Sicherheitsmanagementsysteme
- Integrierte Managementsysteme

BSI IT-Sicherheitskongress
Bonn 13.05.2003

Jürgen Herrmann

Vorgeschichte

Ziele

Strategie/Maßnahmen

Organisation/Prozesse

Was hat das Ganze eigentlich mit IT-Sicherheit zu tun?

Umsetzung/Ergebnisse

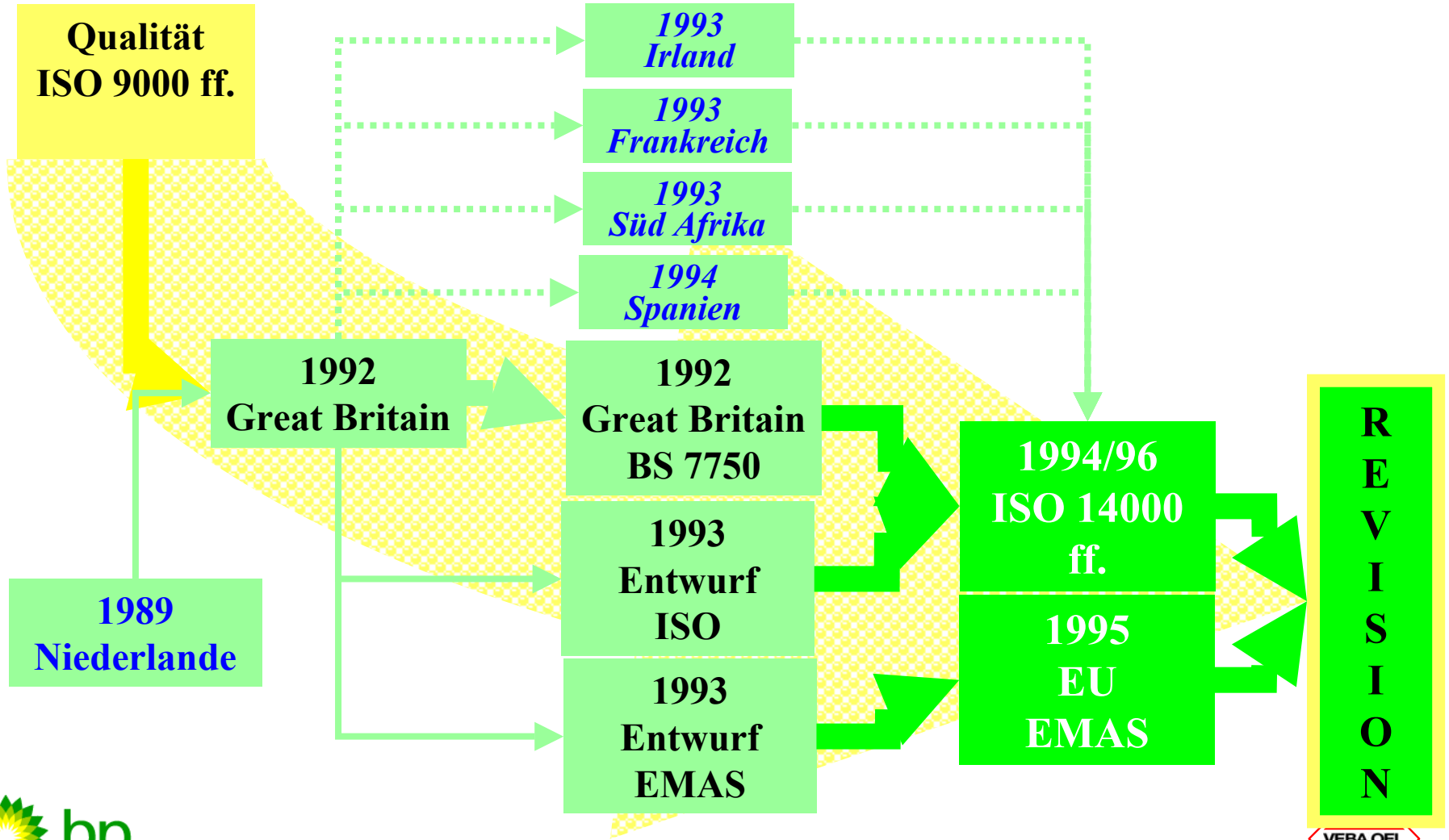
Zusammenfassung/Fragen

Wettbewerb erzwingt Qualitätsmanagement

In der Mineralölindustrie in Deutschland sind 1995 alle großen Gesellschaften nach DIN EN ISO 9001 oder 9002 zertifiziert:

1992	**Shell**
1993	**BP**
1993	**DEA**
1993	**Esso**
1993	**Mobil**
1993	**ÖMV**
1993	***ERN, OMW, ARAL***
1994	***Veba Oel-Zentrale, PCK, WGG***

Umweltschutz- und Qualitätsnormung
... eine Geschichte voller Mißverständnisse?



Anforderungen der Störfall-Verordnung an Unternehmen

Allgm. Vorschriften
§ 1 Anwendungsbereiche
§ 2 Begriffsbestimmungen

Vorschriften für Betriebsbereiche

Grundpflichten
§§ 3 - 8

Erweiterte Pflichten
§§ 9 - 12

Behördenpflichten
§§ 13 - 16

Vorschriften für bestimmte genehmigungsbedürftige Anlagen nach BImSchG

Gemeinsame Vorschriften Schlußvorschriften
§§ 19-21

Anhang I	Anhang II	Anhang III	Anhang IV	Anhang V	Anhang VI	Anhang VPI
Anwendung	Sicherheitsbericht	**Sicherheitskonzept und Sicherheitsmanagementsystem**	AGAP‘s	Information an die Öffentlichkeit	Meldungen	
					Teil 1 Kriterien	Teil 1 Stoffliste § 1 (3)
					Teil 2 Inhalte	Teil 2 Anlagen § 1 (3) Nr. 2
						Teil 3 Anlagen § 1 (3) Nr. 1

Vorgeschichte

Ziele

Strategie/Maßnahmen

Organisation/Prozesse

Was hat das Ganze eigentlich mit IT-Sicherheit zu tun?

Umsetzung/Ergebnisse

Zusammenfassung/Fragen

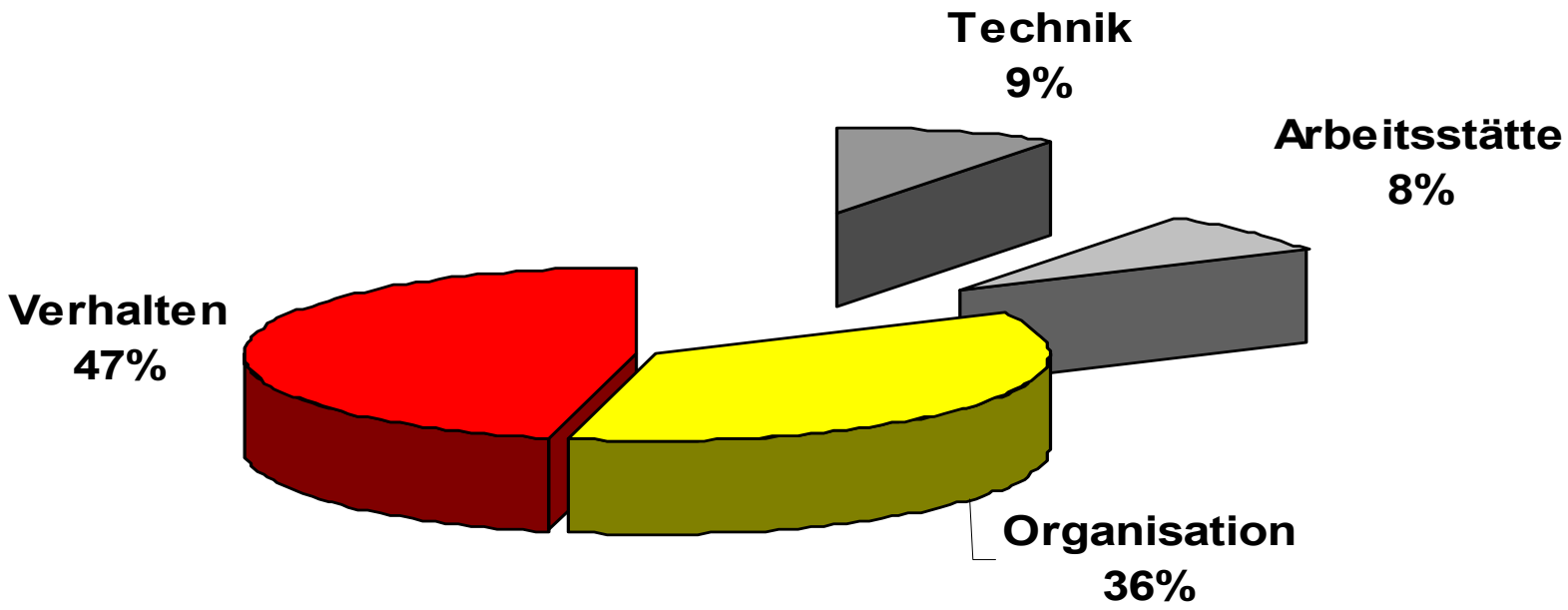
Verbesserung der Sicherheit durch System(sicherheit)?

