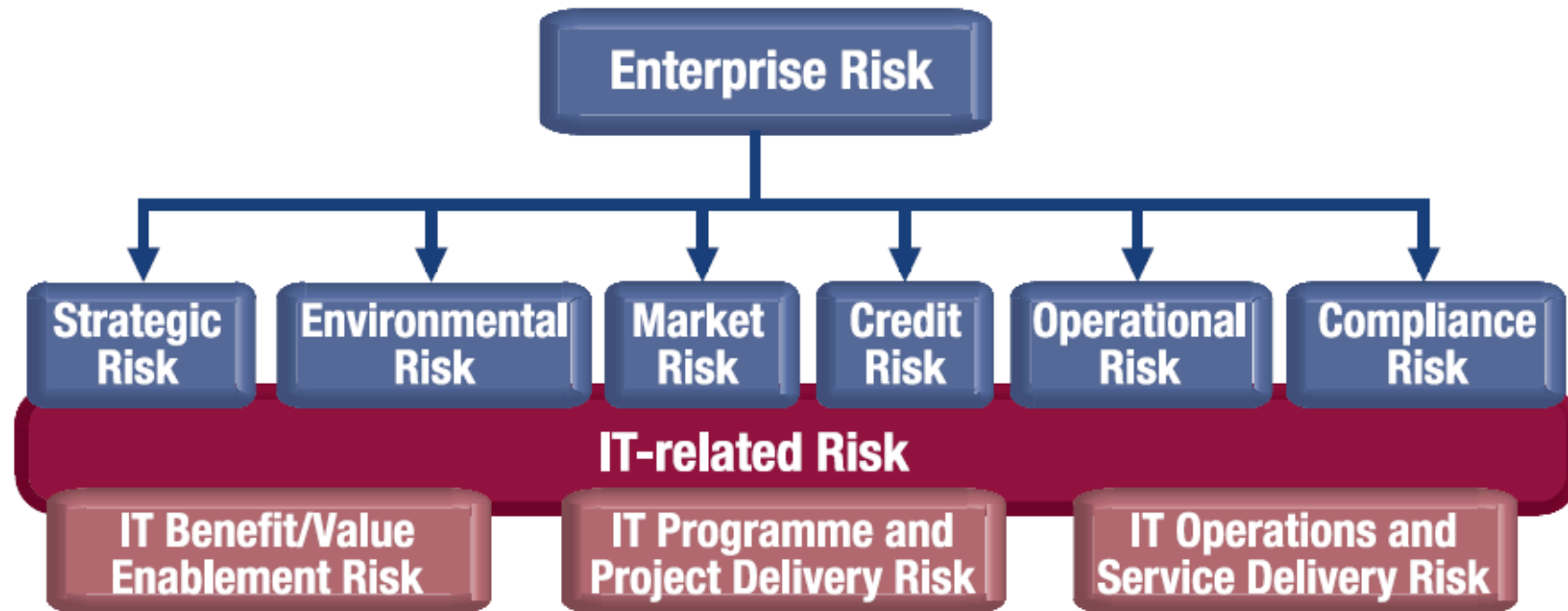
- ▶ COSO ERM
- ▶ AS/NZS 4360; ISO 31000
- ▶ ISO 27005 (ISO 2700x)
- ▶ ONR 45000

Risk IT

- ▶ Berücksichtigt und integriert bereits vorhandene Standards
- ▶ Umfasst sämtliche Aspekte des IT Risikos (nicht nur z.B. IT Security)
- ▶ Lässt sich leicht mit COBIT verbinden (Schnittstellen etc. sind definiert)

Definition von IT Risiko in Risk IT

„IT Risiko ist das geschäftliche Risiko, das mit der Nutzung, dem Besitz, dem Betrieb, der Mitwirkung, dem Einfluß und der Anpassung von IT im Unternehmen verbunden ist.“



