Risikoanalyse zur Informations-Sicherheit: ein Vorgehensmodell

Bernd Ewert

it-sa Oktober 2009
Forum rot

Grundsätzliches zur Risikoanalyse

- Sinn der Risikoanalyse:
  - Übersicht schaffen
  - Schutzmaßnahmen steuern
  - Normen genügen (ggf. Zertifizierung)

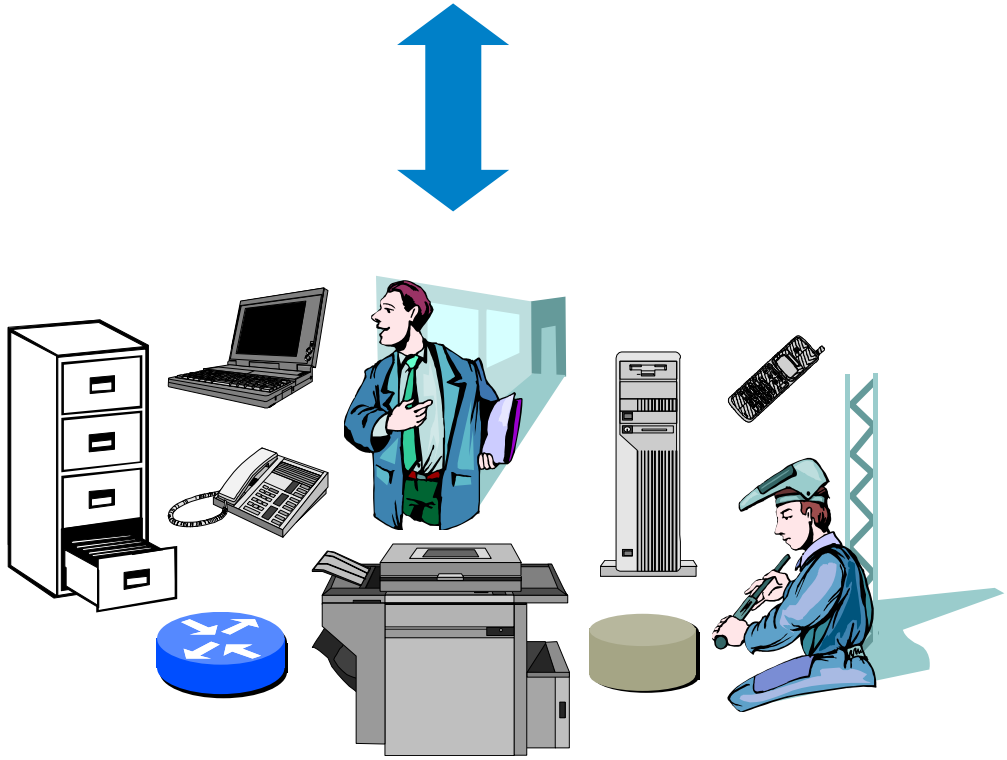
- Anforderungen an die Risikoanalyse:
  - für Geschäftsbereiche verständlich
  - spezifisch technische Risiken berücksichtigt
  - vergleichbare Maßstäbe
  - möglichst geringer Aufwand

- => standardisiertes Vorgehen

Grundsätzliches zu Informationen

- Informationsinhalte
  - Inhalt von Rechnungen
  - Forschungsergebnisse
  - Personaldaten
  - Pläne
  - ...
- Informationsträger
  - Storage Area Network
  - Rechner
  - Server-Raum
  - Internet-Anbindung
  - Papier
  - Telefon
  - Mitarbeiter
  - ...