Seveso 2 (Council Directive 96/82/EC)

(15) „ ... analysis of the major accidents reported in the Community indecates that the majority of them are results of *managerial and/or organizational shortcommings*; ... It is therefore necessary to lay down at Community level basic principles for *management systems* ...“

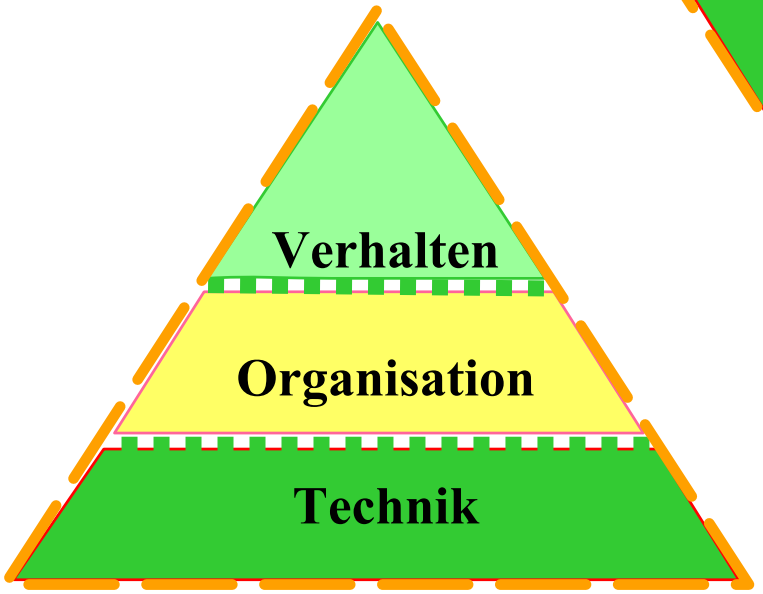
Die Hauptursache für tödliche Arbeitsunfälle liegt bei organisatorischen Mängeln und Verhaltensfehlern!

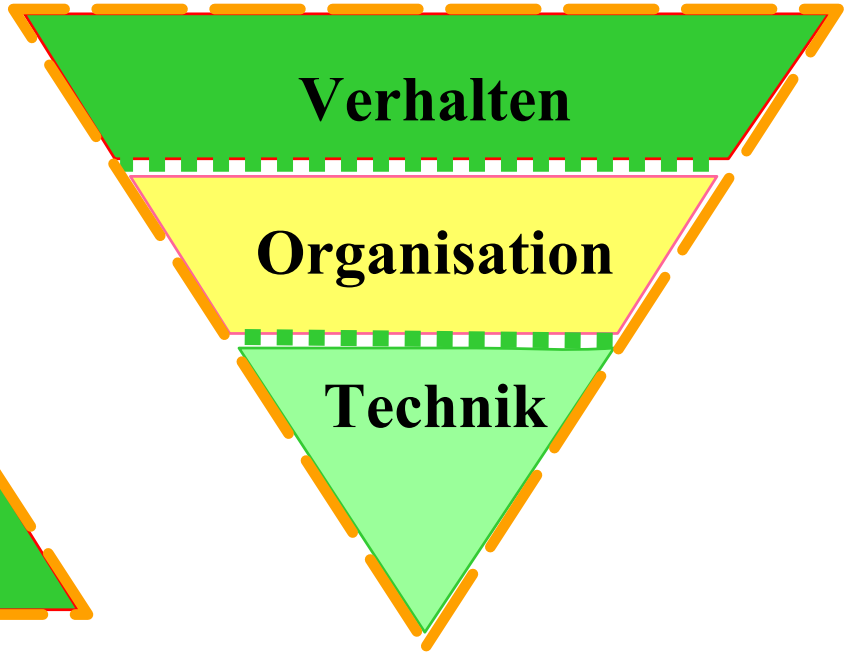
Sicherheitsbericht Deutschland 1999
1167 tödliche Unfälle in 1999
URSACHEN



Bundesarbeitsblatt 4/2001:

Wo liegt der Fokus?





Paradigmenwechsel im Denken der Organisationen?

Altes Denken	Neues Denken
• Unternehmen = Maschine	• Unternehmen = Organismus
• Technokratisches Denken	• Ganzheitliches Denken *(in Systemen)*
• Denken in Funktionen und Zuständigkeiten	• Denken in Prozessen
• Perfekte Organisation *(Bürokratie)*	• Selbstorganisation *(Verantwortung auf niedriger Ebene)*
• Komplexität wird beherrscht	• Komplexität wird geleitet
• Mensch als System-"Bediener"	• Mensch als Entscheider

Ziel = Verhaltensänderung
Strategie = Organisationsänderung (Managementsysteme)

Wenn die Ursache für die *Nichterreichung von Zielen in der Hauptsache im menschlichen Verhalten begründet* ist, so gilt es, das Verhalten der Menschen in einer Organisation zu ändern, und dies nachhaltig!

Die notwendige *Strategie* lautet:
Neue Strukturen schaffen ein neues Verhalten!

Was ist den Mitarbeitern von Veba Oel am Qualitätsmanagement besonders wichtig?

Eine Auswahl aus Antworten von ca. 100 MA WGG 1994

1. Klarheit und Offenheit schaffen:

"Die Festlegung von Schnittstellen und Zuständigkeiten, bisherige Grauzonen wurden aufgedeckt und transparent."

"Die eindeutige Dokumentation von Verantwortlichkeiten, die traditionell bei VO nur unzureichend dokumentiert ist."

2. Klare Regelungen schaffen Verbesserungen:

"Rückverfolgbarkeit von Arbeitswegen und Produktwegen."

"Die Arbeitsabwicklung ist nachvollziehbar und nachweisbar."

"Bessere Koordination der Arbeiten zwischen den Bereichen."

Vorrangige Ziele der dokumentierten Integrierten Managementsysteme von Veba Oel

- **Die Informationen und Dokumente müssen von den Mitarbeitern vor Ort verstanden und akzeptiert werden.**

- **Die Informationen und Dokumente müssen vor Ort vollständig und handhabbar sind.**

- **Die Informationen und Dokumente sollen vor Ort als praktikable Werkzeuge zur Verfügung stehen und Hilfen bei der Bewältigung der anstehenden Arbeiten und Probleme leisten.**

Managementsysteme können nur im Konsens aufgebaut werden!

