IBM Business Consulting Services

Nur eine optimale Abstimmung minimiert die Gefährdung

Markus Pfyffer

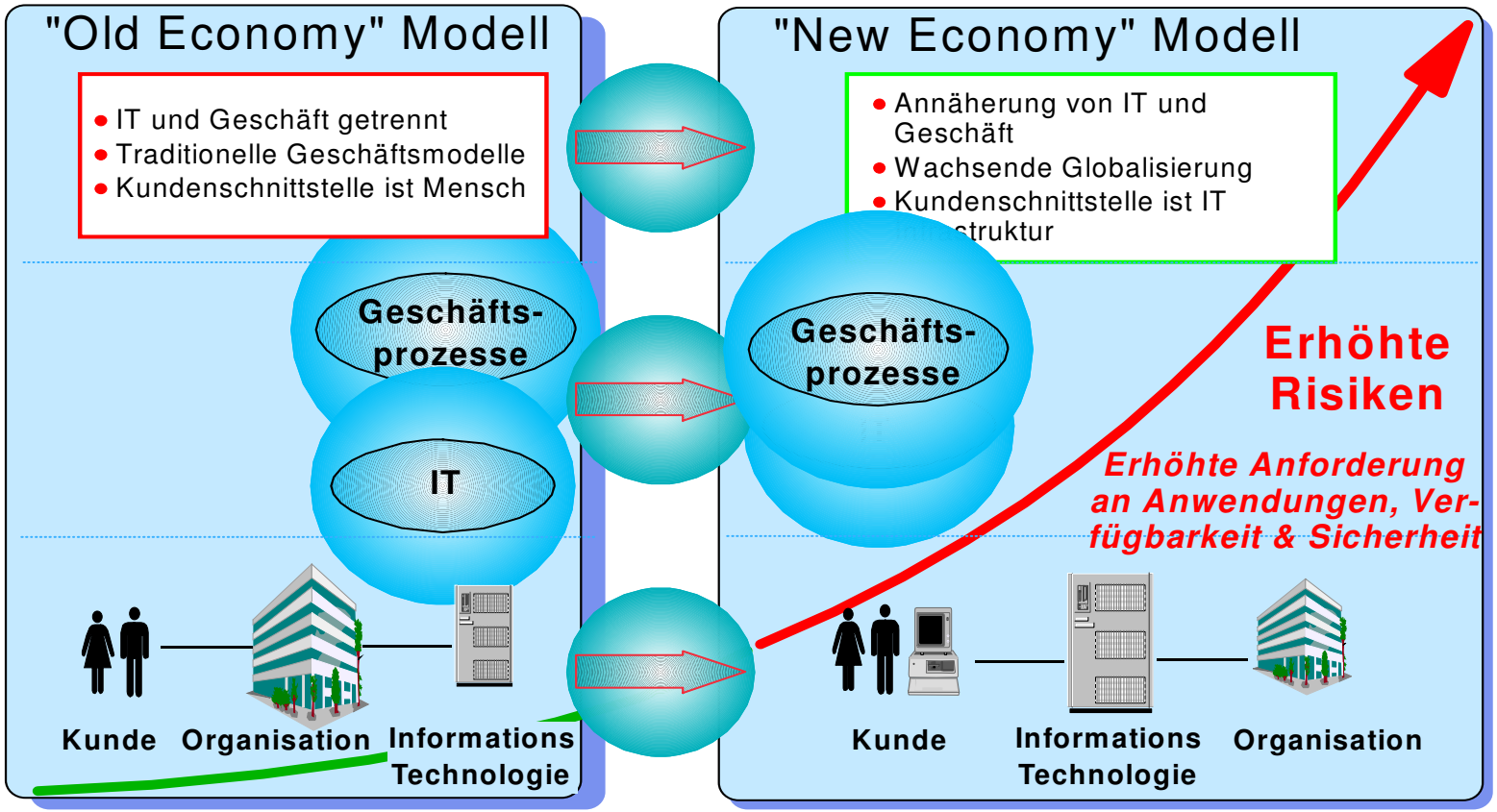
18. September 2003

Agenda

- Treiber für Informationssicherheits-Massnahmen
- Fallbeispiel „Bankneu“
  - Ausgangslage
  - Projekt Approach
  - Schwachstellen, Risiken
  - Risikobewertung
- Lösungsvorschlag (generell)
- Konklusion

