

„Einsatz und Umsetzung von Security Policies“

Detlev Henze

Geschäftsführer TÜV Secure iT

IT Security Day 2004
27. Mai 2004, München



IT-Risiken kennen
Vorausschauend handeln

www.tuv.com



TÜV Rheinland Group

■ Inhalt

■ TÜV Secure iT

■ Gemanagte IT-Security als Erfolgsfaktor für Unternehmen

■ Security Policies:

- Initialisierung
- Analyse
- Planung und Umsetzung
- Betrieb

www.tuv.com



© TÜV Secure iT GmbH 2004



TÜV Rheinland Group

■ IT Risiken kennen – Vorausschauend handeln

Wer wir sind.

- Tochtergesellschaft der TÜV Rheinland Group
- TÜV RG weltweit vertreten an 200 Standorten in 50 Ländern
- TÜV Secure iT: Spezialisten zur dauerhaften Sicherung von IT-Umgebungen
- Konzentration auf IT Services in den Bereichen IT- Security, IT-Prozesse und e-Business



www.tuv.com

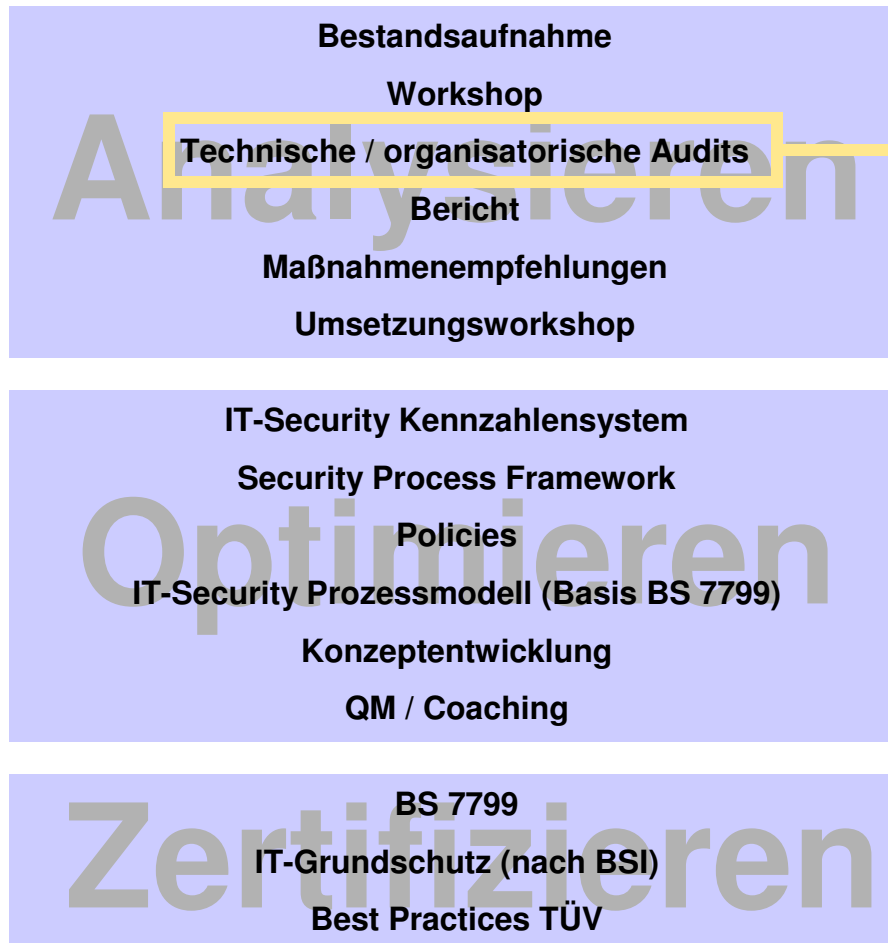


© TÜV Secure iT GmbH 2004



TÜV Rheinland Group

■ Mit Sicherheit zum Erfolg



Technische Audits:

Scanning
Pentesting
Client Hacking
TK-Anlagen Scanning

Organisatorische Audits:

Risikoanalyse
Schutzbedarfsermittlung
GAP-Analyse
Audits
Begehungen

www.tuv.com



© TÜV Secure IT GmbH 2004



TÜV Rheinland Group



■ Inhalt

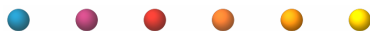
- TÜV Secure iT

- Gemanagte IT-Security als Erfolgsfaktor für Unternehmen

- Security Policies:

- Initialisierung
- Analyse
- Planung und Umsetzung
- Betrieb

www.tuv.com

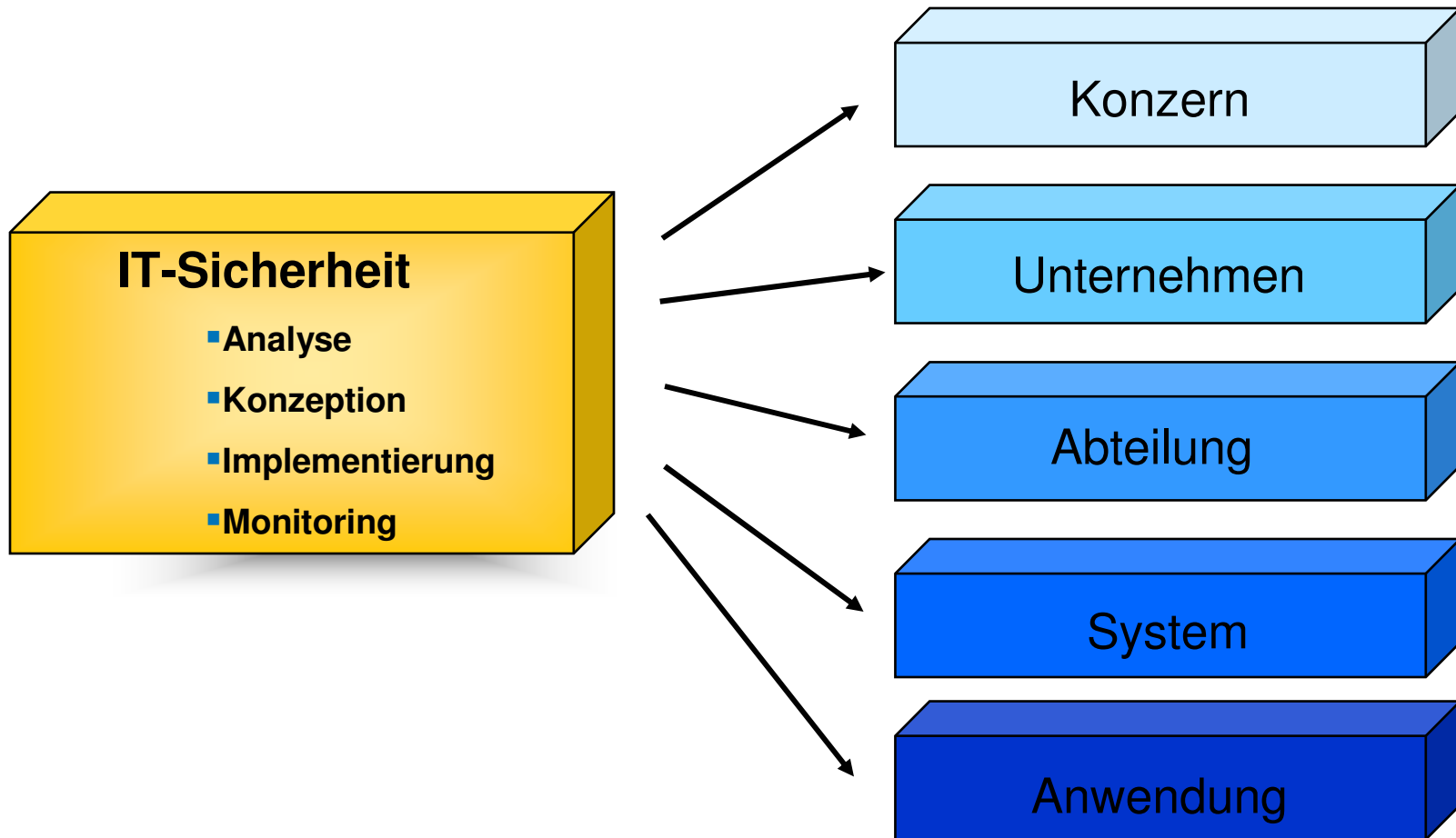


© TÜV Secure iT GmbH 2004

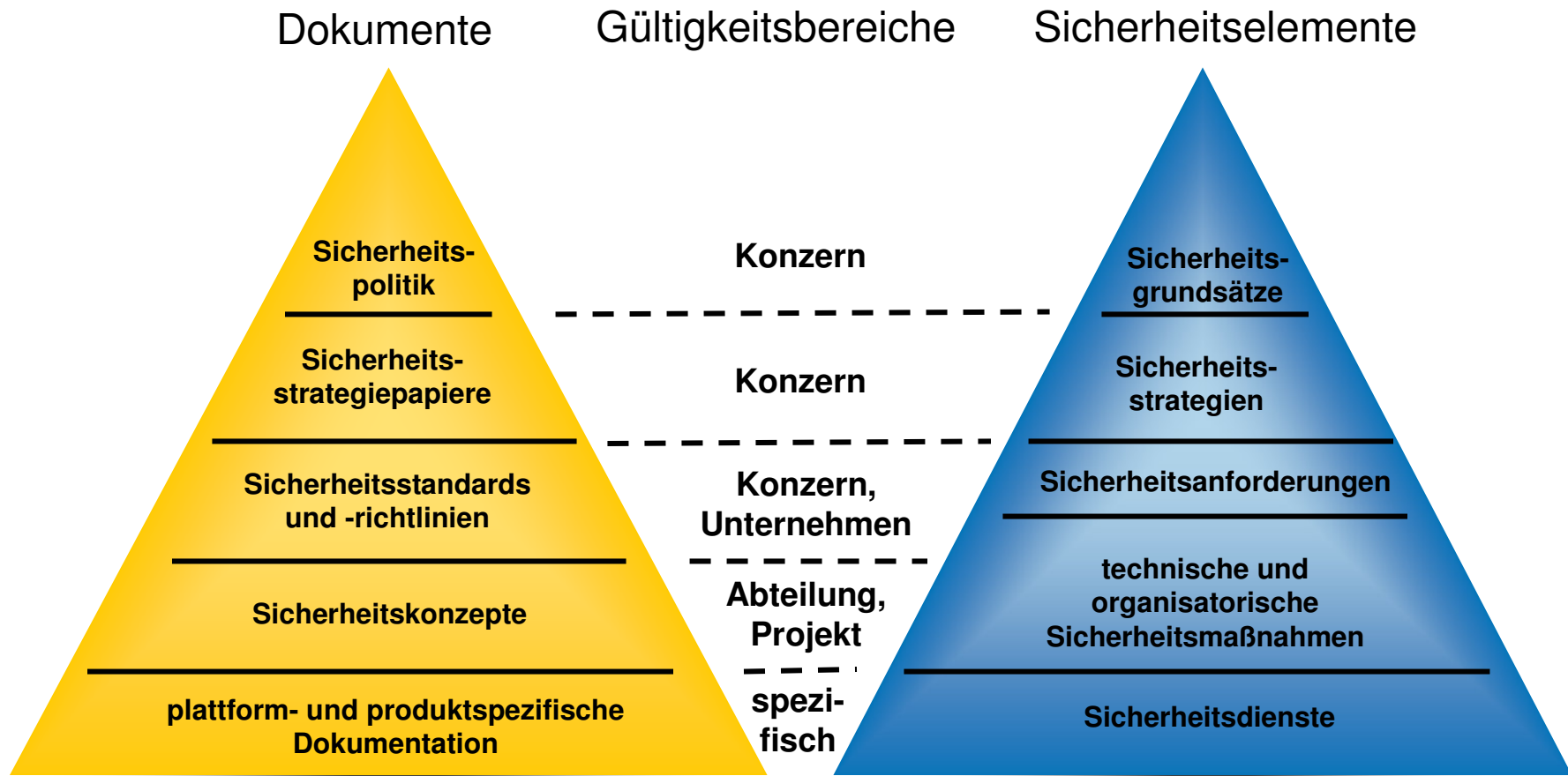


TÜV Rheinland Group

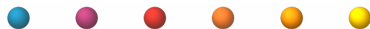
■ Strategisches IT-Sicherheitsmanagement



■ Sicherheitsarchitektur



www.tuv.com

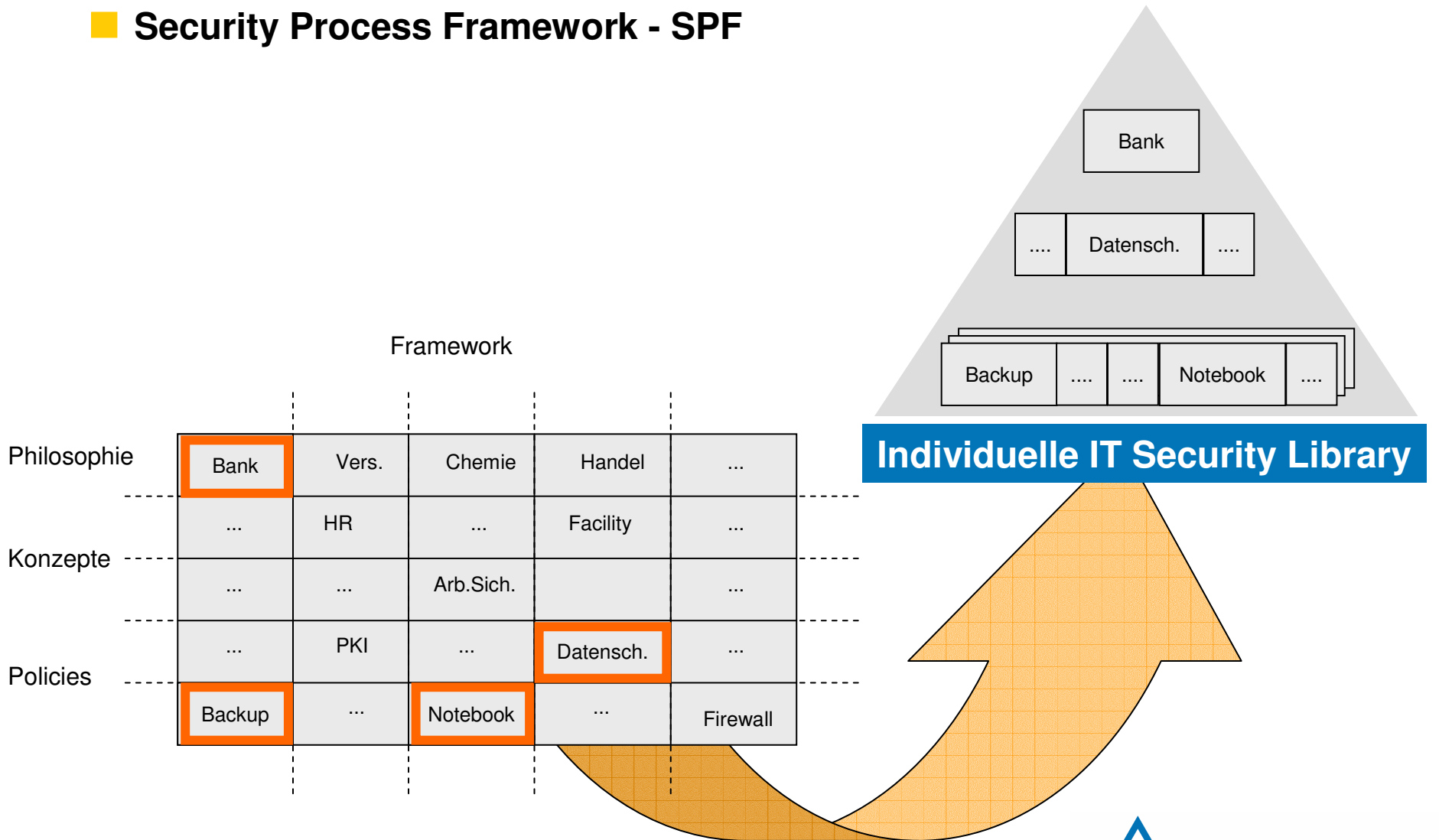


© TÜV Secure IT GmbH 2004



TÜV Rheinland Group

Security Process Framework - SPF



www.tuv.com



© TÜV Secure IT GmbH 2004



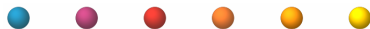
TÜV Rheinland Group

■ Inhalt

- TÜV Secure iT
- Gemanagte IT-Security als Erfolgsfaktor für Unternehmen

- Security Policies:
 - Initialisierung
 - Analyse
 - Planung und Umsetzung
 - Betrieb

www.tuv.com



© TÜV Secure iT GmbH 2004



TÜV Rheinland Group

■ Was ist eine IT-Security Policy?