Click to add Title

Vorgeschichte

Ziele

Strategie/Maßnahmen

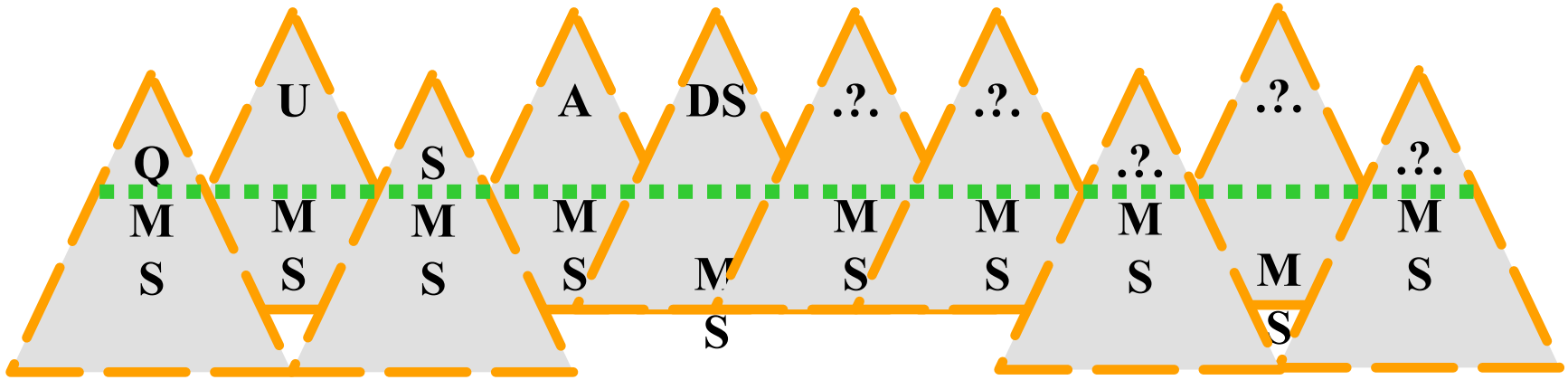
Organisation/Prozesse

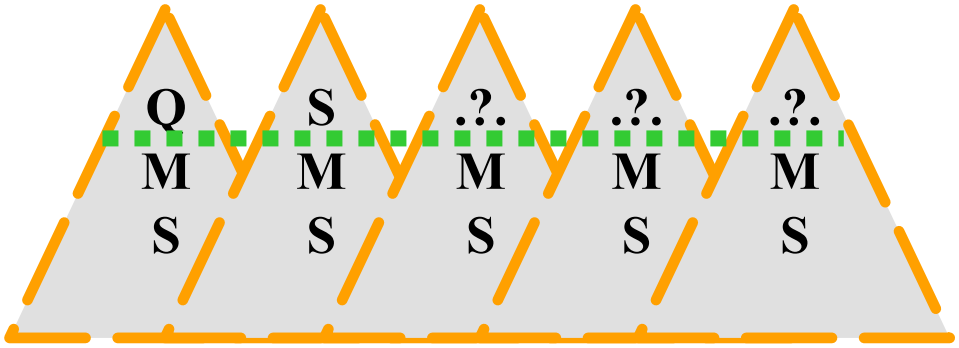
Was hat das Ganze eigentlich mit IT-Sicherheit zu tun?

Umsetzung/Ergebnisse

Zusammenfassung/Fragen

Integration von Managementsystemen





„Zipfel-Modelle“ nach Dr. Adams

„Gemeinsamkeiten vor die Klammer ziehen“

Charakter:

Unveränderte, bestehende Organisationen

- **Teilsysteme nebeneinander**
- **Vernetzung auf der Dokumentenebene**

Vor-/Nachteile:

Standardisiertes, gemeinsames Handbuch

- **Integration nur bis zu einem bestimmten Grad**

Geringe Kommunikation

- **Keine Einbeziehung der Mitarbeiter**
- **Motivations- und Wissenspotentiale nicht umfassend genutzt; Beauftragte wirken durch Anweisungen und formale Machtbefugnisse**

Widerstand gering/Veränderungsbereitschaft eher vorhanden!

Ganzheitliche, Prozeßorientierte Organisation

Charakter:

Ziel ist ständiges Lernen und Verbesserung

- **Zielorientierung der Prozesse**
- **Prozesse bilden Integrationsebene**
- **Know-How Basis der Integrationsgebiete wird aktiv genutzt**

Vorteile/Nachteile:

Oberste Führungskreis wird intensiv gefordert

- **Neue Führungsaufgaben**

Hierarchieübergreifende Mitarbeiterbeteiligung

- **Mitarbeiter in Prozeßteams**

Integration in der täglichen Praxis

- **Praxisgerechte Dokumentation**

Offenes, veränderungstolerantes System

Widerstand groß/Veränderungsbereitschaft eher nicht vorhanden!

Was ist ein Managementsystem?

Managementsysteme beschreiben die *Aufbau- und Ablauforganisation* eines Unternehmens.

Managementsysteme definieren das Unternehmen nach innen und außen.

Managementsysteme sind Werkzeuge/Mittel zur *zielgerichtet*en Steuerung/Lenkung von Unternehmen.

Konsequenzen:
***Unternehmensziele* müssen vorhanden sein!**

Managementsysteme umfassen/betreffen das *gesamte Unternehmen*.

Was ist typisch für ein Managementsystem?

Managementsysteme definieren die Aufbau- und Ablauforganisation eines Unternehmens nach innen und außen.

Ziel der Beschreibung in Managementsystemen ist die eindeutige Festlegung von Verantwortlichkeiten und organisatorischen Schnittstellen.

Besondere *Merkmale von Managementsystemen* sind:

- **die Selbstkontrolle (Audit)**
- **das Lernen aus Fehlern (Korrekturen)**
- **die Vermeidung möglicher Schwachstellen (Vorbeugung)**
- **der kontinuierliche Verbesserungsprozeß (KVP)**

Welche Anforderungen muss ein Managementsystem erfüllen?

Zukunftsorientierung

Wie innovativ und flexibel ist ein Management-system gegenüber aktuellen und zukünftigen Herausforderungen von innen und außen?

Zielorientierung

Wie effizient ist eine Managementsystem bei der Verwirklichung der Unternehmensziele?

Prozeßorientierung

Wie effizient ist ein Managementsystem zur Steuerung/Lenkung/Führung der Unternehmensprozesse?

Kunden
Mitarbeiter
Öffentlichkeit

Gewinnorientierung

Schafft ein Managementsystem Unternehmenswerte?

Perspektiven von Managementsystemen_Prozeß-Orientierung

Führungsprozesse

Unternehmensgrundsätze und -Ziele
Unternehmensorganisation
Controlling/Audits und Revision/Review
Korrigierende und Vorbeugende Maßnahmen

Wertschöpfungsprozesse

Produktion, Instandhaltung, Logistik,
Ein-/Verkauf usw., Dienstleistungen

Unterstützungsprozesse

Organisationsentwicklung
Dokumentation und Information
Information und Training
Durchführung von Audits

Prozess Landschaft 3*: Raffinerie

Management Prozesse

- Unternehmensentwicklung
- KVP
- Risikomanagement und Vorsorge

Kernprozesse

- Verarbeitung
- Logistik
- *Kunden-orientierte Prozesse* → *werden durch die Vertriebsabteilungen aufrechterhalten*

Support Prozesse

- Personal
- IT-Management
- Einkauf
- Controlling
- Labor
- Projekt Management
- Umweltschutz Management
- Kommunikation

*ohne Teilprozesse

Vorgeschichte

Ziele

Strategie/Maßnahmen

Organisation/Prozesse

Was hat das Ganze eigentlich mit IT-Sicherheit zu tun?