Treibende Kräfte, Gründe für Informationssicherheitsdienste

Verzahnung der Geschäftsprozesse mit der IT

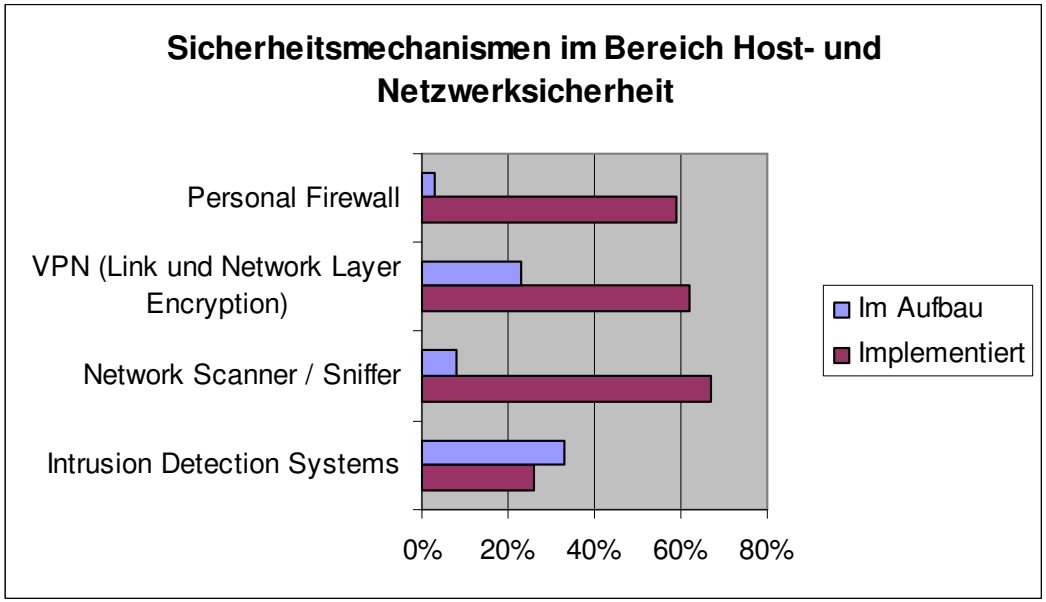


Treibende Kräfte, Gründe für Informationssicherheitsdienste

- **Vermehrte Angriffe**:
  - 40% der Unternehmen machten Angaben zum finanziellen Verlust; dieser lag durchschnittlich bei über **2 Millionen USD**
    "2002 CSI/FBI Computer Crime and Security Survey", Computer Security Institute, 2002
  - Gesamter **finanzieller Verlust** durch den "I-Love-You"-Virus: **2,6 Milliarden USD**
- **Bessere Benutzerkenntnisse** für Angriffe auf Computersysteme (spezialisierte Tools sind öffentlich erhältlich)
- Rasende **Entwicklungsgeschwindigkeit** im Sicherheitsbereich (neue Patches, Methoden, Gegenmaßnahmen)

Treibende Kräfte, Gründe für Informationssicherheitsdienste
Wahrnehmung vs Wirklichkeit

- Marktstudie: Informationssicherheit 2002 von PwC Consulting zeigt, dass „viele“ technische Sicherheitsmassnahmen bereits implementiert sind:



… und trotzdem

- **erhöhte** sich **die Zahl der gemeldeten Zwischenfälle** von **3’734** (in 1998) **auf 83’658** (in 2002)
  “Security & Privacy”, IEEE Computer Society, 2002
- **geben 64%** der befragten Unternehmen an, dass Computer Systeme in Ihrem Unternehmen **unberechtigterweise genutzt** worden sind.
  “2001 CSI/FBI Computer Crime and Security Survey”, Computer Security Institute, 2001

Fall-Beispiel

Ausgangslage für ein Network Security Assessment

- Die durch die **Fusion von Bank A und Bank B entstandene „Bankneu“** hat in den letzten Jahren eine außerordentlich dynamische Geschäftsentwicklung erlebt. Mit der Fusion der beiden Banken wurden auch die Informatikverantwortlichkeiten der beiden Banken zusammengelegt. Durch die unterschiedlichen Ausrichtungen der beiden Banken (z.B. Retail und Private Banking) kamen auch **unterschiedliche Geschäfts/Informatik Strategien, Strukturen und Kulturen** zusammen.

- Weiter verzeichnet die Bankneu ein grosses Wachstum (steigende Mitarbeiterzahl, neue Lokationen) , bietet **neue Kundenlösungen** an (ua. Internet Banking, Mobil Sales), **verlagert Erfassungsfunktionen** auf Vertriebspartner (Partnerbanken) was zusätzliche Anforderungen an die Informatik bzw. Sicherheit generiert.

- Um sicher zu stellen, dass bei all der geschilderten Dynamik die Sicherheitsanforderungen angemessen Berücksichtigung fanden und finden, möchte die Bankneu ein Assessment für Netzwerk-Sicherheit durchführen.

- Bankneu ist in **5 Ländern** mit mehreren Tausend Mitarbeitern vertreten

Fallbeispiel
Zielsetzung und Auftrag von IBM

- Aufzeigen der vorhandenen **Risiken und Schwachstellen** mittels eines Netzwerk Security Assessments (RAS-Server, Firewalls, Proxy-Server, Mail-Server, Firewall, Authentication-Server, Links zu Dritten (Bloomberg, Swift, Reuters, ..))
- NSA) und „Best Practice“ Vergleichen