■ Definition nach ISO/IEC 17799:

- Im Kern jeder Implementierung von Informationssicherheit muss die Formulierung eines fundierten und realistischen Sicherheitskonzepts (Information Security Policy) stehen.
- Nur durch ein solches Dokument kann die Unternehmensleitung umfassende Vorgaben dahingehend geben, wie die Informationssicherheit in der Unternehmenskultur und im Unternehmenskonzept integriert ist.
- Eine solche Sicherheitspolitik gibt den einzelnen Abteilungen und allen Mitarbeitern die Vorgaben, die sie bei der Umsetzung bei der täglichen Arbeit benötigen.
- Sie legt auch die Grundlagen für die organisatorische Umsetzung der notwendigen Prozeduren und Richtlinien und erlaubt damit eine umfassende Implementierung aller Sicherheitsaspekte.

www.tuv.com



© TÜV Secure IT GmbH 2004



TÜV Rheinland Group

■ Was sind und sollen Policies?

- Ziel: Sicherheit nachhaltig verbessern
- Sicherheitsprozess wird
 - handhabbar
 - managebar
 - nutzbar
- Einerseits allgemeine Regelungen bzw. Vorgaben
 - Handlungsspielraum wird definiert
- Andererseits konkrete Regelungen
 - Handlungsspielraum wird ausgefüllt
- Kontextbezogen

www.tuv.com

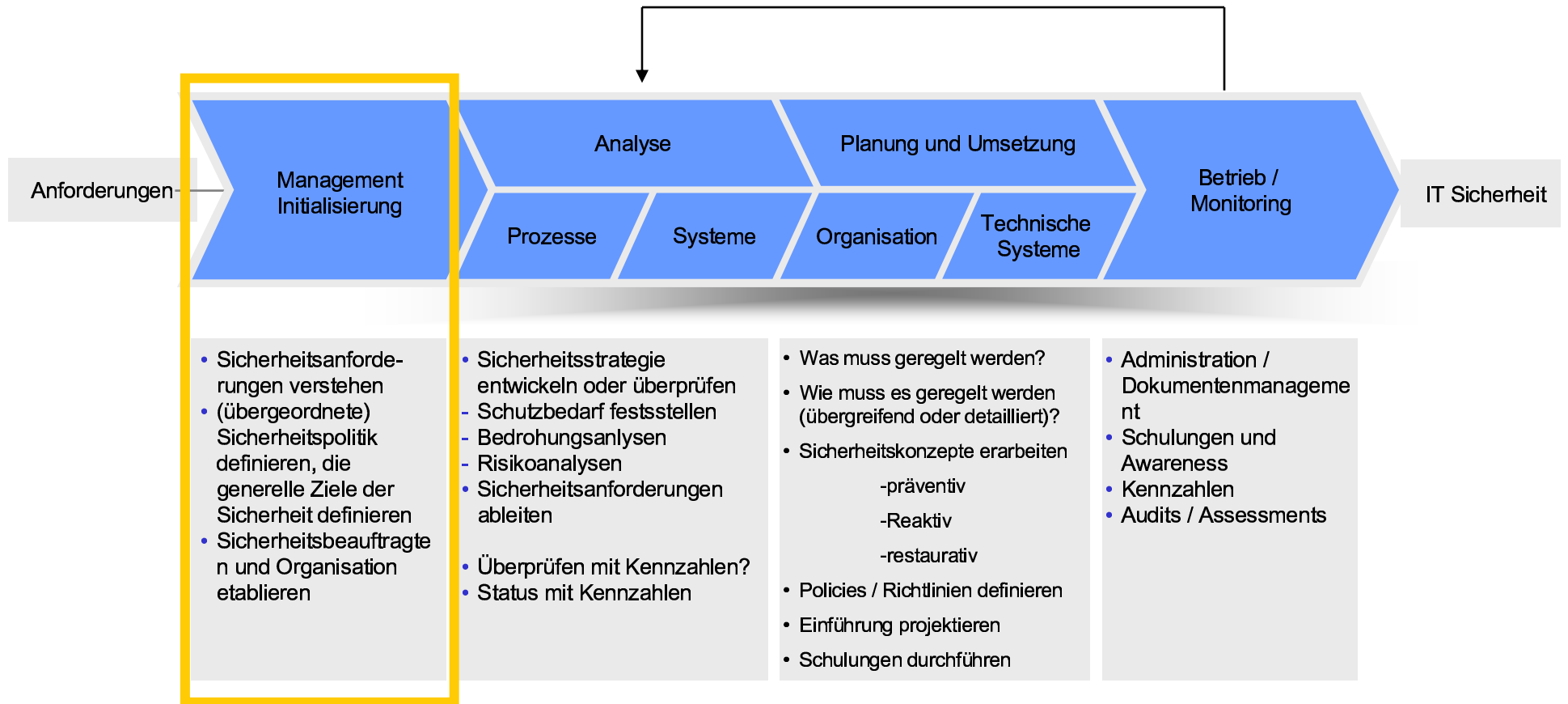


© TÜV Secure IT GmbH 2004



TÜV Rheinland Group

■ Der Implementierungsprozess für Security Policies



■ Management Aufgaben

■ Initialisierung des Sicherheitsprozesses

- IT-Sicherheitspolitik formulieren und verabschieden
- IT Sicherheitsorganisation etablieren: IT Sicherheitsbeauftragten (ITSB) benennen, Organisation entsprechend der Unternehmensgröße und Struktur aufbauen
- Verantwortung zuweisen, delegieren

■ Grundlagen für Sicherheitsprozess legen

- Schutzbedarfsfeststellung durchführen
- Ausgehend von Geschäftsprozessen wird Schutzbedarf ermittelt und daraus Klassifizierung abgeleitet
- Schadensklassen festlegen

■ „Awareness“ bilden und pflegen

- Aufmerksamkeit aller Mitarbeiter für die Belange des Informationsschutzes wecken und (vor allem) wach halten
- „internes Marketing“ betreiben – Maßnahmen mit Außenwirkung, z.B. Zertifizierung, Audits, Preisausschreiben, Kampagnen, ...

www.tuv.com



© TÜV Secure IT GmbH 2004



TÜV Rheinland Group

■ Initialisierung durch Kickoff-Workshop

■ Teilnehmer

- Leitende Mitarbeiter aus: Management, Organisation, IT, Datenschutz und Informationssicherheit, Kaufmännische Leitung, Technische Leitung

■ Input

- Bestimmung der generellen Sicherheitspolitik
- Bestimmung der übergeordneten Sicherheitsziele
- Bestimmung der Bereiche

■ Ergebnis

- Übereinstimmender „Zielkorridor“
- Etablierung eines Sicherheitsbeauftragten und der Organisation
- Motivation der Verantwortlichen und Zuständigen
- Optimale Vorbereitung