Umsetzung/Ergebnisse

Zusammenfassung/Fragen

1995: ZWEI Handbücher beschreiben das Managementsystem

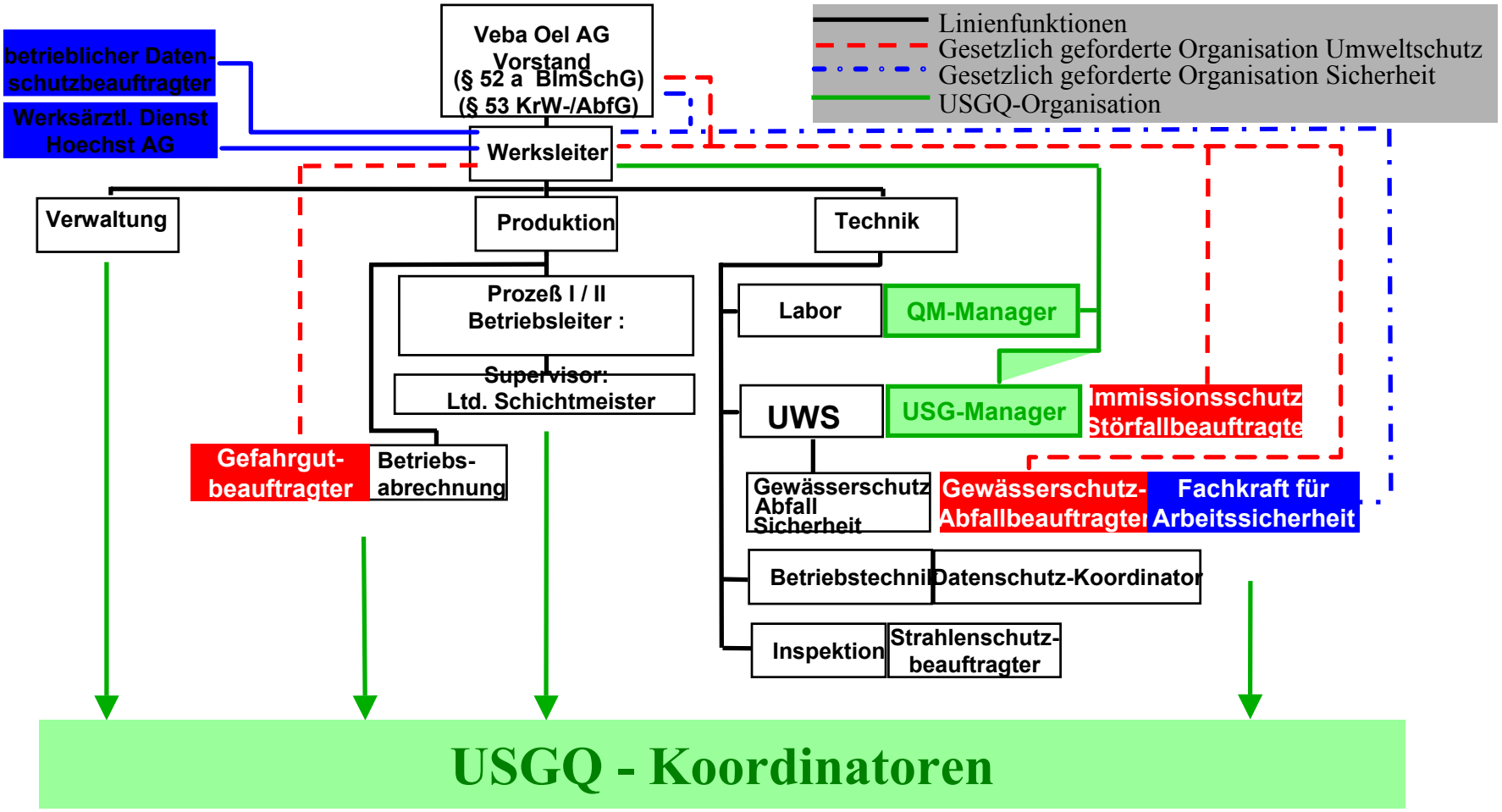
USGQ-Managementhandbuch

01	Unternehmensdarstellung
02	USGQ-Grundsätze und –Ziele
03	USGQ-Managementsystem
04	Dokumentation
05	Organisation und Kommunikation
06	Schulung, Unterweisung und Training
07	KVP, Korrekturmaßnahmen, Audits und Review
08	Umweltauswirkungen
09	Vorsorgemaßnahmen
10	Gesundheitsvorsorge
11	Standortübergreifende Geschäftsprozesse

USGQ-Managementhandbuch Produktion

P01	USGQ-relevante Anforderungen an Verfahren und Produkte
P02	Produktionsplanung und Ablauf
P03	Qualität und Freigabe von Produkten
P04	Handhabung, Lagerung und Transport von Produkten

USGQ-Organisation



Rolle der „§-Beauftragten“ in Managementsystemen

Früher?

Sachverwalter von § § § und innerbetriebliche Vollzugshilfe

Stark ausgeprätes Bedürfnis nach Sicherheit
- Kontrollen

Mißtrauen:
- geringe Glaubwürdigkeit
- Distanz zu Mitarbeitern
- geringe Risikobereitschaft

Individuelle Aktionen
- Information ist Macht

Zukünftig?

Berater und Systemmanager

Neugier
- Immer neue Lösungen finden
- Experimentieren

Vertrauen:
- Glaubwürdigkeit
- Nähe zu Mitarbeitern
- Innovationsklima

Teamarbeit
- Projektmäßige Arbeit
- Gegenseitiges Commitment

Dafür bringen sie gute Voraussetzungen mit:

Umwelt-Beauftragte	= Rechts- und Behördenexperten
Datenschutz, -sicherheit	= Rechts- und Behördenexperten
Unternehmenssicherheit	= Kontakte zu „Diensten“
Sicherheitsfachkraft	= Arbeitsexperte vor Ort
Arbeitsmediziner	= Persönlicher Berater vor Ort
Qualitäter	= Systemexperten

EIN ... USGQ-Audit untersucht das Managementsystem systematisch

Werden die USGQ-Regeln eingehalten?

Stimmen IST-Werte (Nachweis in Aufzeichnungen) mit SOLL-Vorgaben (Dokumentiert in Dokumenten: Handbüchern, Richtlinien, Verfahrensanweisungen, Arbeitsanweisungen usw.) überein?

Sind die USGQ-Regeln sinnvoll und angemessen?

- **Können die Regeln eingehalten werden?**
- **Was muß an den Regeln verändert werden?**
- **Was kann verbessert werden?**

Ein gemeinsames USGQ-Audit wird durchgeführt:

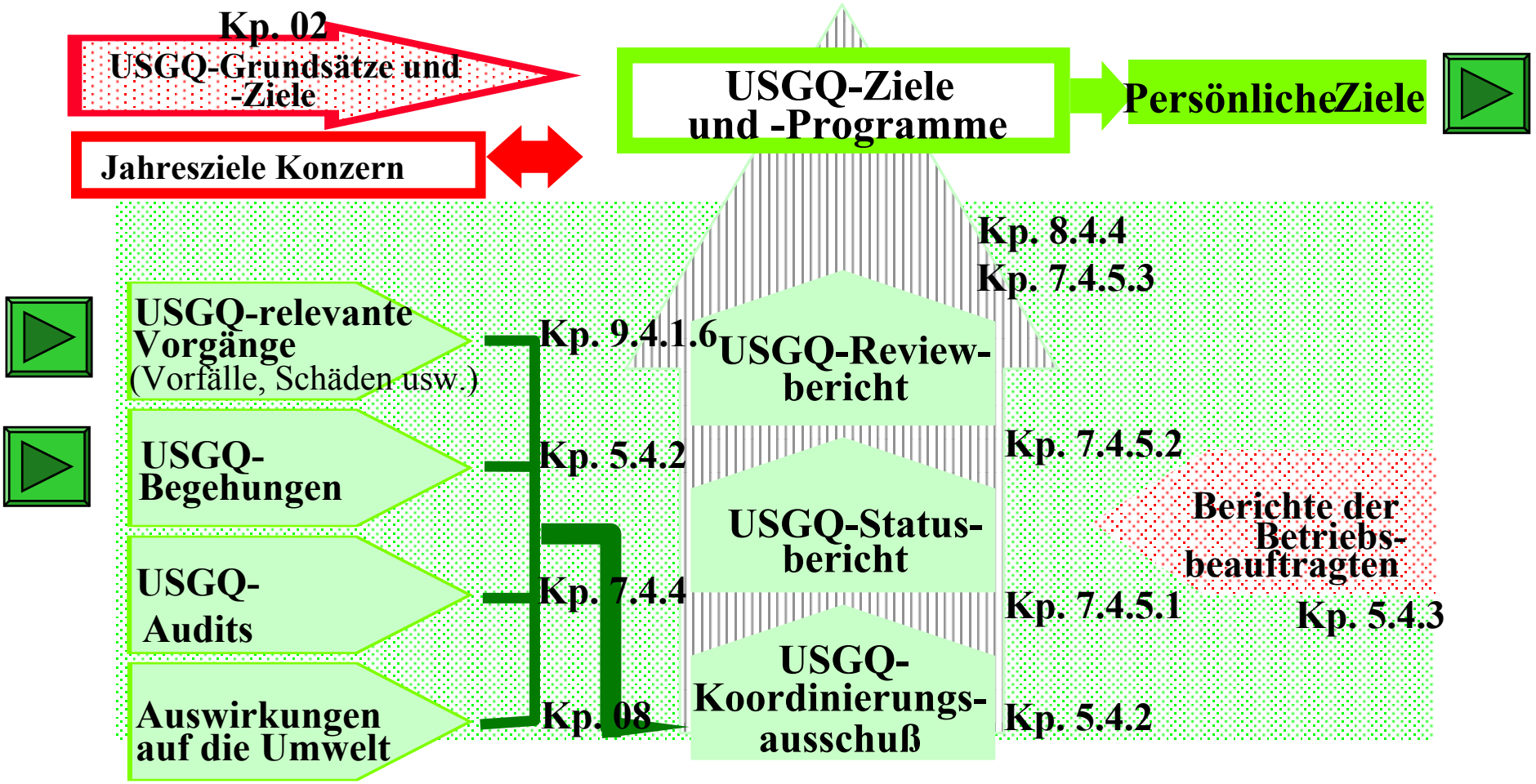
Ein Audit-Schwerpunkt, U S G oder Q, wird festgelegt.