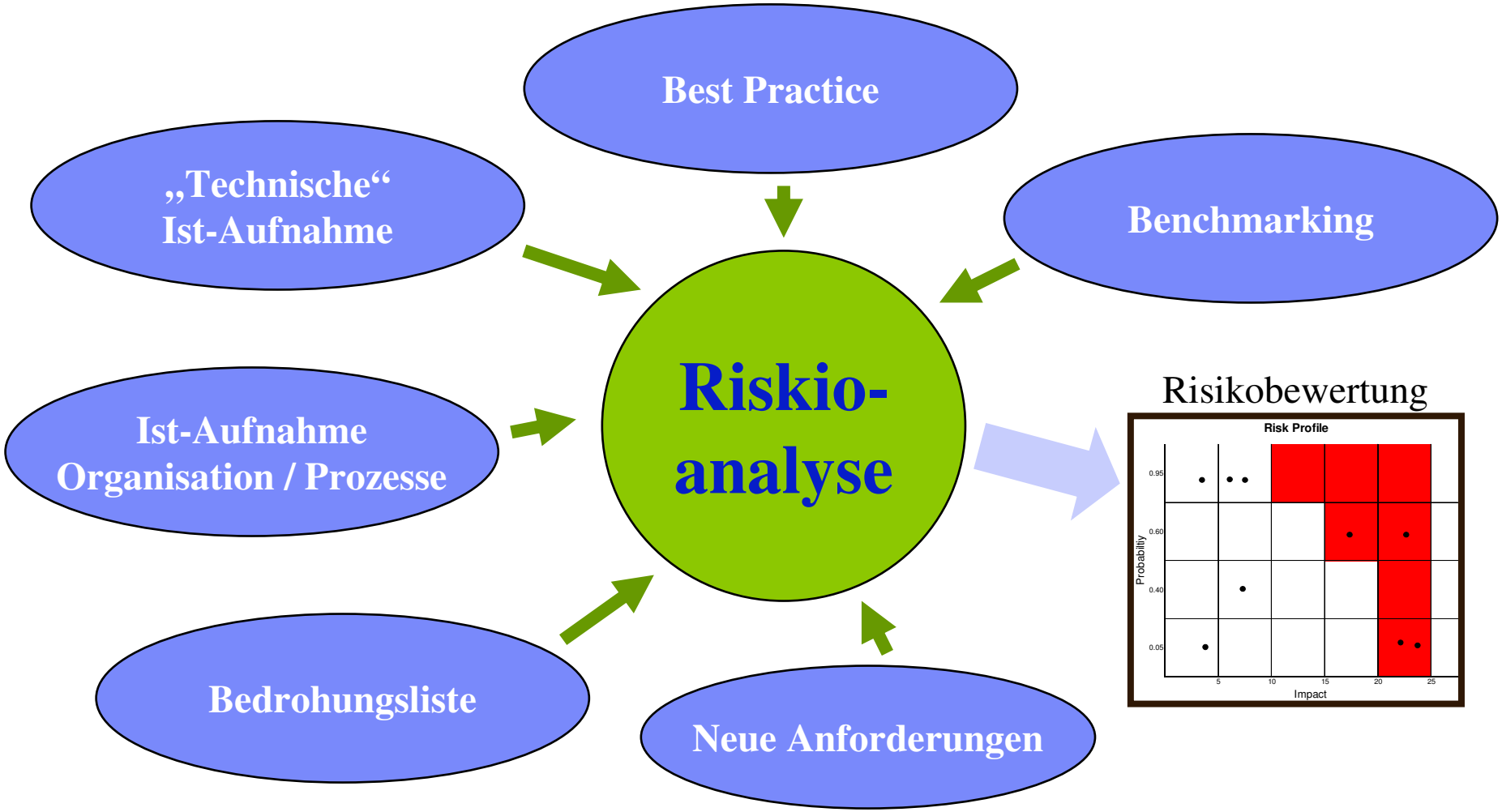
- Sofortige **Weiterleitung** der kritischen **Schwachstellen**

- Erzielung von schnellen Resultaten (Konzentration auf das Notwendige und Realistische) durch gemeinsames Festlegen und Priorisieren der notwendigen Maßnahmen

- Festlegung auf ein Security Framework (vorhandenes oder zu evaluierendes) bzw. eventuelle Übernahme vom übergeordneten Security Projekt

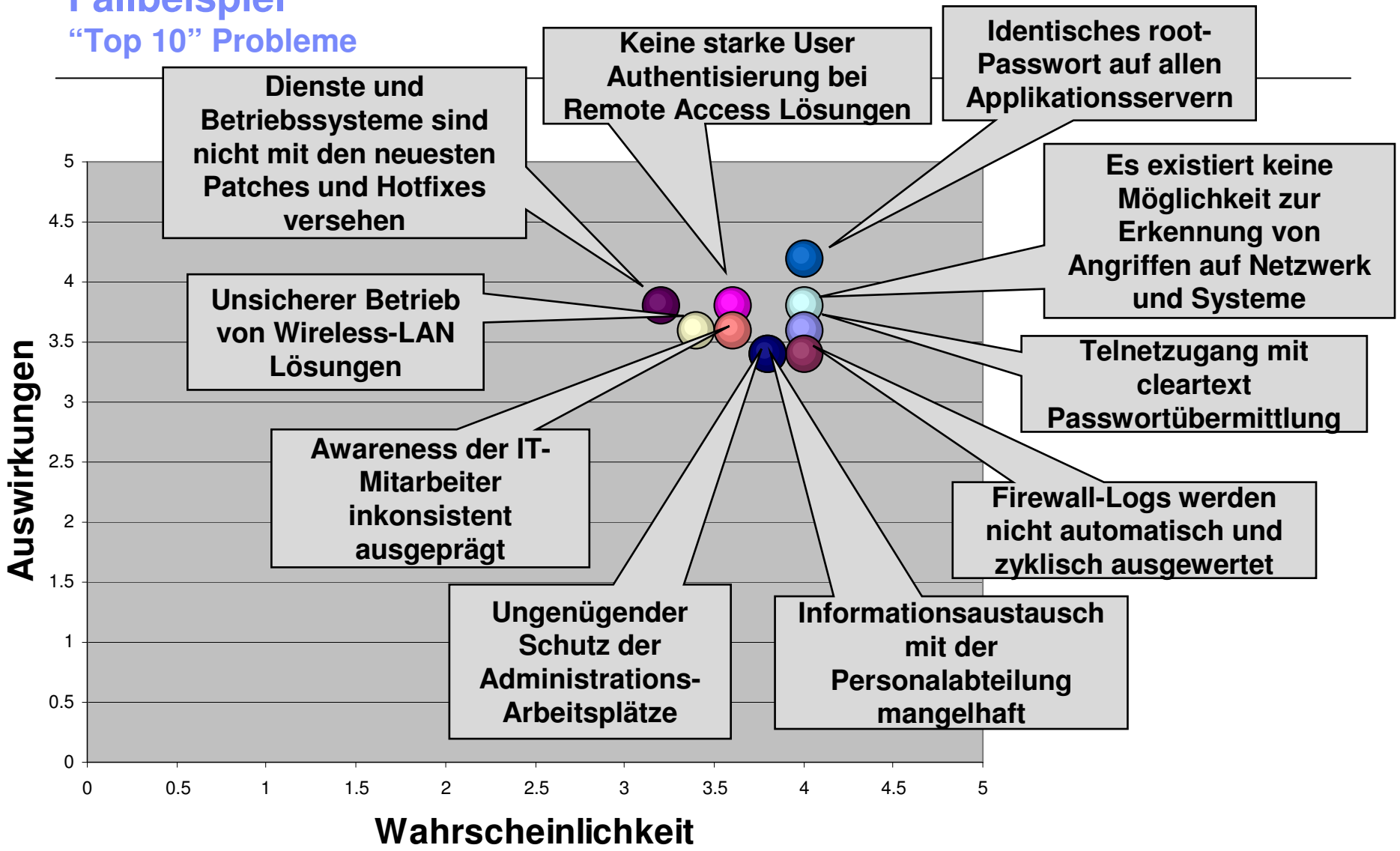
- Implementierung von konzernweiten **Security Baselines**