Risikokategorien in Risk IT

Drei Risikokategorien

- ▶ IT Nutzen- und Wertbeitragsrisiko
 - ▶ (versäumte) Chancen, IT zur Effizienz- und Effektivitätssteigerung der Geschäftsprozesse oder als Enabler für neue Geschäftsinitiativen einzusetzen
- ▶ IT Programm- und Projektrisiko
 - ▶ Risiken in Zusammenhang mit neuen oder verbesserten Business Solutions (idR in Form von Projekten und Programmen)
- ▶ IT Betriebs- und Serviceerbringungsrisiko
 - ▶ Risiken in Zusammenhang mit der Performance von IT Systemen und IT Services, die zu einer Zerstörung oder Minderung von Werten des Unternehmens führen können

Ziel und Zweck von Risk IT

Ermöglichung von risikobewussten Entscheidungen durch

- ▶ Integration des IT Risikomanagements in das Enterprise Risk Managements (ERM) einer Organisation
- ▶ gut vorbereitete Entscheidungen über den Umfang von Risiken, Risiko Appetit und Risiko Toleranz
- ▶ Verständnis, wie auf Risiken reagiert werden soll (risk response)

Risk IT stellt dafür zur Verfügung

- ▶ End-to-end Prozess-Framework für IT Risikomanagement
- ▶ Anleitung für Praktiker inklusive Tools und Techniken, um konkrete Risiken der Geschäftstätigkeit zu verstehen und zu managen

Prinzipien von Risk IT

- ▶ Verknüpfung mit Unternehmenszielen
- ▶ Abstimmung der IT-relevanten Geschäftsrisiken mit dem ERM
- ▶ Abwägen von Kosten und Nutzen des Managements von IT Risiken
- ▶ Förderung der angemessenen und offenen Kommunikation von IT Risiken
- ▶ Sicherstellung der richtigen Einstellung der Unternehmensführung („tone from the top“), Definition und Durchsetzung persönlicher Verantwortung und wohldefinierter Toleranzlevel
- ▶ Kontinuierlicher Prozess als Teil des Tagesgeschäfts

Das Risk IT Framework

- ▶ Drei Domänen
- ▶ Neun Prozesse
- ▶ 43 Aktivitäten

- ▶ Prozesselemente
 - ▶ Prozessbeschreibung
 - ▶ Eingangs- und Ausgangswerte (auch zu COBIT und Val IT)
 - ▶ RACI-Tabellen
 - ▶ Metriken



Risk Governance

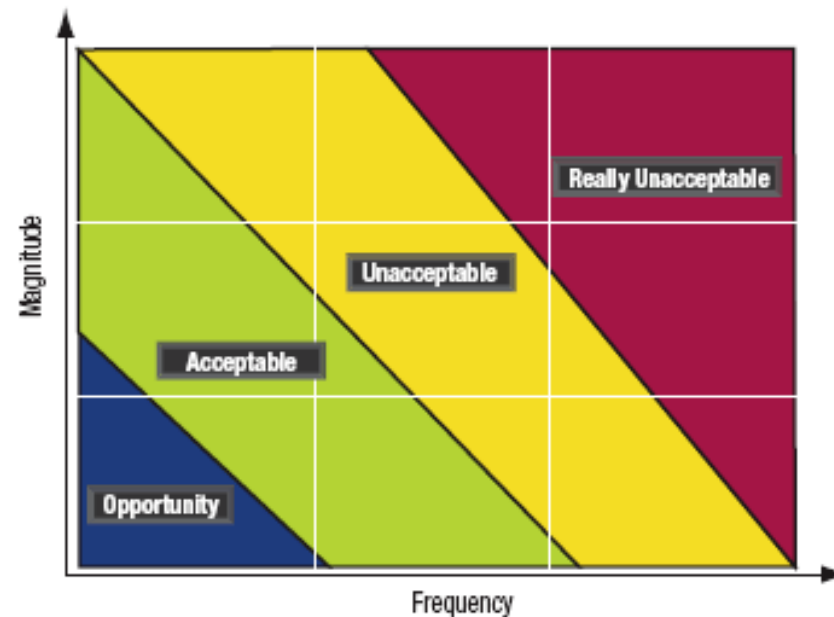
Inhalte

- ▶ Risikoappetit und Risikotoleranz
- ▶ Pflichten und Verantwortlichkeiten im IT Risikomanagement
- ▶ Sensibilisierung und Kommunikation
- ▶ Risikokultur