Auditoren geben Kommentare um Verbesserungsmöglichkeiten anzusprechen.

Auditoren vereinbaren Korrekturmaßnahmen um Abweichungen abzustellen,

Kommentare und Korrekturmaßnahmen werden im Auditbericht dokumentiert.

Kontinuierliche Verbesserung



Click to add Title

Vorgeschichte

Ziele

Strategie/Maßnahmen

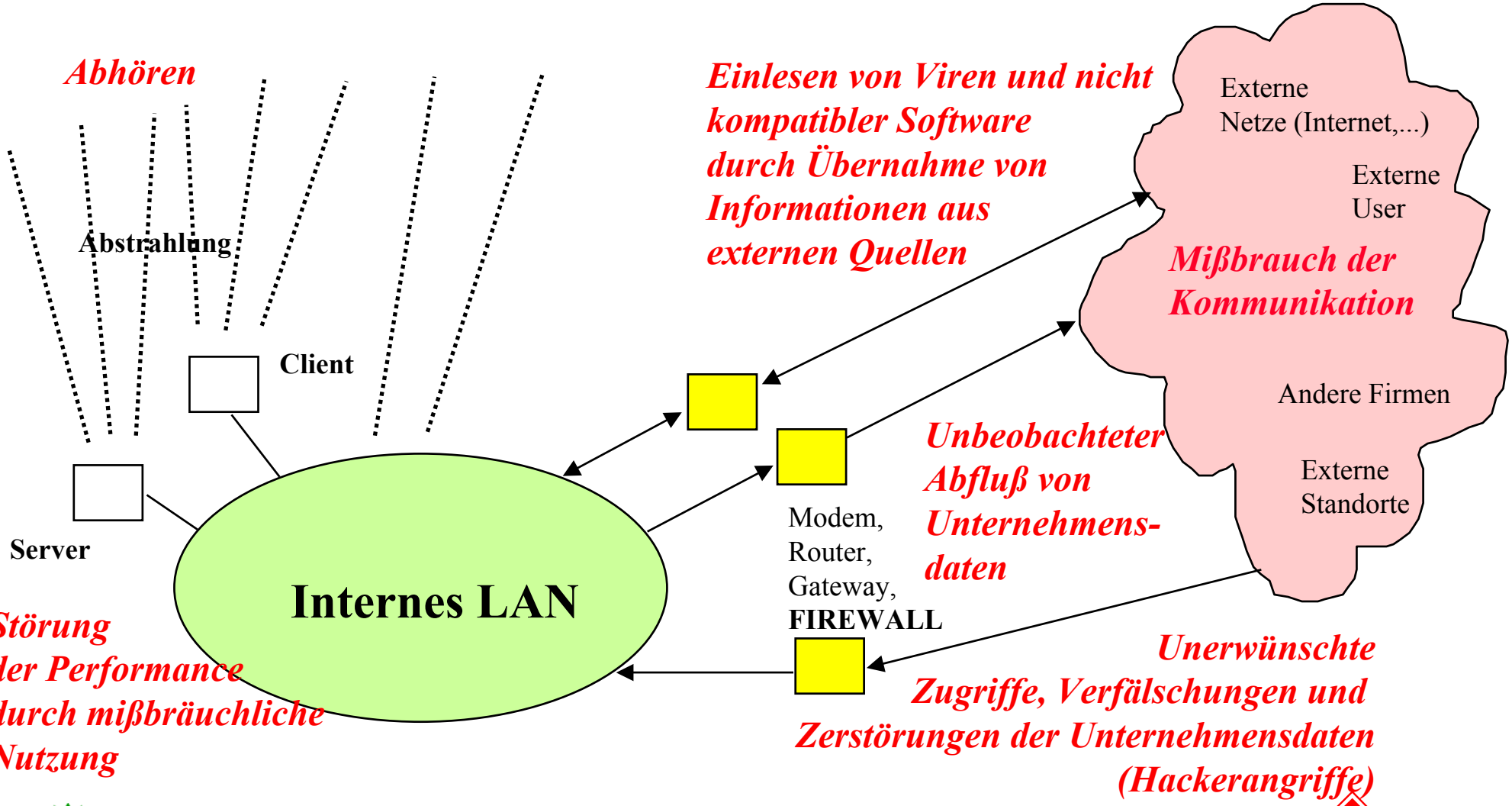
Organisation/Prozesse

Was hat das Ganze eigentlich mit IT-Sicherheit zu tun?