Fallbeispiel
Methodik / Vorgehen



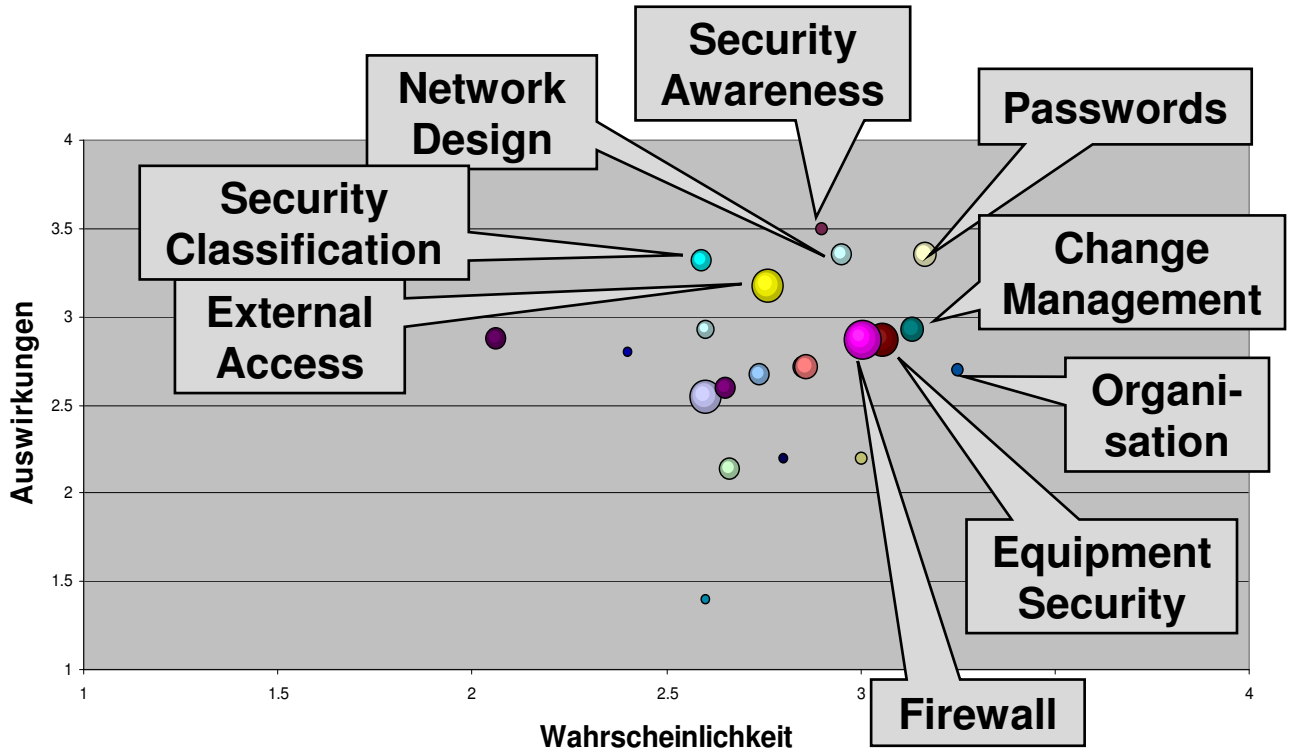
Fallbeispiel

"Top 10" Probleme



Fallbeispiel

Auszug aus der Risikogruppierung



Fallbeispiel
Ergebnis der Risikoanalyse

- Resultate Ist-Aufnahme der Schwachstellen bzw. Risiken -→ „Beispiel Bankneu“:
  - Policies
  - Organisation
  - Prozesse Awareness/Auditing
  - Technologie