Risikoappetit und Risikotoleranz

Risikoappetit (Risk Appetite)

- ▶ Höhe des Gesamtrisikos, die eine Organisation bei der Verfolgung ihrer Ziele zu akzeptieren bereit ist



Risikotoleranz

- ▶ Akzeptierte Abweichung bei der Erreichung einzelner Ziele

Sensibilisierung und Kommunikation

Sensibilisierung von Risiken

- ▶ Kenntnis und Management aller Risiken in einer Organisation

Kommunikation

- ▶ Erwartungen an das Risikomanagement
- ▶ Fähigkeiten des Risikomanagements in der Organisation
- ▶ Aktueller Status der IT Risiken
 - ▶ Risikoprofil
 - ▶ Key Risk Indicators (KRIs)
 - ▶ Schadensereignisse und deren Ursache
 - ▶ Möglichkeiten zur Begegnung der Risiken (Kosten und Nutzen)
- ▶ Kommunikation an alle relevanten Stakeholder

Risikokultur

- ▶ Risikoeinstellung
 - ▶ Risikoavers – Übernehmen von Risiken
- ▶ Einhaltung von Richtlinien
 - ▶ Compliance – Non-Compliance
- ▶ Verhalten bei Schadensfällen (oder versäumter Chancen)
 - ▶ Lernkultur – Kultur der Schuldzuweisung

Symptome unangemessener Risikokultur

- ▶ Tatsächlicher Risikoappetit spiegelt sich nicht in den Richtlinien wieder
- ▶ Existenz einer Kultur der Schuldzuweisung

Risiko Evaluierung

Inhalte

- ▶ Beschreibung der Auswirkungen von IT Risiken auf das Geschäft (Business Impact)
- ▶ Risikoszenarien