Rabatte
Rezepturen



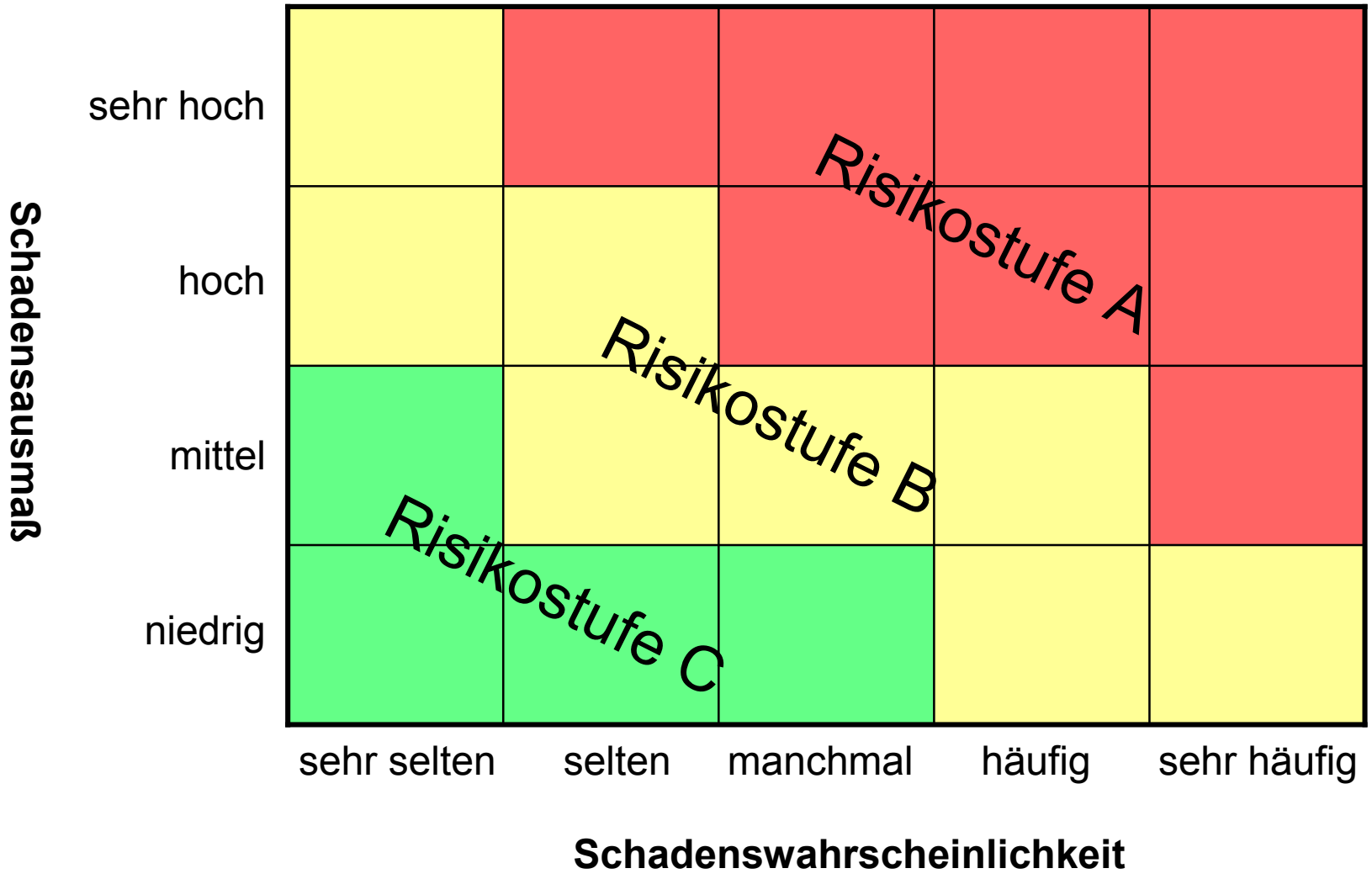
Risiko für Informations-Sicherheit

- Risiko = Schadenspotential x Eintrittswahrscheinlichkeit
- Schadenspotential:
  - direkt nur Sachschaden
  - Folgen hängen vom Inhalt der Informationen ab
- Eintrittswahrscheinlichkeit:
  - Bedrohungen universell gültig
  - Schwachstellen und Schutzmaßnahmen hängen vom Träger der Information ab
  - für absichtliche Delikte Schadenspotential relevant

Ablauf der Risikoanalyse: Vorbereitung

- Bedrohungen identifizieren
  - für Gesamtorganisation
  - Verursacher Natur, Mensch, Dienstleister, Technik
  - vorsätzlich oder nicht
- Schadenskategorien identifizieren
  - Schädigung von Menschen
  - Rechtsverstoß
  - direkte Geldeinbuße
  - Beeinträchtigung des Geschäftsablaufs
  - Image-Schaden
  - Reduktion von Knowhow-Vorteilen
- Risikomatrix