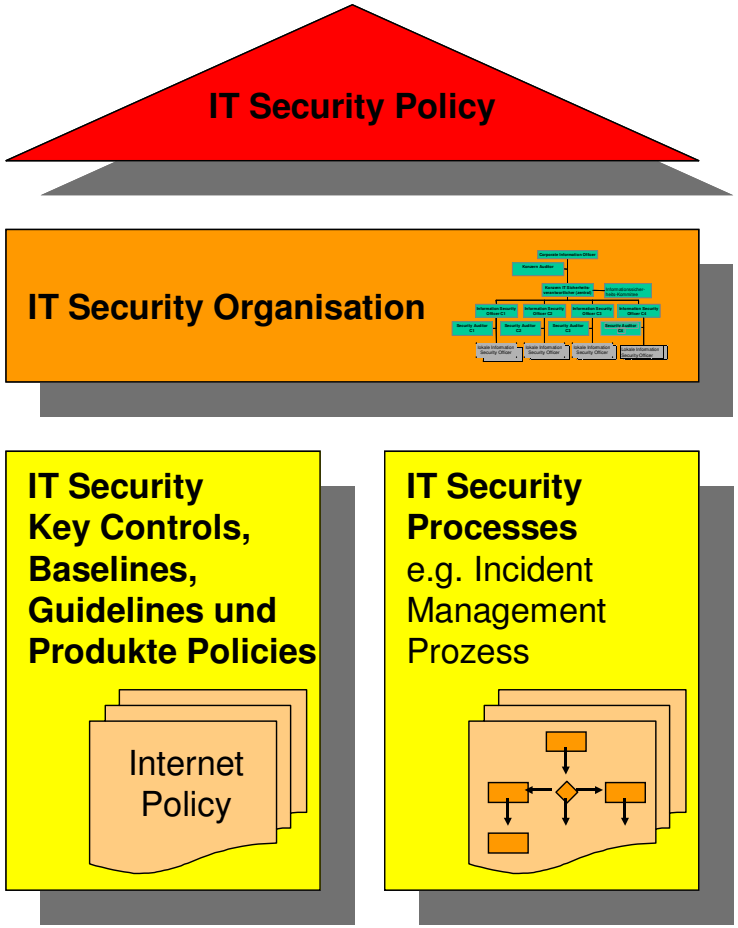
- Branchen-Benchmark mit mehr als 100 anderen Instituten --- „Bankneu“ liegt weit abgeschlagen zurück

- Bedrohungen durch neue Technologien liegen nicht explizit vor

Fazit: Zunächst müssen alle relevanten Risiken ermittelt und zumindest qualitativ bewertet worden sein, um zu Wissen, welche Sicherheitslösungen zur Reduzierung welcher Risiken benötigt werden