Business Impact

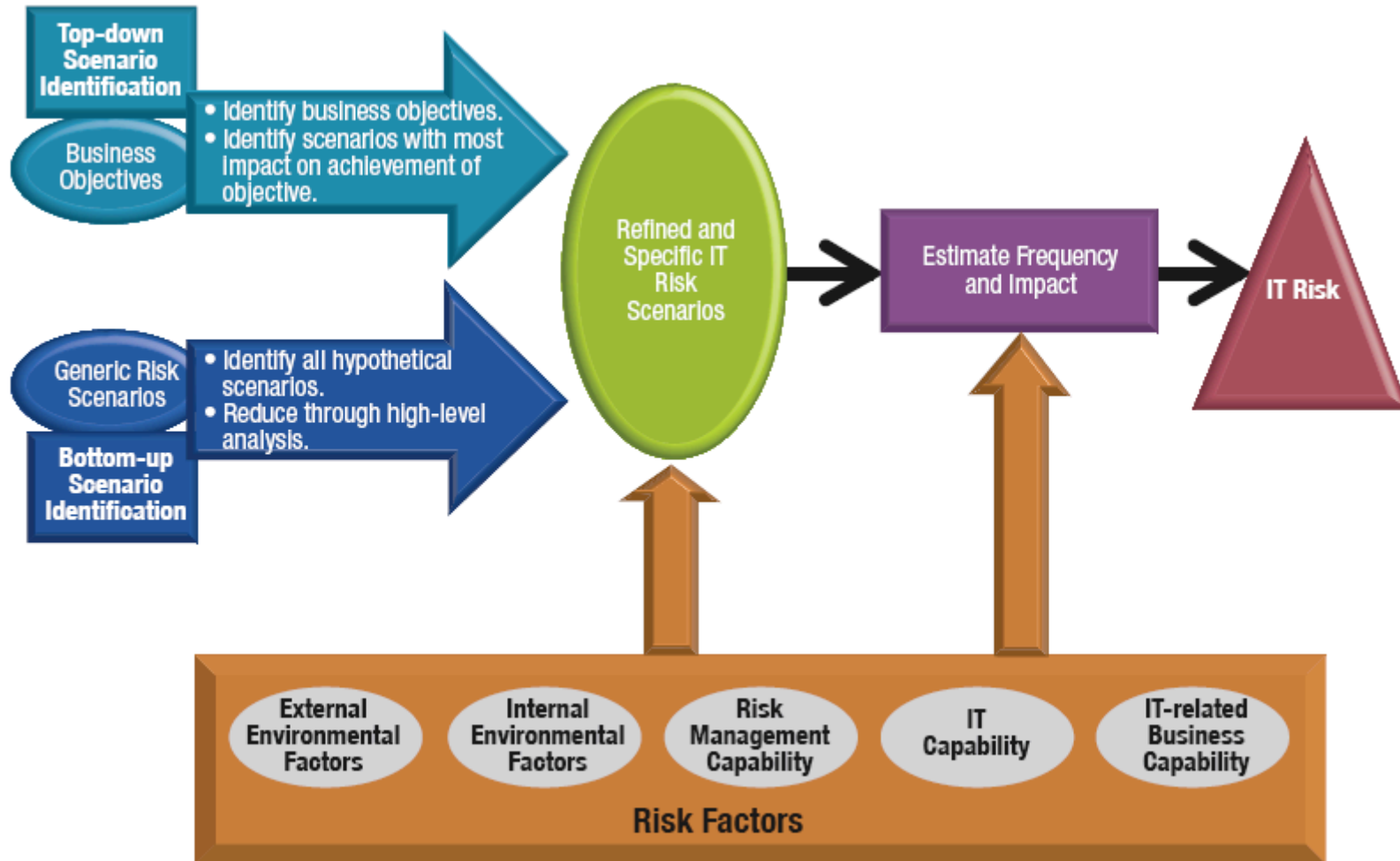
Beschreibung der Auswirkungen von IT Risiken ist erforderlich für eine angemessene Risikobewertung

- ▶ Verständlich für sämtliche Betroffene (IT-Mitarbeiter und Mitarbeiter der Fachabteilungen)
- ▶ Beschreibung, wie Fehler in der IT Geschäftsprozesse beeinträchtigen können

Beschreibung mittels

- ▶ Cobit Information Criteria
- ▶ Balanced Score Card (BSC)
- ▶ Extended BSC
- ▶ Westermann
- ▶ COSO ERM
- ▶ FAIR

Entwicklung von Risikoszenarien



Elemente eines Risiko Szenarios



Risk Response

Inhalte

- ▶ Key Risk Indikatoren (KRIs)
- ▶ Definition und Priorisierung der Risikoreaktion

Key Risk Indikatoren

Messgrößen, die anzeigen, ob ein Risiko den Risikoappetit einer Organisation überschreiten (könnte).

Vorgehen bei der Definition

- ▶ Berücksichtigung aller Betroffenen
- ▶ Performance Indicators, Lead Indicators, Trends
- ▶ Berücksichtigung der Ursache (nicht nur Auswirkungen)

Kriterien zur Auswahl

- ▶ Auswirkung der Risiken
- ▶ Aufwand für Implementierung, Messung und Berichterstattung
- ▶ Verlässlichkeit
- ▶ Sensitivität (Empfindlichkeit)

Definition und Priorisierung der Risikoreaktion

Möglichkeiten der Risikoreaktion

- ▶ Risikovermeidung
- ▶ Risikoreduzierung / -bewältigung
- ▶ Risikoüberwälzung
- ▶ Risikoakzeptanz