www.tuv.com

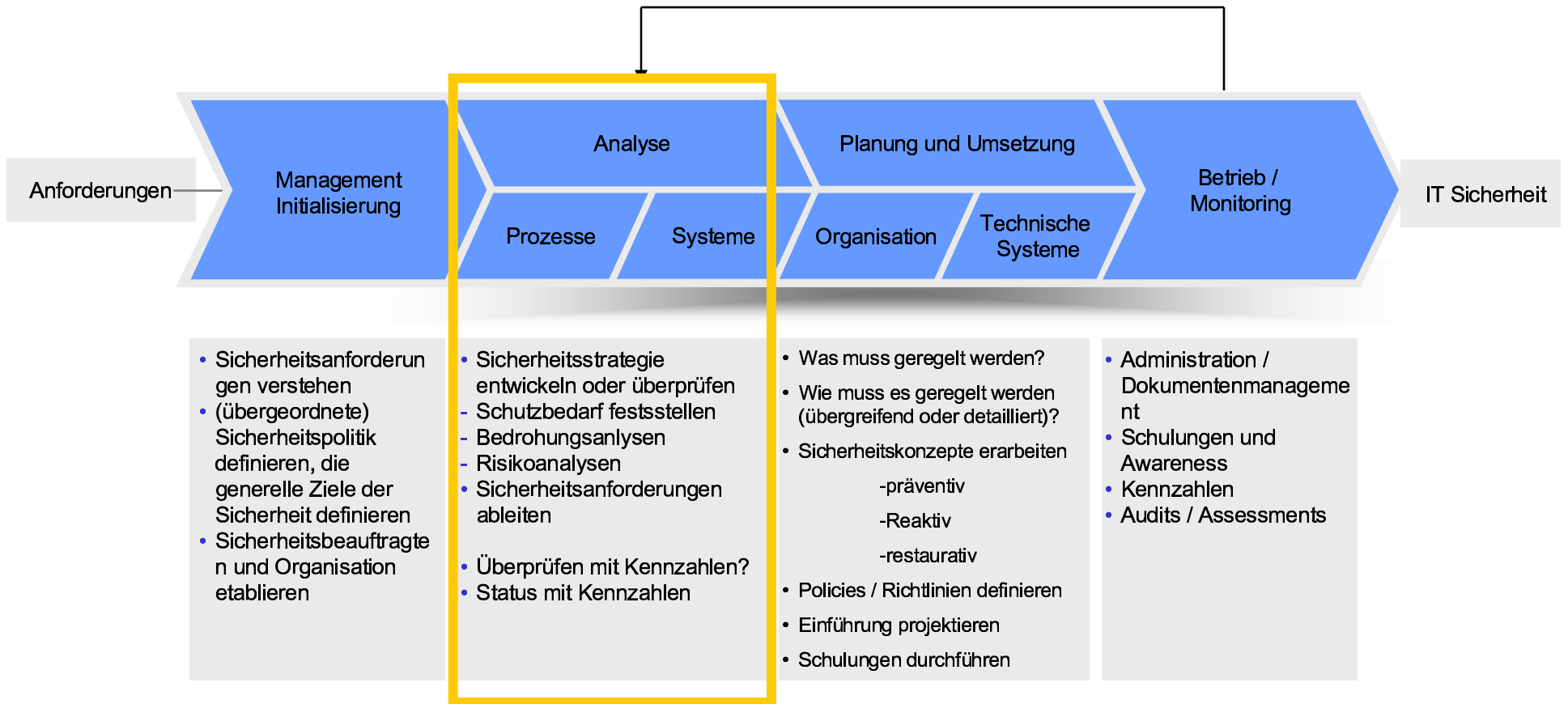


© TÜV Secure IT GmbH 2004



TÜV Rheinland Group

■ Der Implementierungsprozess für Security Policies



■ Bedrohungsanalyse / Risikoanalyse

- Analyse der Schwachstellen und Bedrohungen
 - Ziel der Analyse der Schwachstellen und Bedrohungen ist das Entdecken möglichst aller vorhandenen Schwachstellen und das Erkennen aller „wesentlichen“ Bedrohungen
- Bewertung der dadurch erkannten Risiken
 - Bewertung der aktuellen Risiken durch Bedrohungen hinsichtlich Schadenswirkung und Schadenshäufigkeit
- Festlegung geeigneter Sicherheitsmaßnahmen
 - Bestehende Schutzmaßnahmen hinsichtlich gefundener Schwachstellen und Bedrohungen bewerten und ggf. für die in der vorhergehenden Analyse als untragbar hoch erkannten Risiken zusätzliche Maßnahmen auswählen
- Ziel ist Prävention von, sowie (richtige) Reaktion auf Ereignisse

www.tuv.com



© TÜV Secure IT GmbH 2004



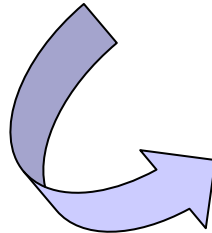
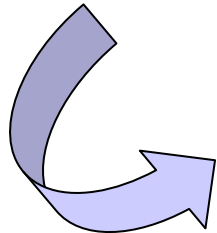
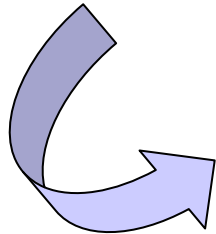
TÜV Rheinland Group

Bewertung des Sicherheitsniveaus anhand eines Kennzahlen-Systems

Risikoanalyse

Frage n-Nr.	Inhalt	Abzug	Eingabe Key-Fragen	Eingabe vertiefende Fragen	Bemerkungen
Risiken					
D1.01	Liegt eine angemessene Risikoanalyse vor?	KO-T	100	100	
D1.02	Werden in dieser Risikoanalyse die Schäden für das Geschäft unter Berücksichtigung des Verlusts von Vertraulichkeit, Integrität und Verfügbarkeit hinreichend bewertet?			100	
D1.03	Werden in dieser Risikoanalyse die Wahrscheinlichkeit des Eintritts des Bedrohungs-/Schadensfalls hinreichend berücksichtigt?			100	
D1.04	Ist der gesetzliche Rahmen identifiziert worden, der für die angemessene Durchführung der Geschäftsprozesse erforderlich ist?			100	
D1.05	Wurden die gesetzlichen Haftungsrisiken identifiziert und bei der Risikoeinstufung berücksichtigt?			100	
D1.06	Wurden die Schwachstellen jemals vollständig analysiert und daraus eine Sicherheitsstrategie entwickelt?		100	100	

Analyse der Bereiche



www.tuv.com



© TÜV Secure IT GmbH 2004

Ergebnis für vertiefende Fragen ohne KO-Faktor:	Gewichtung Key-Frage	Gewichtung vertiefende Fragen	Ergebnis Key-Frage (%)	Ergebnis vertiefende Frage (%)	KO-C?	KO-T?
A	70	10	70	10	0	0
A		20	0	20	0	0
		20	0	20	0	0
		20	0	20	0	0
	10	0				
	30	20	30			
	100	100	100			

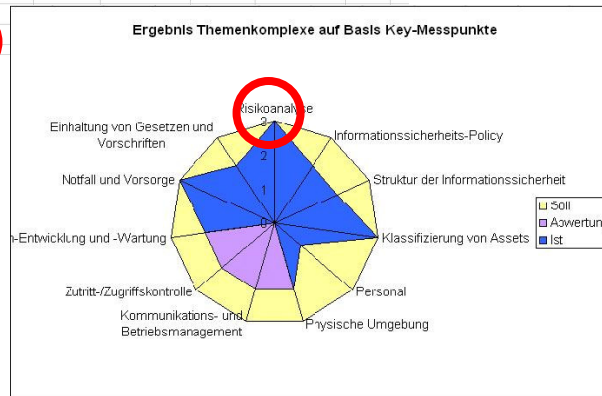
Gewichtung der Teilbereiche

Gewichtung der Themenkomplexe auf Basis von BS 7799

Risikoanalyse	Vorgehen (P)	Gewichtung (P)	Ergebnis für vertiefende Fragen ohne KO-Faktor	Ergebnis für vertiefende Fragen mit KO-Faktor	Ergebnis für Key-Fragen ohne KO-Faktor	Ergebnis für Key-Fragen mit KO-Faktor	Key-Frage (C)	Key-Frage (T)
Risiken	A	40	A	A	A	A	100,00	
RZ-Fragen/Wirtschaftlichkeit	A	40	A	A	A	A	92,00	
RZ-Versicherungen	A	20	A	B	D	D	88,00	
		100						

KO Container:

Ergebnis für vertiefende Fragen ohne KO-Faktor:	A
Ergebnis für vertiefende Fragen mit KO-Faktor:	A
Ergebnis für Key-Fragen ohne KO-Faktor:	A
Ergebnis für Key-Fragen mit KO-Faktor:	A