Lösungsansatz

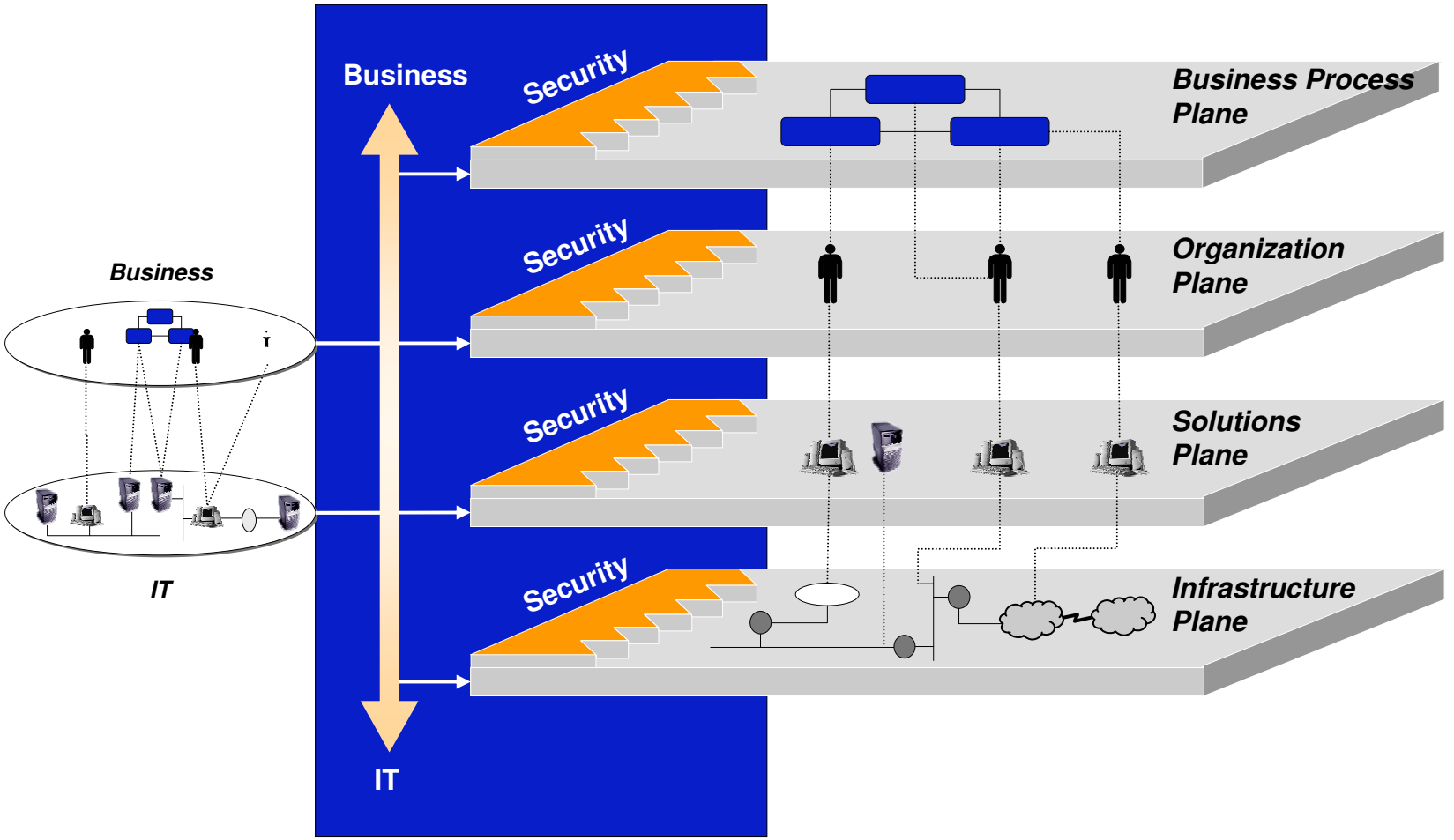
IT Security Framework



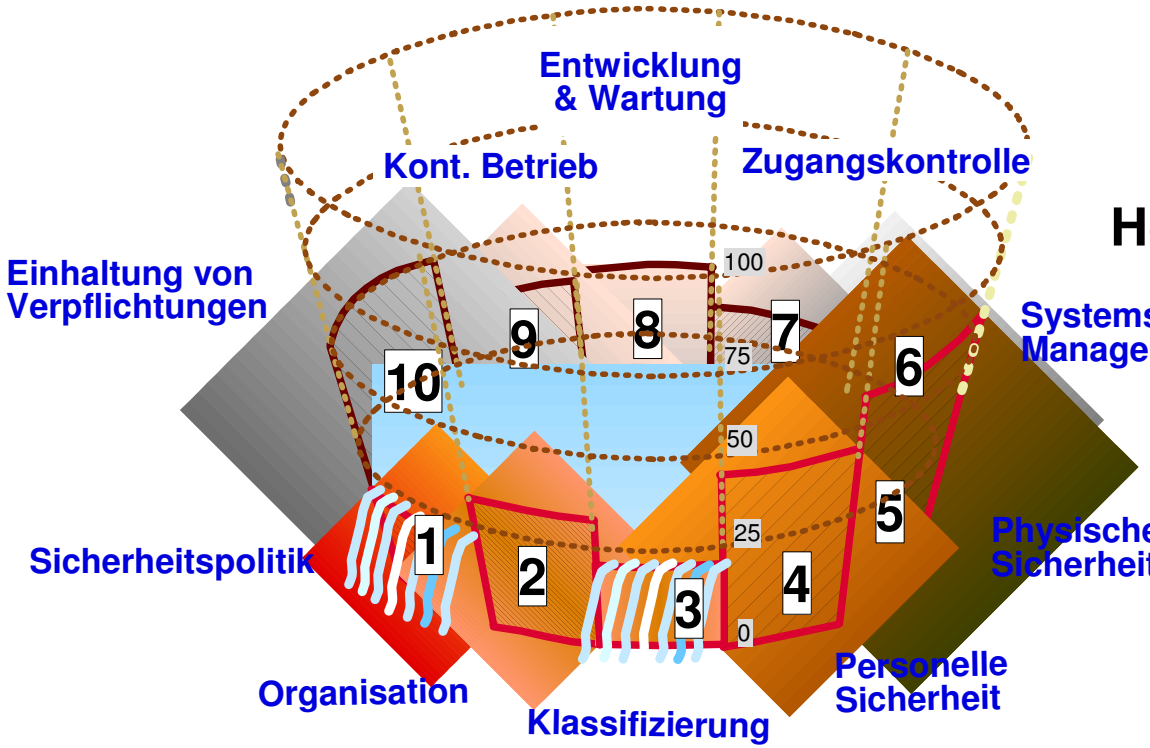
- **IT Security Policy**: Eine „high level“ IT Security Policy welche firmen- oder konzernweit die Grundsätze festlegt
- **IT Security Organisation**: werden die Rollen (auf Firmen, ggf. auch auf Konzernebene) festgelegt und die entsprechenden Verantwortlichkeiten zugewiesen
- **IT Security Key Controls**: hier wird vorgeschrieben, WAS in den verschiedenen Bereichen bezüglich IT Security befolgt und WIE es entsprechend umgesetzt werden muss
- **IT Security Prozesse**: Beschreiben die IT sicherheitsrelevanten Abläufe und müssen unbedingt in schon bestehende Prozesse integriert werden