Definition der Risikoreaktion

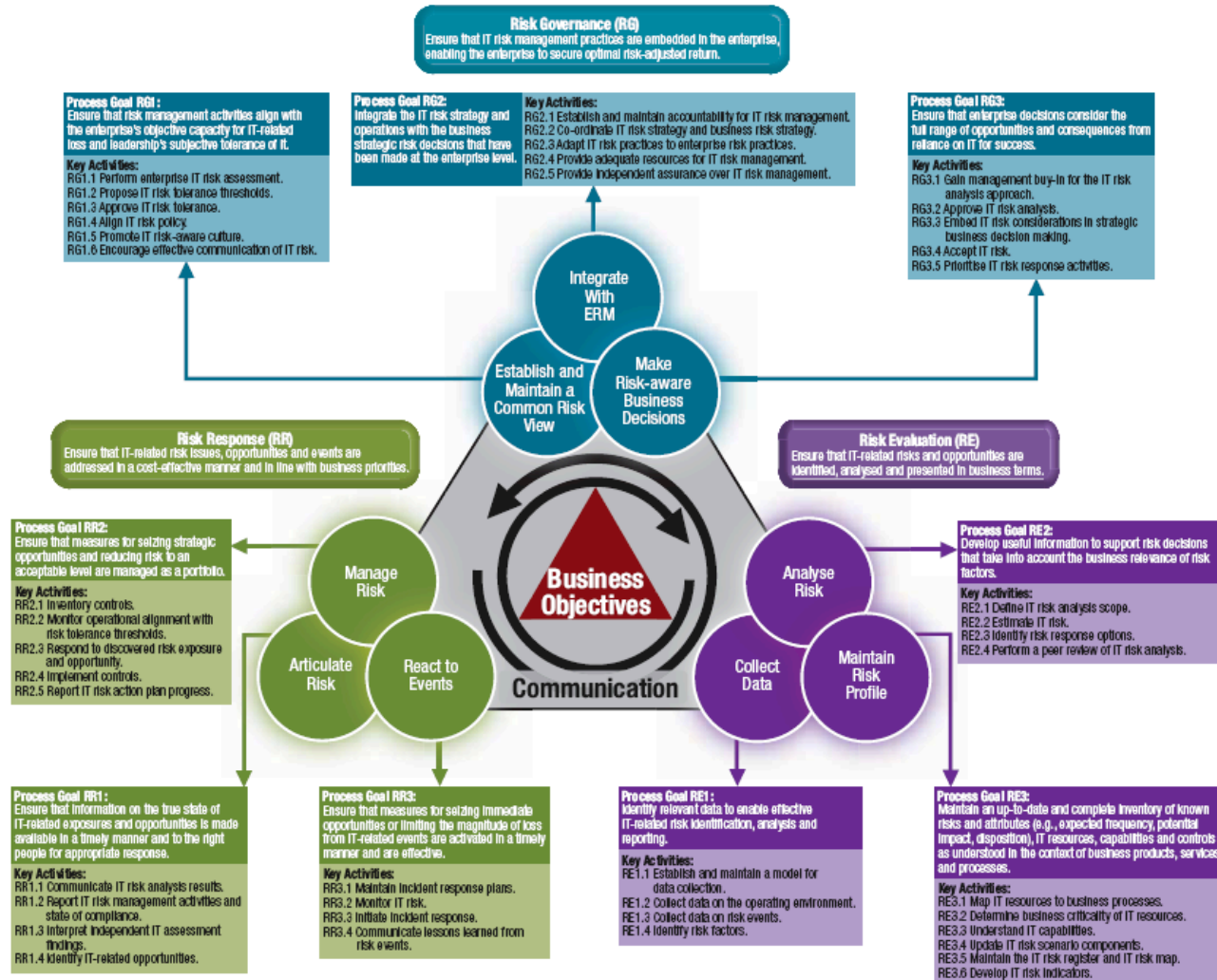
- ▶ Kosten
- ▶ Wesentlichkeit des Risikos
- ▶ Fähigkeit der Organisation, die Maßnahme zu implementieren
- ▶ Effektivität
- ▶ Effizienz