Risikomatrix



Ablauf der Risikoanalyse: Durchführung 1

- Informationsinhalte identifizieren
  - Orientierung an Prozessen
- Schadenspotential und damit Schutzbedarf erheben
  - getrennt nach Vertraulichkeit, Verfügbarkeit, Integrität ...
- Informationsträger identifizieren
  - direkte Träger, aber auch Räume und Gebäude
- Risikoobjekte bilden
  - Mengen von Inhalten und Trägern, die gemeinsam auftreten

Zusammenführung zu Risikoobjekten

~ 100
Informationsinhalte

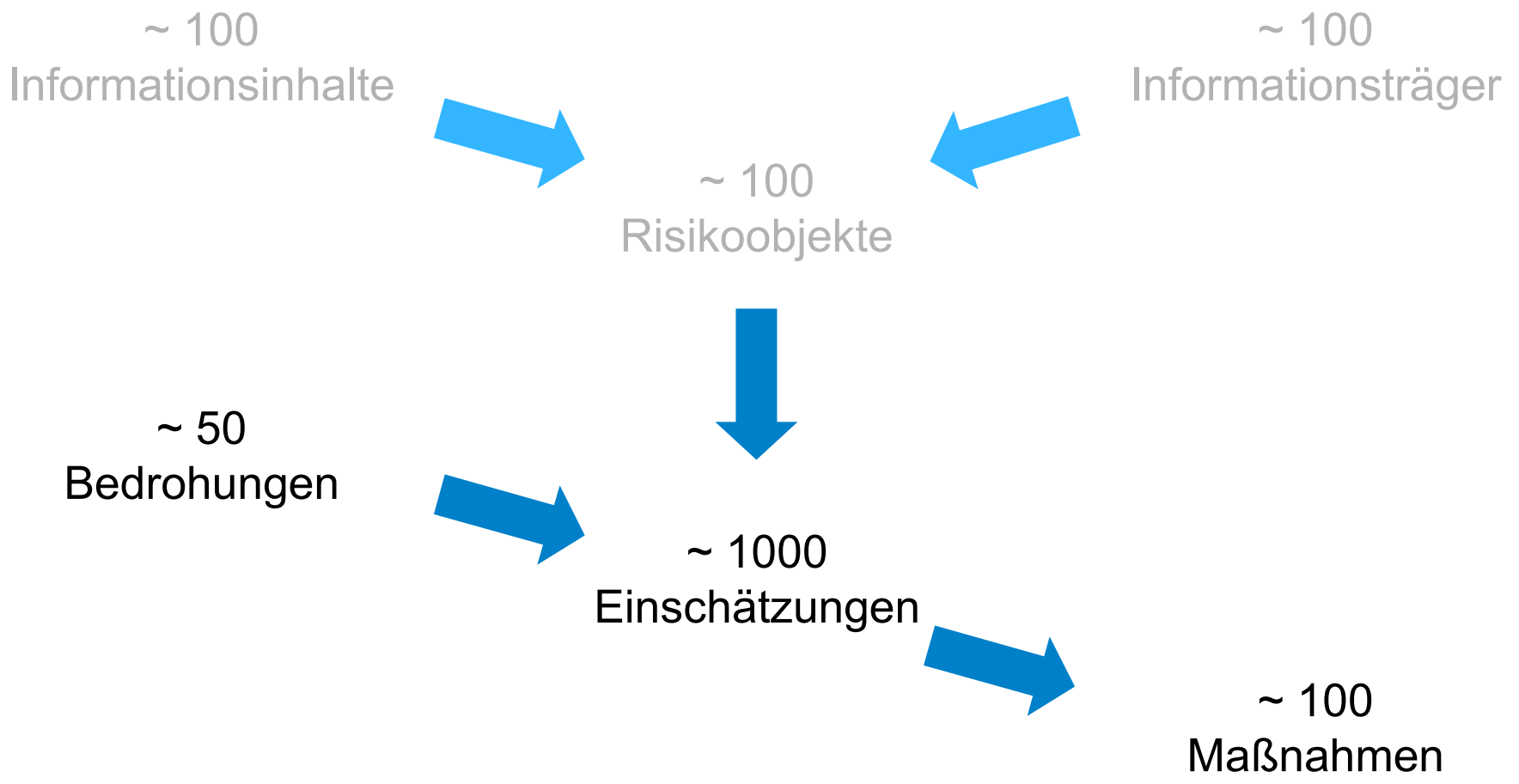
~ 100
Informationsträger

~ 100
Risikoobjekte

Ablauf der Risikoanalyse: Durchführung 2

- Bedrohungen für Objekte identifizieren
- Schwachstellen und vorhandene Schutzmaßnahmen identifizieren
- Eintrittswahrscheinlichkeiten ableiten
- Schadenspotentiale schätzen
- Risiken ableiten