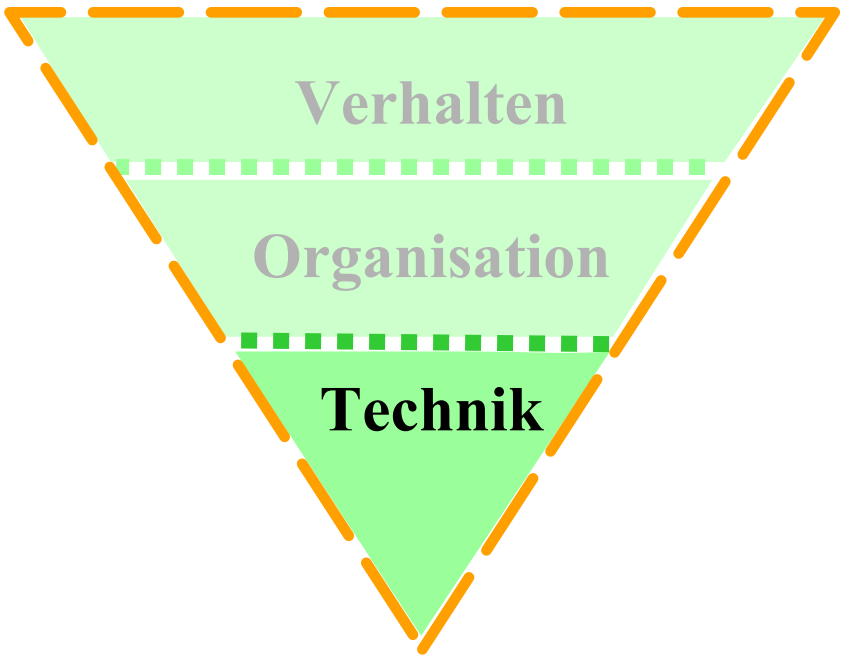
Umsetzung/Ergebnisse

Zusammenfassung/Fragen

IT-Sicherheit: Gefährdungsanalyse

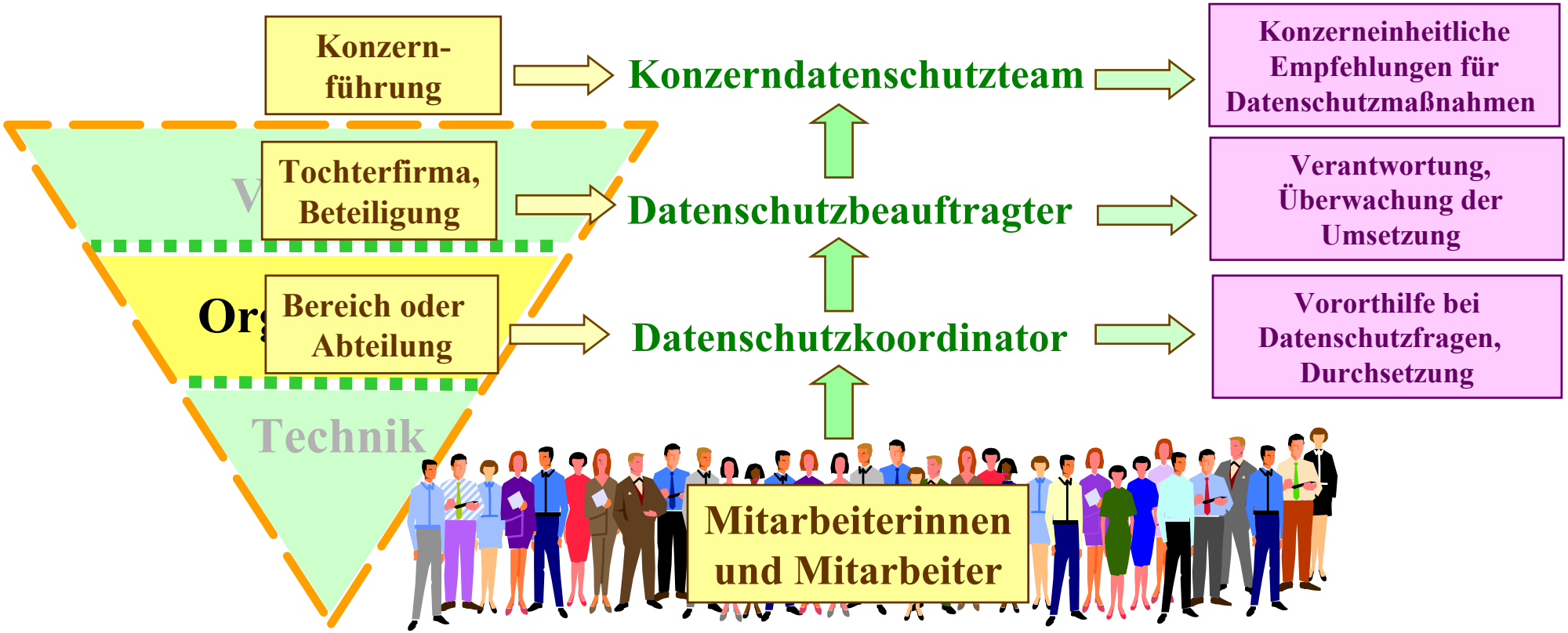


IT-Sicherheit:...Technik, Organisation, Verhalten?

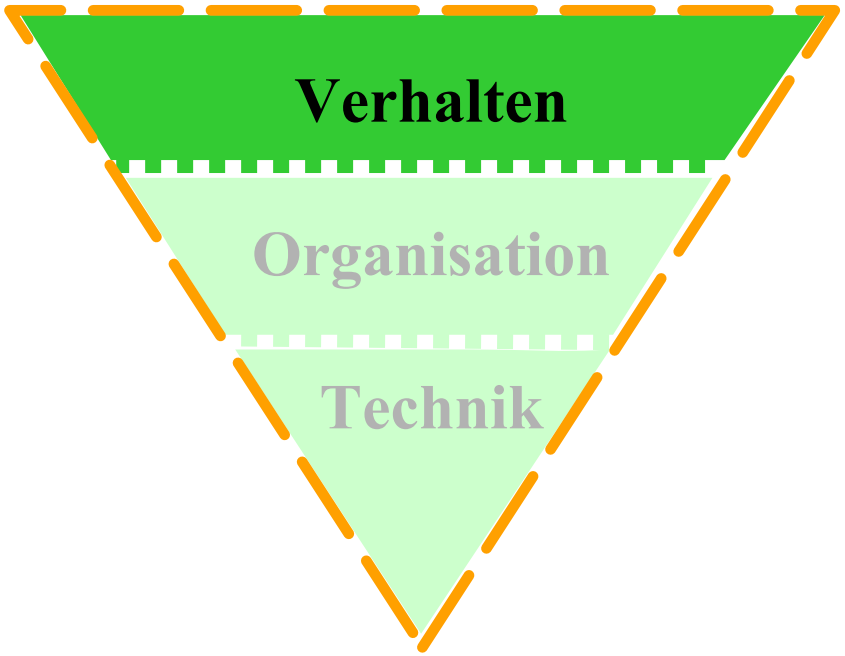


- Kein externer Kontakt ohne Firewall
- Einschränkungen im E-Mail-Verkehr (Filter in der Firewall)
- Aktuelle Virenscanner unterschiedlicher Hersteller auf
  - der Firewall
  - allen Servern
  - allen Clients
- Contentfilter
- Eingeschränkte Möglichkeiten für den User, Einstellungen des Client zu verändern
- Zugangskontrollen
- Berechtigungskonzept
- ....

IT-Sicherheit: Wo liegt der Fokus? ...Organisation?



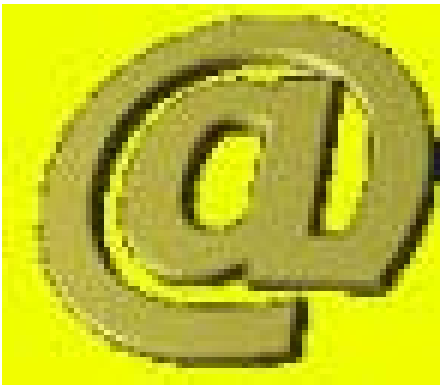
IT-Sicherheit: Wo liegt der Fokus? ...Verhalten?



- 60% - 80% der Schäden/Verstöße geschehen durch eigene Mitarbeiter „von Innen“
- Nicht „böse Absicht“, sondern Unwissenheit

- Sorgloser Umgang bei externem Mailingverkehr:
  - Ausspähen des Unternehmens
  - Verpflichtungen durch unseriöse E-Commerce Geschäfte
  - Aktivierung von Viren, Trojanischen Pferden
- Fehleinschätzung bei internem Mailingverkehr :
  - Performanceverluste im Netz (z. B. durch Kettenbriefe)
- Surfen im Netz kann zur Folge haben:
  - Übernahme von Störprogrammen, Viren etc. (Cookies, AktiveX, Java, ...)
- Weitergabe von Passwörtern oder anderen Informationen:
  - Geschäftsschädigung durch Informationsweitergabe
  - Kommerzielle Nutzung durch Dritte

eMail (2) - Kettenbrief



Ketten-Briefe per e-Mail an eine riesige Verteilerliste

Belastung des Netzwerks

Verbindung zu den Tankern auf See unterbrochen

Passwortschutz - Qualität

- **Gutes Passwort häufig einziger Schutz gegen Angriffe !!!**

So viel Zeit benötigt 1Ghz – Rechner für das Entschlüsseln:

„London"	-	1	Sekunde
„bplondon"	-	7	Minuten
„Bplndn"	-	3	Jahre
„&1Lndn"	-	35	Jahre
„kzr67DÄX?§§w56H**v5@"		307	Jahre
„Ichbinok!"	-	3	Jahre

Managementsystem für IT-Sicherheit

- Unternehmensgrundsätze
- Policies (Managementhandbücher mit Politik, Leitlinien und allgemeinen Regeln)
  - Spezielle Policies für
    - Internetauftritt
    - Datenschutz
- Regeln für den IT-Bereich (Festlegung der Details des Prozesses)
  - Verfahrensanweisungen
  - Betriebsanweisungen
  - Arbeitsanweisungen
- Dokumentationsfestlegungen
- Kommunikation über das Managementsystem
- Überprüfung der Regeln in Audits
- Verfolgung der Auditergebnisse
- Verbesserung der Regeln, kontinuierlicher Verbesserungsprozess

Managementsystem für IT-Sicherheit

Click to add Title

Vorgeschichte
Ziele
Strategie/Maßnahmen
Organisation/Prozesse
Was hat das Ganze eigentlich mit IT-Sicherheit zu tun?
Umsetzung/Ergebnisse
Zusammenfassung/Fragen

Die Managementsystemstruktur von DIN EN ISO 9001

Unterstützungsprozesse

- 4.1 Verantwortung der Leitung
- 4.2 Qualitätsmanagementsystem
- 4.5 Lenkung der Dokumente und Daten
- 4.16 Lenkung von Qualitätsaufzeichnungen
- 4.18 Schulung