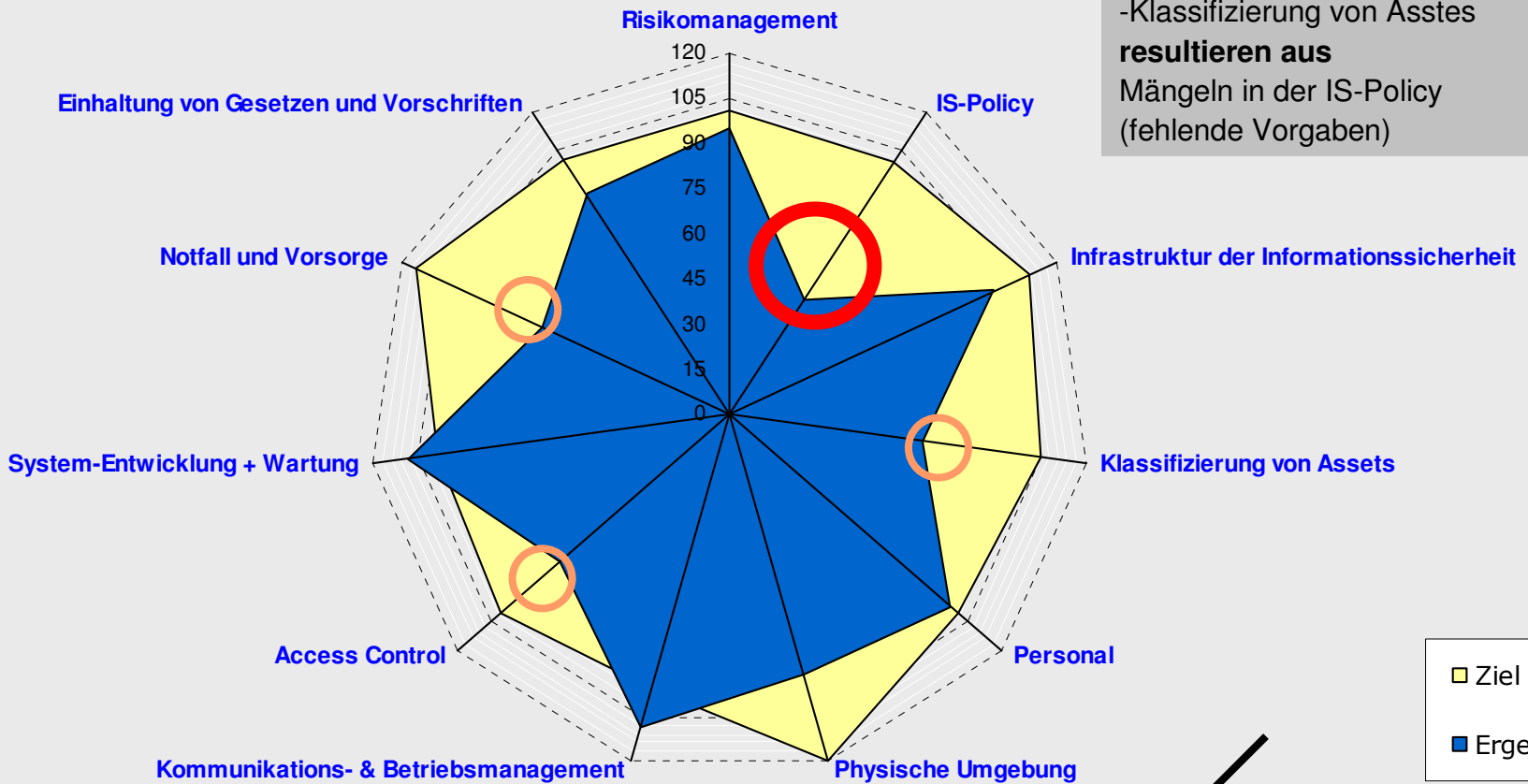


Kennzahl-Grafik mit Ist-Soll-Abgleich



TÜV Rheinland Group

■ Graphische Darstellung



www.tuv.com

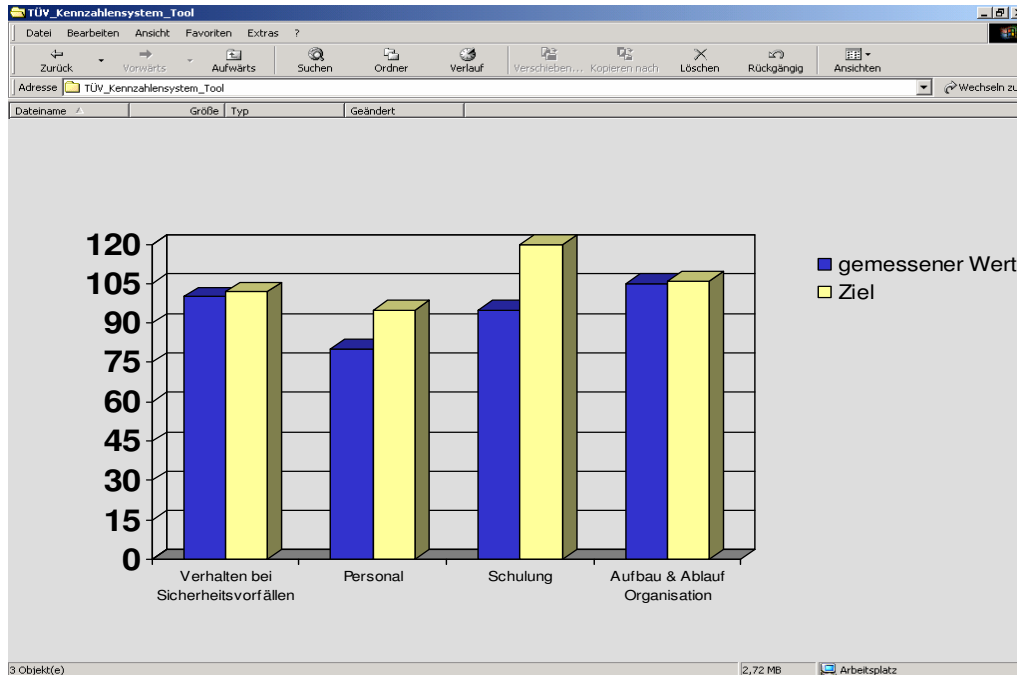


**Zielgerechter Einsatz limitierter Ressourcen
in den notwendigen Bereichen**

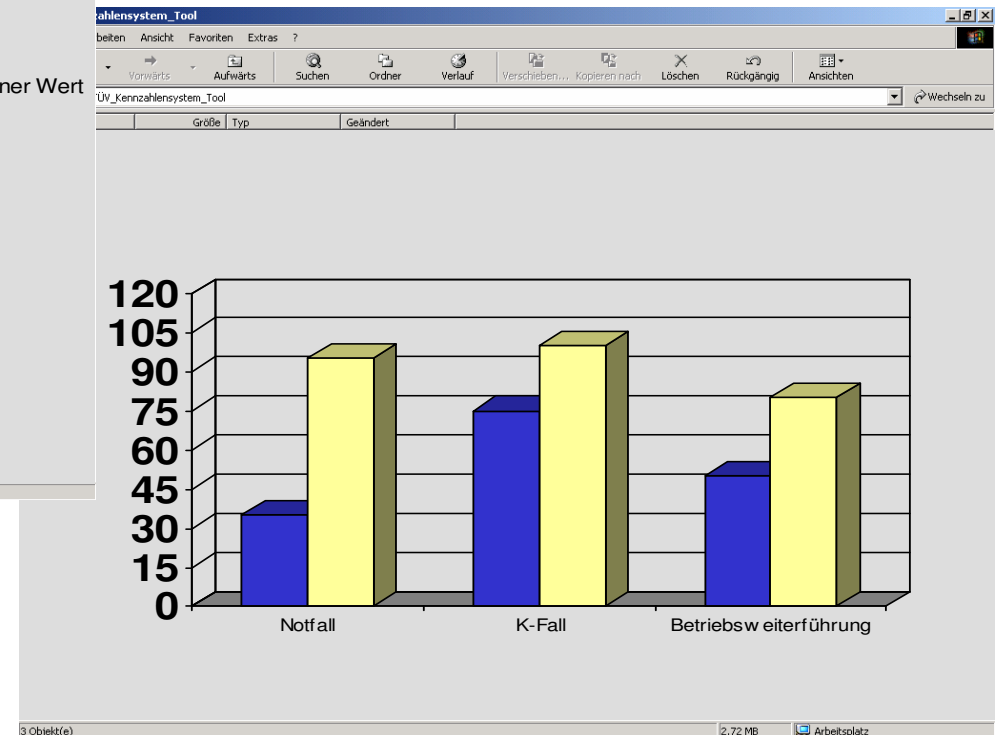
TÜV

TÜV Rheinland Group

Tiefergehende Ergebnisse



Beispiel: Personal



Beispiel: Notfall und Vorsorge

www.tuv.com

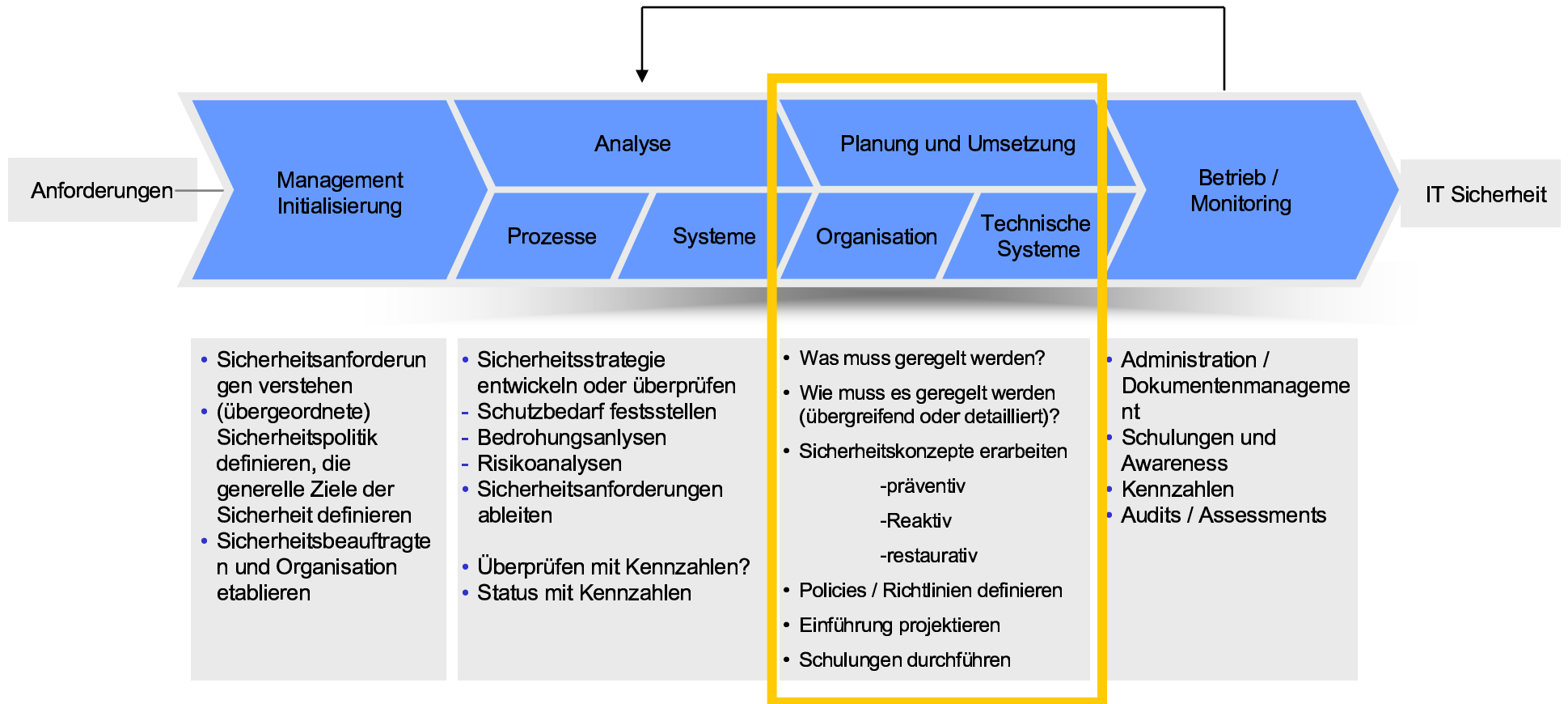


© TÜV Secure IT GmbH 2004



TÜV Rheinland Group

■ Der Implementierungsprozess für Security Policies