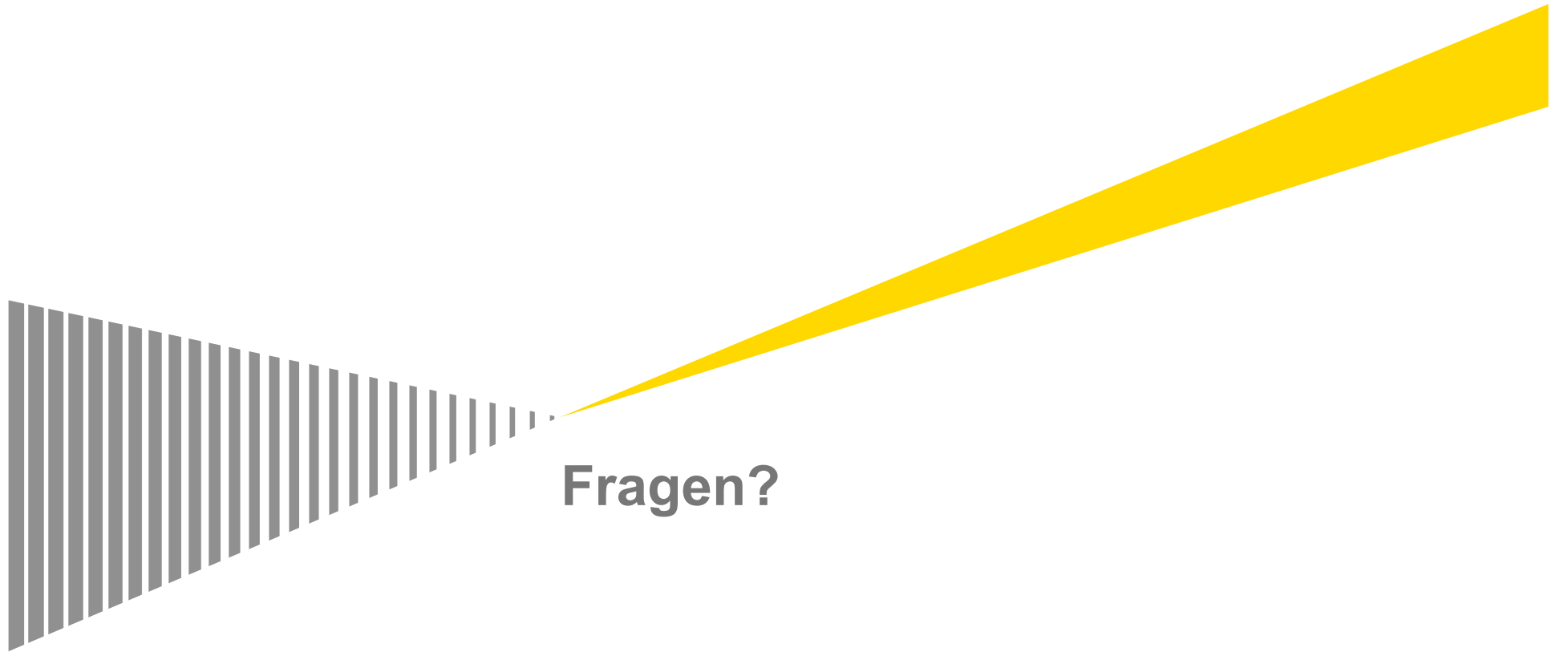
Definition und Priorisierung der Risikoreaktion

Priorisierung der Maßnahmen



Risk IT Framework





Fragen?