Führungsprozesse

- 4.1 Verantwortung der Leitung
- 4.2 Qualitätsmanagementsystem
- 4.14 Korrektur- und Vorbeugungsmaßnahmen
- 4.17 Interne Qualitätsaudits

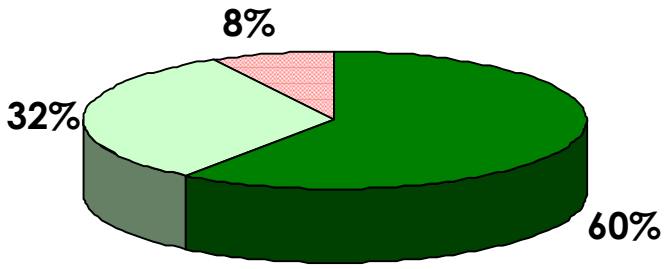
Wertschöpfungsprozesse

- 4.3 Vertragsprüfung
- 4.4 Designlenkung
- 4.6 Beschaffung
- 4.7 Lenkung der vom Kunden beigestellten Produkte
- 4.8 Kennzeichnung und Rückverfolgbarkeit von Produkten
- 4.9 Prozeßlenkung
- 4.10 Prüfungen
- 4.11 Prüfmittelüberwachung
- 4.12 Prüfstatus
- 4.13 Lenkung fehlerhafter Produkte
- 4.15 Handhabung, Lagerung, Verpackung, Konservierung und Versand
- 4.19 Wartung
- 4.20 Statistische Methoden

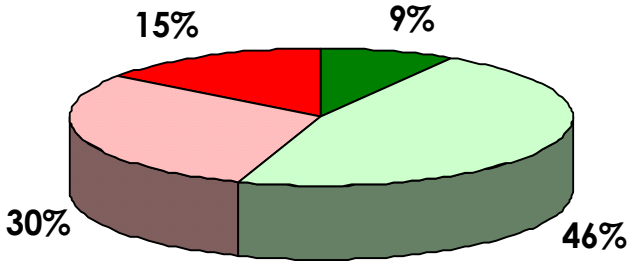
DIN EN ISO 9001 legt die Schwerpunkte auf die Wertschöpfungsprozesse!

Stellenwert des USGQ-Managementsystems Münchsmünster 1999

Das USGQ-System hat in MM einen hohen Stellenwert



Die Mitarbeiter haben genug Zeit für das USGQ-System zur Verfügung



Legende

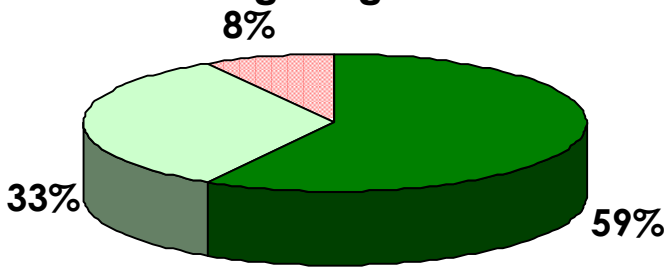
++

+

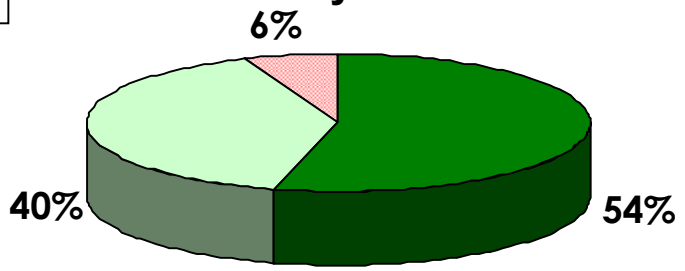
-

--

Das USGQ-System wird durch das Top-Management getragen

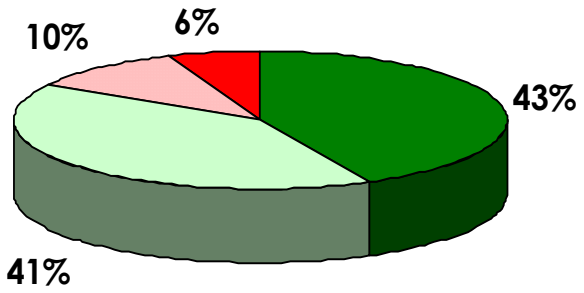


Das Top-Management engagiert sich für das USGQ-System

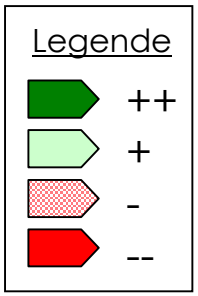


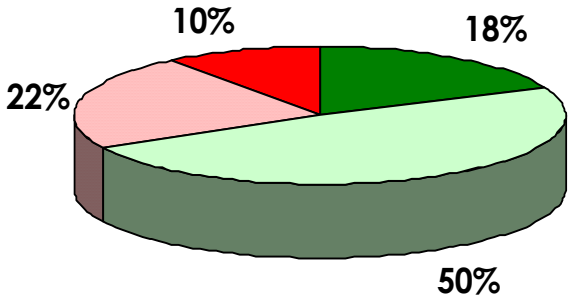
Einführung des USGQ-Managementsystems Münchsmünster 1999

Das USGQ-System wurde den Mitarbeitern nahegebracht/erklärt

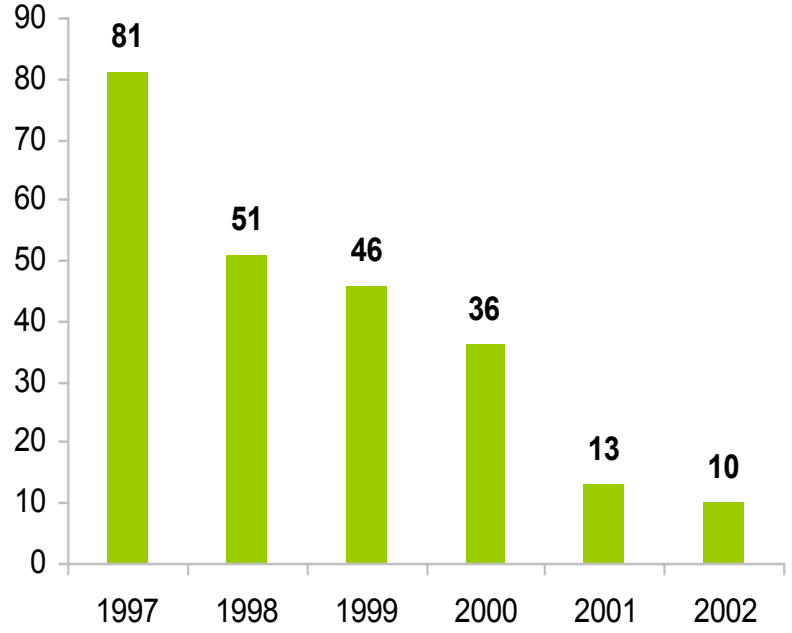


Die Mitarbeiter fühlen sich in die Gestaltung des USGQ-Systems einbezogen

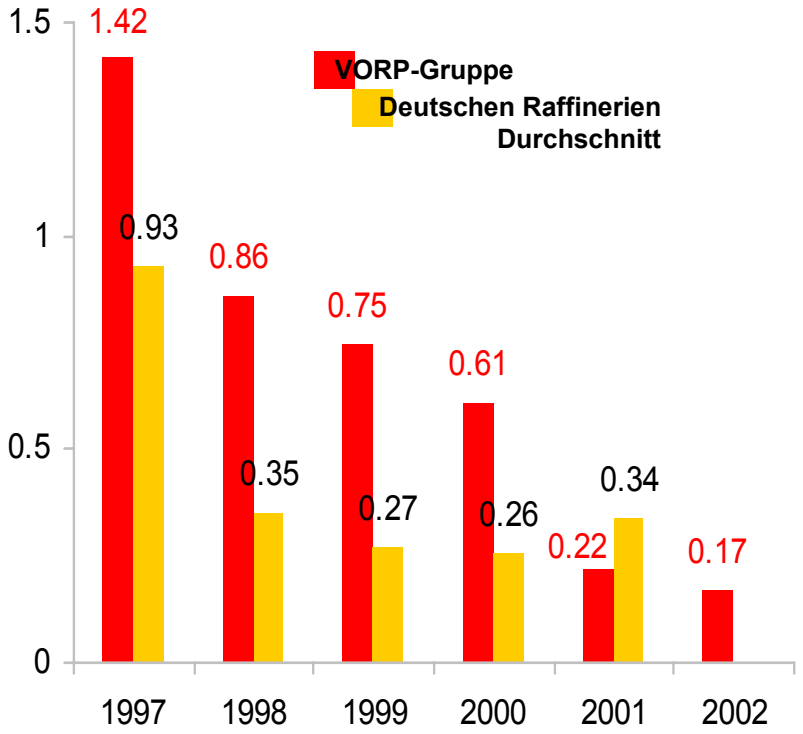




Entwicklung der Unfallzahlen VORP (eigene Mitarbeiter)