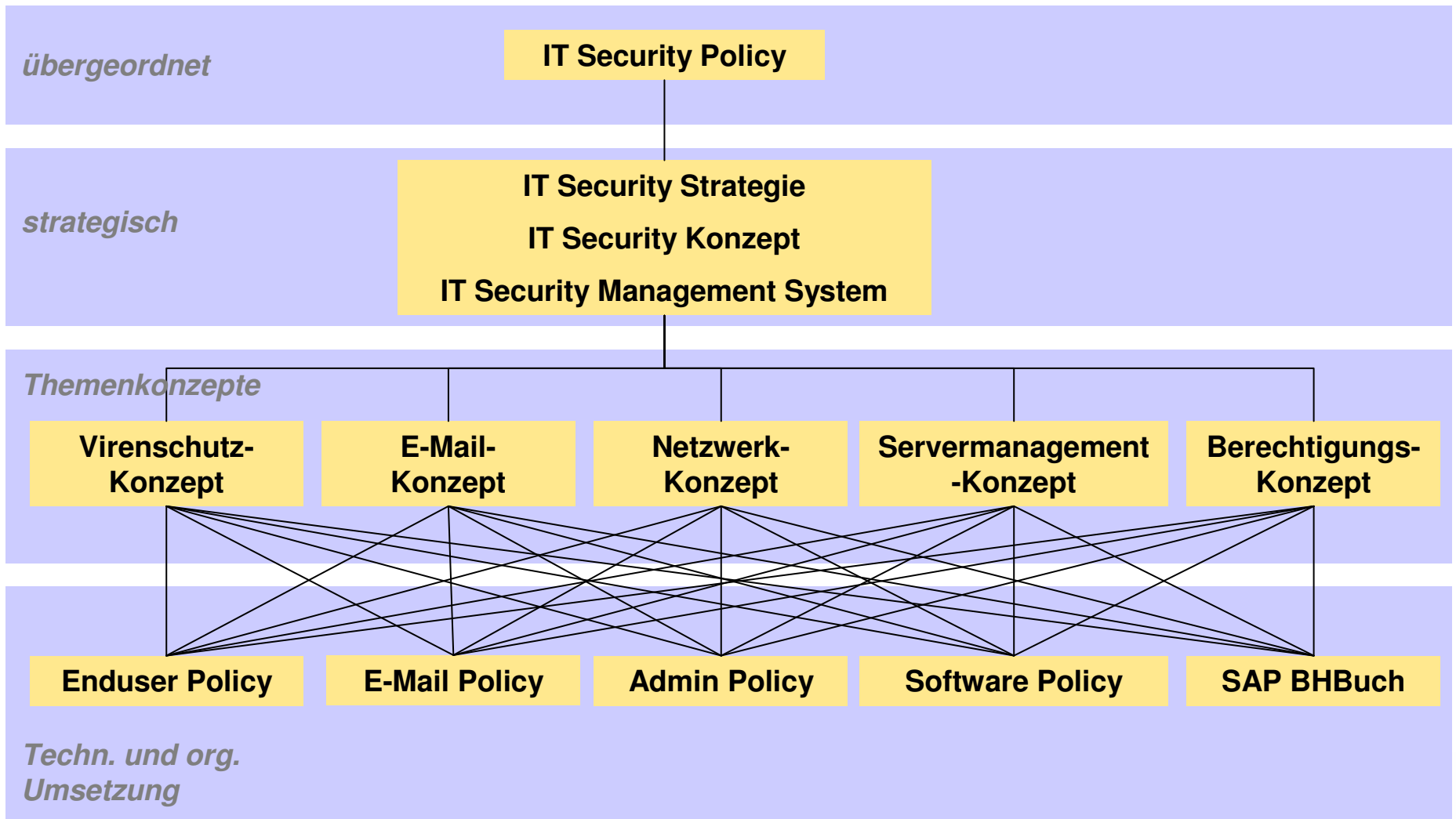


■ Sicherheitskonzepte /Policies

- Aus der Risikoanalyse ergibt sich als nächster Schritt die Erstellung eines Sicherheitskonzeptes zum sicheren Betrieb jedes Objektes.
- Ein Sicherheitskonzept enthält organisatorische und technische Maßnahmen:
 - **Präventive Maßnahmen**, die Gefahren bereits im Vorfeld vermeiden helfen
 - **Überwachende Maßnahmen**, die Angriffe und Ereignisse erkennen und sie ggf. schon abwehren, berichten, dokumentieren
 - **Reaktive Maßnahmen**, die nach Eintritt der Bedrohung die Folgen minimieren können