Lösungsansatz

4-Layer Modell - ganzheitliche Sicht



Lösungsansatz
Sicherheitsbereiche

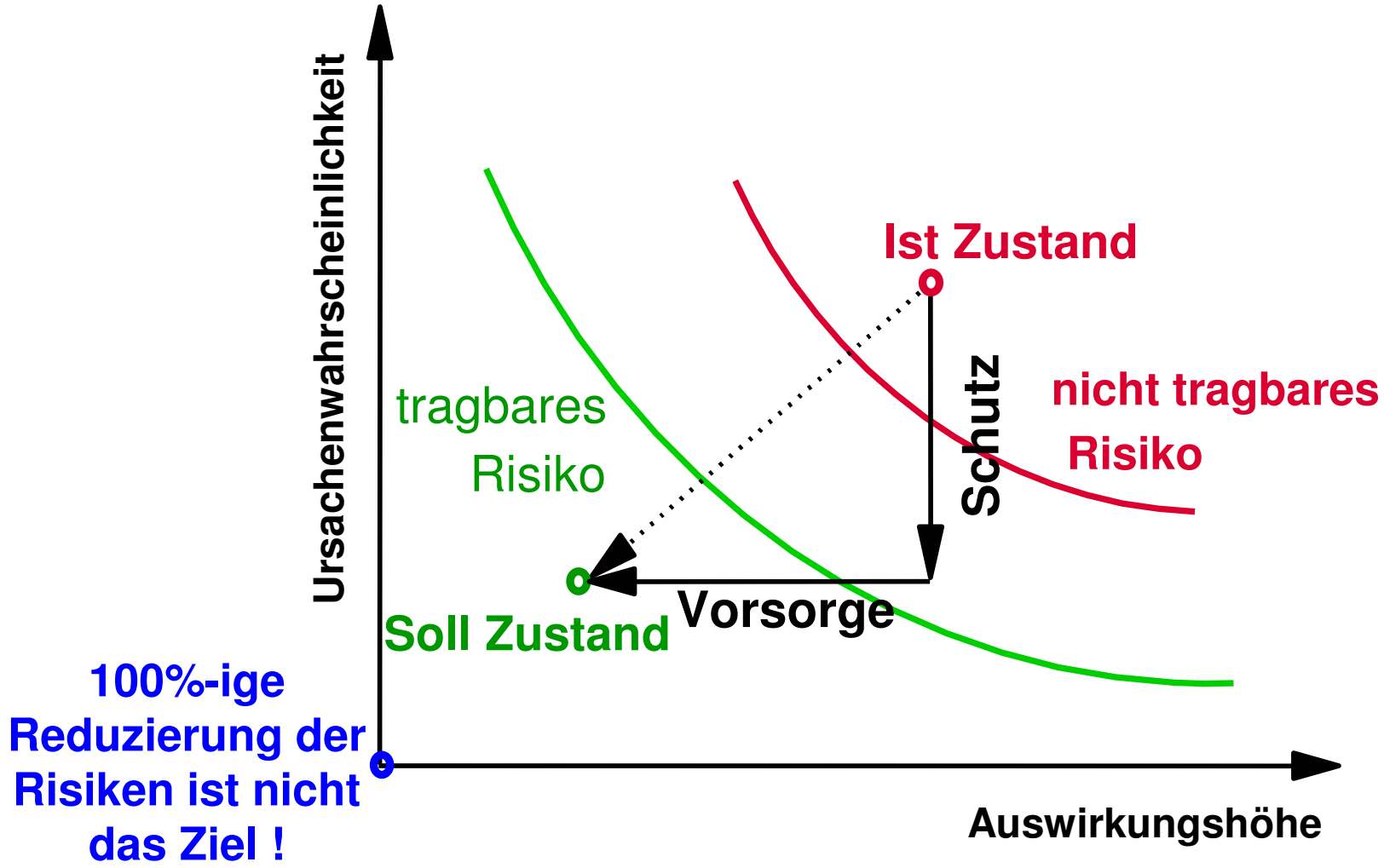


Holzeimermodell

In diesem Beispiel wurde dem Sicherheitsaspekt "5" (physische Sicherheit) große Aufmerksamkeit geschenkt, während "1" (Sicherheitspolitik) und "3" (Datenklassifizierung) vernachlässigt wurden. Die Gesamtsicherheit ist beeinträchtigt, so daß Bedrohungen eintreten.

Lösungsansatz

Risikomanagement - das Risiko auf ein akzeptierbares Niveau reduzieren



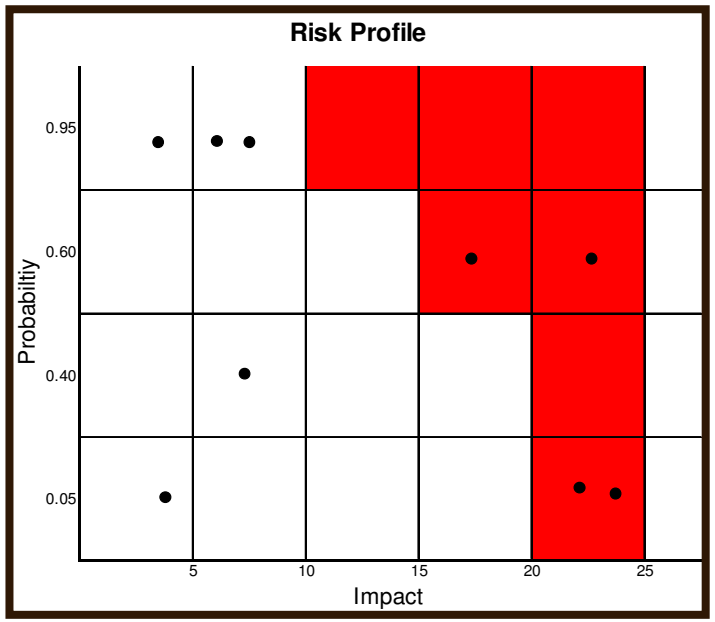
Lösungsansatz
Risikomanagement - Ableitung von entsprechenden Massnahmen

- **Schutz (Beispiele):**
  - Schutz des Firmennetzes durch verschiedene Sicherheitszonen, deren Übergänge besonders geschützt sind
  - Schutz der Daten in Anwendungen/Portalen durch starke Authentifizierungs-verfahren
  - Schutz der Daten durch Gewährleistung von Vertraulichkeit, Urheberschaft und Integrität beim Transport