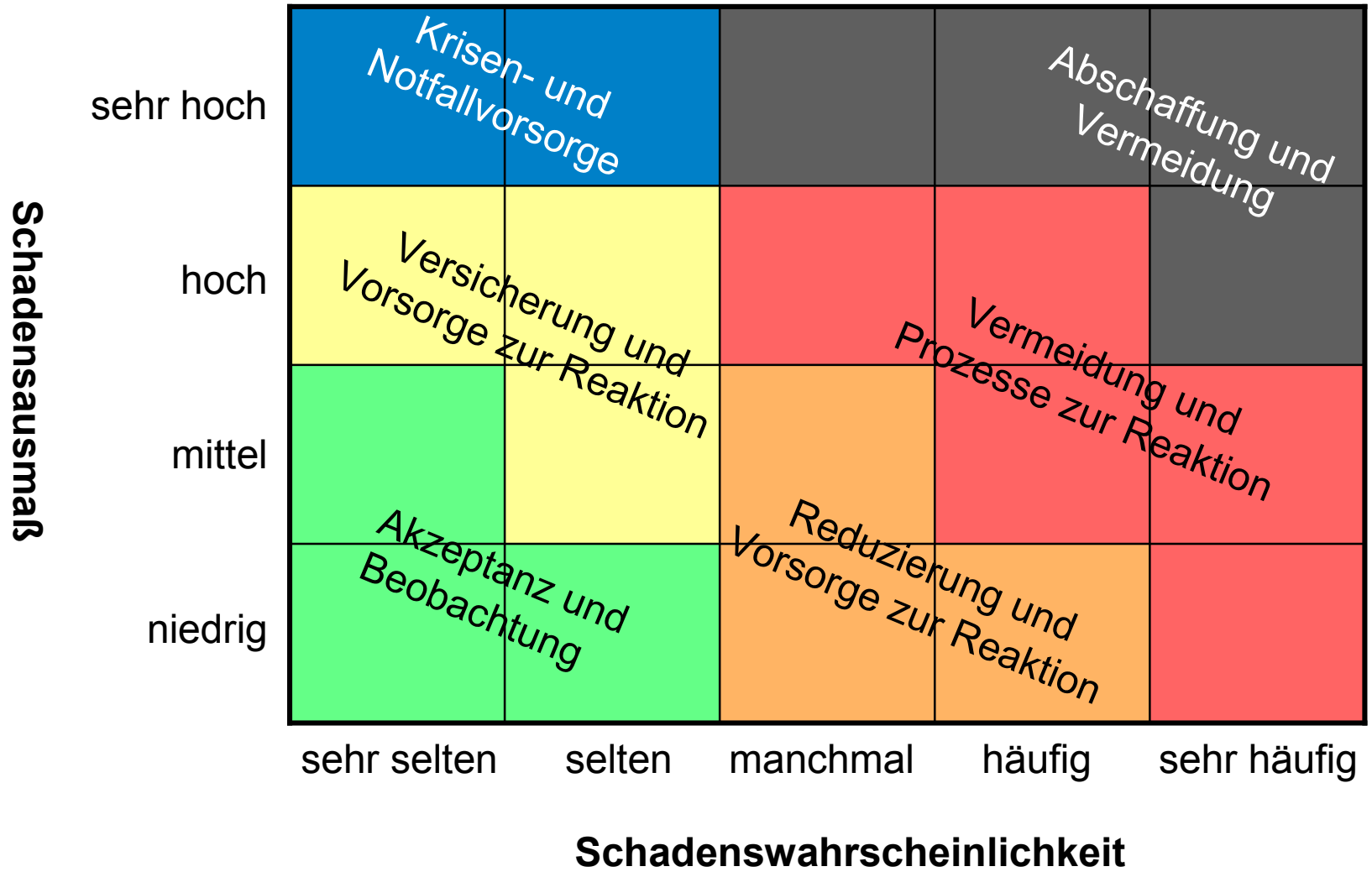
Risikoeinschätzung und Maßnahmenfindung



Ablauf der Risikoanalyse: Nachbereitung

- Umgang mit dem Risiko festlegen
  - vermeiden, reduzieren, abwälzen, akzeptieren
- Schutzmaßnahmen identifizieren
  - Nutzen abschätzen
  - Aufwand und Kosten schätzen
- Schutzmaßnahmen konsolidieren
  - Zusammenführung ähnlicher Tätigkeiten
  - Genehmigung einholen
  - Verantwortlichkeit festlegen

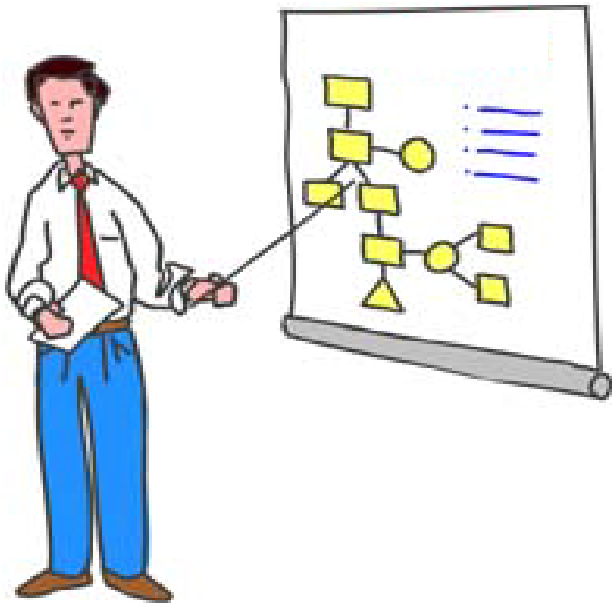
Schutzstrategie

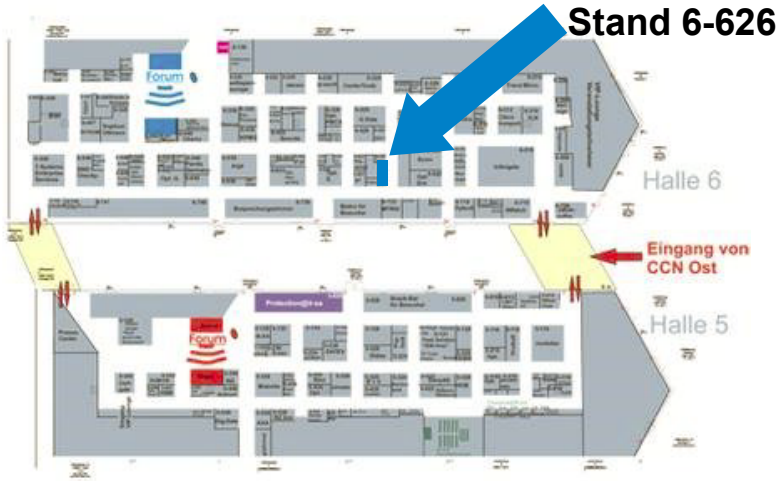


Aufwand und Kosten

- Kernteam: ISO (ggf. mit Berater)
- Vorbereitung: ~ 5 AT
- Interviews Leiter Geschäftsbereiche:
  20 x 1-2 Stunden x 2-3 Personen ~ 20 AT
- Interviews Service-Bereiche:
  100 x 1-4 Stunden x 2-3 Personen ~ 50 AT
- Nachbereitung: ~ 5 AT
- Unterstützung mit Tool

Vielen Dank
für Ihre Aufmerksamkeit!





consequa

Dipl.-Inform.
Bernd Ewert
Geschäftsführer

consequa GmbH
Süderstraße 73
20097 Hamburg
www.consequa.de

Tel.: 040 / 78 89 70 61
Fax: 040 / 78 89 70 66

bernd.ewert@consequa.de