■ Generisches Policy-Modell



■ Auswahl Themenkonzepte

- Anti Virus Konzept
- E-mail Konzept
- Firewall-Zonen Konzept
- Dialin Konzept
- Netzwerk Konzept
- Authentisierungs- und Rechtekonzept / PKI Konzept
- Serverbetriebskonzept
- Client Konzept
- Versorgungskonzept (Klima, Energie)
- Maintenance (Hardware- / Softwarewartung)
- Betrachtung rechtlicher Aspekte
- Entsorgungskonzept

www.tuv.com



© TÜV Secure IT GmbH 2004



TÜV Rheinland Group

■ Auswahl Organisatorische Policies / Anweisungen

- **Datenschutz Policy**
- **End-User Policy**
- **Dokumenten Klassifizierung**
- **Software Policy**
- **Backup Policy und Archivierung**
- **Operator Policy**
- **Netzwerk Policy**
- **Server Component Policy**
- **Beschaffung & Support**
- **Firewall Policy**
- **Incident und Problem Management / Reporting**
- **Desaster Recovery Policy**
- **Telekommunikations Policy**
- **User Administration Policy**
- **ICM Policy (Installation und Konfigurations Management)**
- **Roaming User / Heimarbeitsplätze / Partner Netzwerke**



■ Auswahl technische Umsetzung / Betriebshandbücher

- Technische End-User Policy
- Berechtigungen: Nachweise des Lebenszyklus und dessen Pflege
- Serverbetrieb
- Firewallbetrieb
- Betrieb Antiviren
- ...

www.tuv.com



© TÜV Secure IT GmbH 2004



TÜV Rheinland Group

■ Beispiel 1: E-Mail Konzept / Policy

Inhaltsverzeichnis:

- 1 Die Bedeutung der sicheren e-Mail
- 2 Regeln für den Benutzer.....
 - 2.1 Nutzung.....
 - 2.2 Schutzbedürftige Informationen.....
 - 2.3 Unternehmensschädigende oder gesetzeswidrige Inhalte
 - 2.4 Ausführbare Dateien.....
 - 2.5 Sichern empfangener Attachments
 - 2.6 Bereinigen des Posteingangs.....
 - 2.7 Reduzierung der Server- und Netzwerke.....
- 3 Betrieb des e-mail Systems.....
 - 3.1 Plattform.....
 - 3.2 Einweisung in e-mail-Client
 - 3.3 Personal
 - 3.4 begrenzter Speicherplatz
 - 3.5 Größe von e-mails.....
 - 3.6 Virenschutz.....
- 4 Regeln auf Anwendungsebene
- 4.1 Zugangsschutz.....
- 4.2 kein Weiterleiten von e-Mails an private Mail- Adressen.....
- 4.3 Einsatz kryptographischer Verfahren.....
- 5 weitere Regeln zum fachgerechten Umgang mit e-Mail
- 5.1 keine langfristige Archivierung von Nachrichten.....
- 5.2 Namenskonvention für e-mail-Adressen
- 6 Referenzierte Dokumente

3.1 Plattform

Als e-mail-System wird einheitlich für das ganze Unternehmen das Produkt lotus notes eingesetzt. Die Anweisungen für Betrieb und Konfiguration des mail-Servers sind im Themenkonzept Server-Betrieb [Ser_K] und der Detailpolicy „Betrieb Lotus Domino“ [LD_P] zu entnehmen. Der e-mail-Server ist gemäß [FW_K] in das Firewall-Konzept des Unternehmens einzubeziehen.

Die Qualität und Angemessenheit der eingesetzten Softwareplattform für das e-mail-System wird regelmäßig überprüft und neu bewertet. Richtlinien für die Bewertung, Beschaffung und Einführung von Software sind durch das Themenkonzept Software-Management [SW_K] geregelt.

Der Mail-Server wird gesichert (in einem Serverraum oder Serverschrank) gemäß der Detailpolicy „Aufstellen von Hardware“ [HWI_P] untergebracht.

4.3 Einsatz kryptographischer Verfahren

Alle als „vertraulich“ eingestufte Dokumente sind vor dem Versand per e-mail zu verschlüsseln. Die Maßgabe zur Einstufung der Dokumente obliegt dabei dem jeweiligen Fachvorgesetzten. Zur Verschlüsselung werden ausgewiesene Standardprodukte eingesetzt, die die Verschlüsselung von Dateien vor dem Versand per e-Mail ermöglichen. Hier sollen grundsätzlich nur Produkte mit starker Verschlüsselung ausgewählt werden.

Alle als „kritisch“ eingestuft Dokumente sind vor dem Versand per e-mail zu signieren. Die Maßgabe zur Einstufung der Dokumente obliegt dabei dem jeweiligen Fachvorgesetzten. Zur Signatur werden ausgewiesene Standardprodukte eingesetzt, die die Signatur von Dateien vor dem Versand per e-Mail ermöglichen

Die Qualität/Stärke der Verfahren ist über die Zeit hinweg jeweils neu zu bewerten. Konkrete Anleitungen hierzu finden sich im Themenkonzept PKI [PKI_K] sowie in der Detailpolicy „Einzelarbeitsplatz“ [EA_P] bzw. „Server Betrieb“ [Ser_K].

www.tuv.com



■ Beispiel 2: Laptop Policy

Inhaltsverzeichnis:

1	Einleitung und Überblick.....
2	Geltungsbereich
3	Bedrohungen und Schutzbedarf.....
3.1	Allgemeine Bedrohungen.....
3.2	Spezielle Bedrohungen durch die Verwendung des Internet als Verbindungsmedium.....
3.3	Typische Angriffsszenarien.....
4	Grundsätzliche Regeln für den Benutzer.....
4.1	Nutzung.....
4.2	Schutzbedürftige Informationen.....
4.3	Unternehmensschädigende oder gesetzeswidrige Inhalte.....
4.4	Ausführung von Programmen & Ausführbare Dateien.....
4.5	Behandlung von Daten und Datenträgern.....
4.6	Umgang.....
5	Regeln für Konfiguration und Installation.....
5.1	Verschlüsselung.....
5.2	Anbindung.....
5.3	Sonstiges.....
6	Standard Konfiguration / Installation.....
6.1	Grundsätzliche Regeln / Hardware.....
6.2	Anwendungen / Software.....
6.3	Sonstige Regelungen.....
7	Referenzierte Dokumente.....

4.5 Behandlung von Daten und Datenträgern

Drucken von Dokumenten:

- Unterlagen, etc. außerhalb der **Firma XYZ** ist grundsätzlich verboten.

Lokale Speicherung:

- Administratoren Laptop: Das lokale Speichern von Informationen ist grundsätzlich verboten
- Präsentationen: Lokale Speicherung ist zulässig, Datei und/oder Speicherbereich muss entsprechend dem Schutzbedarf der Informationen angemessen geschützt sein.
- Lokale Speicherbereiche sind in regelmäßigen Abständen zu löschen um die ungewollte Anhäufung sensibler Informationen auf mobilen Arbeitsplätzen zu verhindern.

Unterlagen / Dokumente:

- Dokumente sind sicher zu vernichten (Schredder). Entstehender Abfall ist angemessen sicher zu entsorgen.
- Die Übertragung auf Systeme Dritter ist grundsätzlich verboten. Dies betrifft sämtliche möglichen Übertragungsformen, also auch: FD, IR, USB, Firewire, PCMCIA, Email, Netzwerk und alle weiteren nicht aufgeführten, externen Speichermedien, Computer, etc.

6.2.1 Virenschutz

Emails mit ausführbaren Attachments oder bestimmten Subjects werden aus dem e-Mail-Verkehr herausgefiltert, um die Ausbreitung von Computerviren zu verhindern.

Der Viren-Scanner darf nicht durch den Benutzer abschaltbar sein.