- **Vorsorge (Beispiele):**
  - Verlagern von Risiken (z.B. durch Versicherungen), so dass die Schadenshöhe begrenzt ist.
  - Mindern von Risiken durch Reduzierung der betroffenen Geschäftswerte pro Geschäftsvorfall
  - Rückzug aus Geschäftsfeldern

Lösungsansatz
Risikoorientierte Umsetzung

Risikobewertung

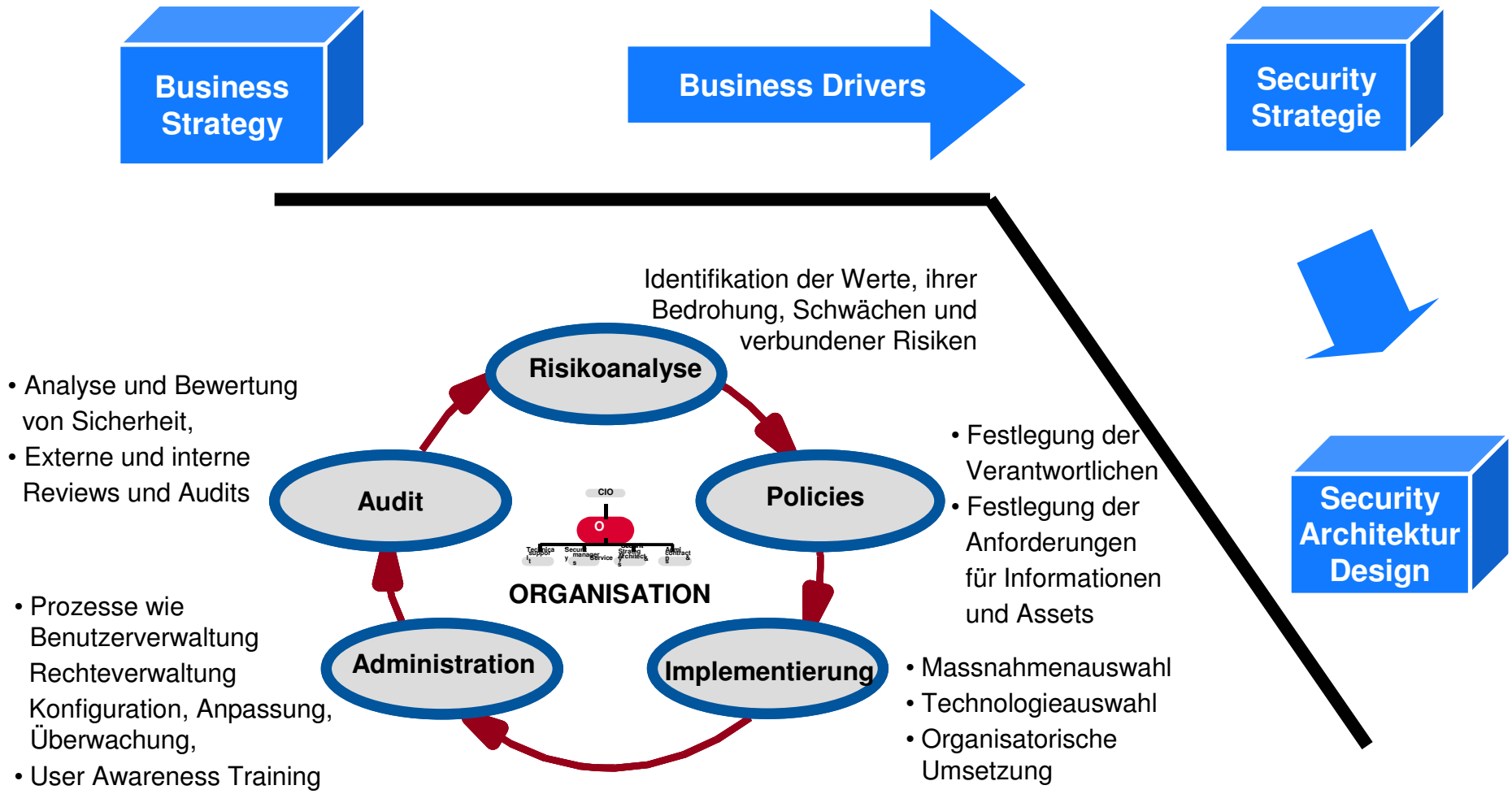


„Wie viel Risiko kann und will ich tragen?“

Nur die Beantwortung dieser Frage erlaubt bei der Priorisierung der Projekte/Vorhaben die richtigen Schwerpunkte zu setzten !!

Konklusion

IBM‘s Ansatz - Zielorientiertes Vorgehen auch in Zukunft



Konklusion

- Es bedarf einer **optimalen Abstimmung** zwischen Policies/Vorgaben, Prozessen und den entsprechenden technischen Systemen und Technologien – ein Element alleine hilft nicht !!

- Security Vorgaben und Prozesse basieren auf einem **risikogewichteten Verfahren** -- ergibt die Priorisierung (Balance zwischen Kosten, Sicherheitslevel und Anwendbarkeit/Akzeptanz)

Dieser Ansatz bildet auch für die erwähnte Bank in der Zwischenzeit die Basis für eine **nachhaltige Umsetzung** der Sicherheitspolitik bzw. **bewusster Umgang** mit den **Risiken**.