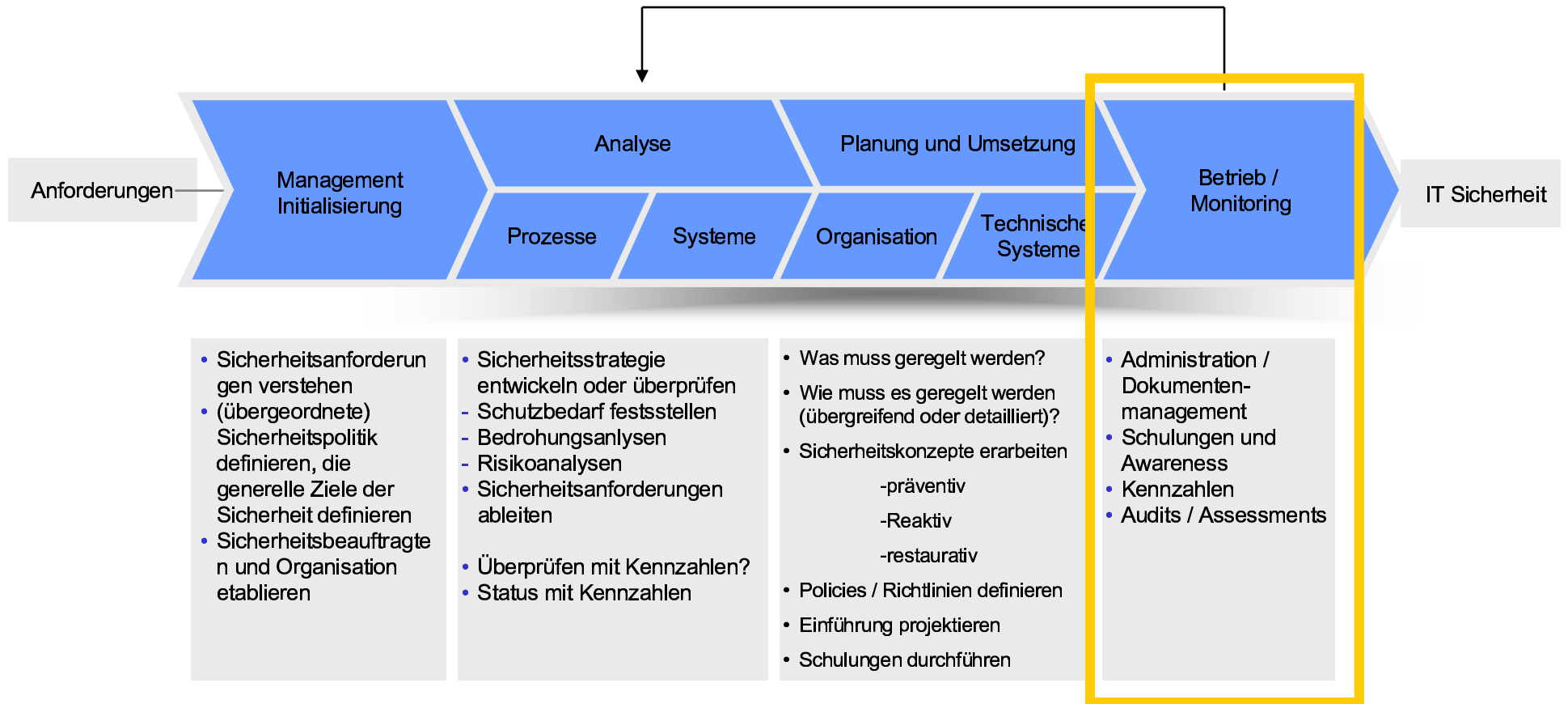
Alle Schreib- und Lesevorgänge werden überwacht.

Der Virens Scanner muss den Inhalt aller Dateien unabhängig von der Dateilendung prüfen.

Siehe außerdem das Themenkonzept „Virenschutz“ [VS_IQ].



■ Der Implementierungsprozess für Security Policies



■ Beispiel: Awareness durch E-Learning

- Entwicklung eines E-Learning-Tools zur IT-Sicherheit
- Ziel: Steigerung des Informationssicherheitsbewusstseins der Anwender von IT-Systemen
- Lerneinheiten:
 - Informationen
 - Arbeitsplatz
 - Passwörter
 - E-mail und Internet
 - Telefonieren
 - Unbekannte Personen



■ Inhalte E-Learning am Beispiel „Informationen“ und „Internet“

■ Lerneinheit: Information

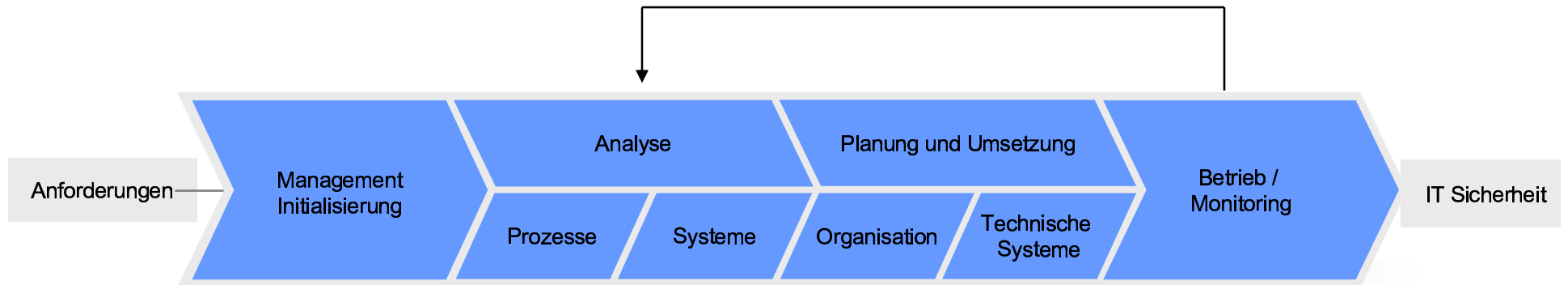
- Bedeutung von Informationen
- Arten von Informationen
- Schutzziele
- Verantwortung für Informationssicherheit
- Sicherheitsvorfälle

■ Lerneinheit: E-Mail und Internet

- Sicherer Gebrauch von E-Mails
 - Umgang mit eingehenden E-Mails (Gefahren, Risiken, Folgen)
 - Umgang mit dem Versand von E-Mails
- Sicherer Gebrauch von Internet



■ Der Implementierungsprozess für Security Policies



- Sicherheitsanforderungen verstehen
- (übergeordnete) Sicherheitspolitik definieren, die generelle Ziele der Sicherheit definieren
- Sicherheitsbeauftragte n und Organisation etablieren

- Sicherheitsstrategie entwickeln oder überprüfen
 - Schutzbedarf feststellen
 - Bedrohungsanalysen
 - Risikoanalysen
- Sicherheitsanforderungen ableiten
- Überprüfen mit Kennzahlen?
- Status mit Kennzahlen

- Was muss geregelt werden?
- Wie muss es geregelt werden (übergreifend oder detailliert)?
- Sicherheitskonzepte erarbeiten
 - präventiv
 - Reaktiv
 - restaurativ
- Policies / Richtlinien definieren
- Einführung projektieren
- Schulungen durchführen

- Administration / Dokumentenmanagement
- Schulungen und Awareness
- Kennzahlen
- Audits / Assessments



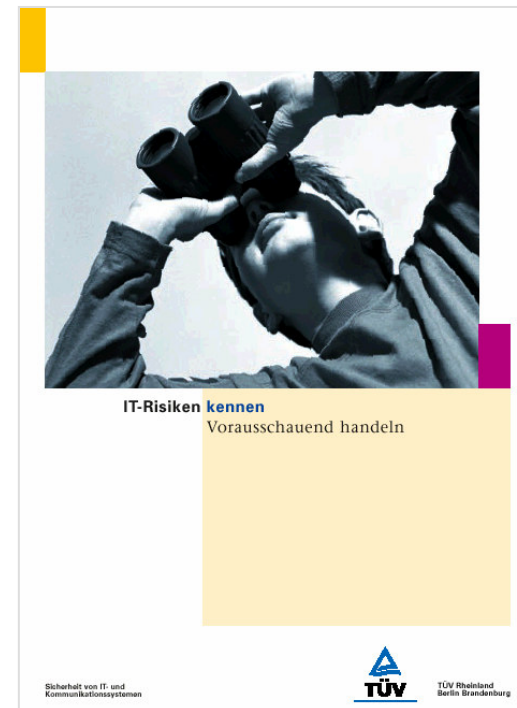
■ Zusammenfassung

- Security Policies sind ein wesentlicher Baustein eines umfassenden Sicherheitssystems
- Sie müssen verbindlich sein und dürfen nur wenig Interpretationsspielraum lassen
- Das Policy System sollte modular sein und „lebt“, d.h. es muss aktuell gehalten werden
- Konkrete, handlungsleitende Informationen erleichtern die Etablierung
- Regelmäßiges Monitoring unterstützt die Umsetzung und gibt Feedback für notwendige Anpassungen
- Konsequenzsysteme und Sanktionen müssen vorhanden sein und angewendet werden

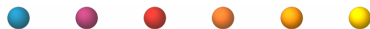


■ Vielen Dank.

- Haben Sie Fragen?
- Detlev Henze,
■ Geschäftsführer
- TÜV Secure iT GmbH
- Am Grauen Stein
- 51105 Köln
- 0221 – 806 33 14
- henze@de.tuv.com



www.tuv.com



© TÜV Secure iT GmbH 2004



TÜV Rheinland Group