DAFWC for VORP-Group
(Days Away From Work Cases= Unfälle ab 1.Ausfalltag))



DAFWCF for VORP-Group
(DAFWC per 200,000 Arbeitsstunden)

Vorgeschichte

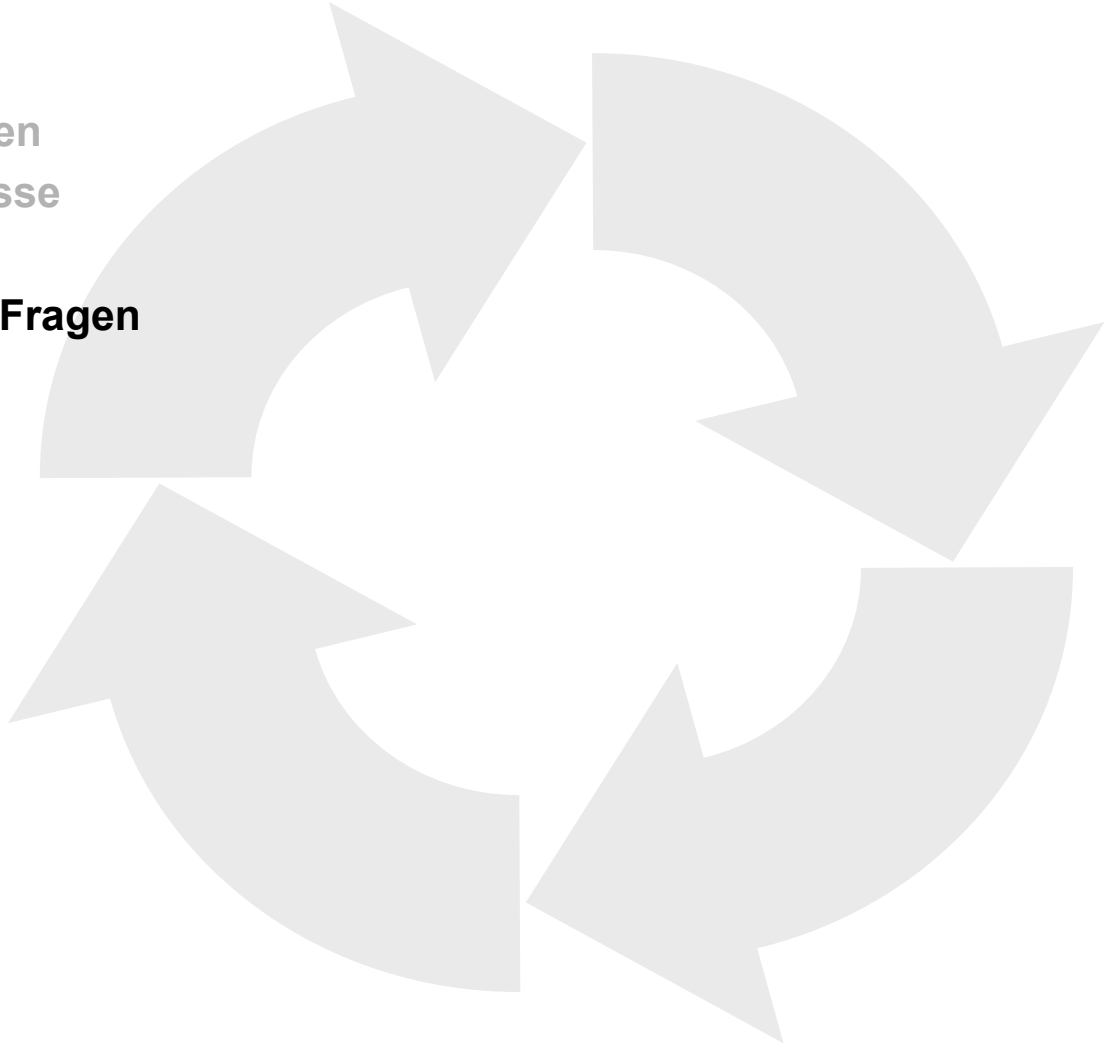
Ziele

Strategie/Maßnahmen

Organisation/Prozesse

Ergebnisse

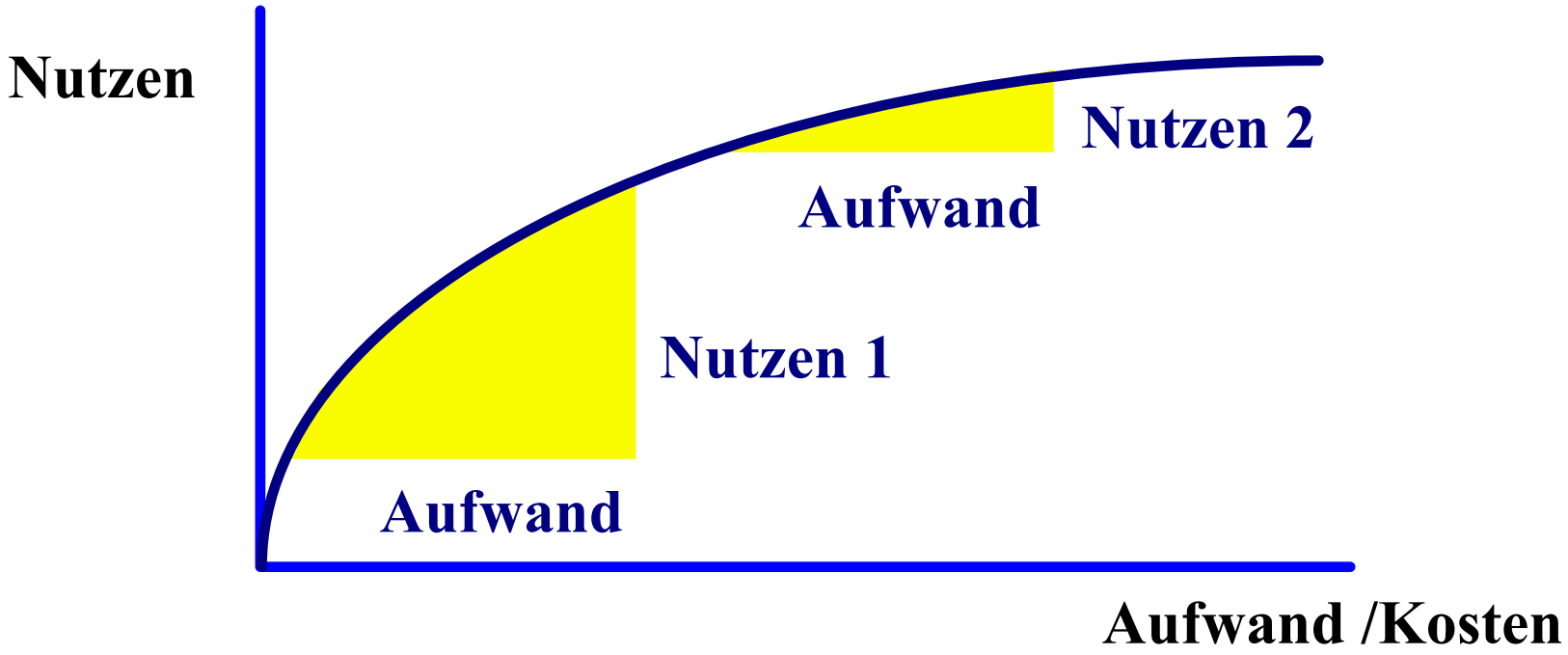
Zusammenfassung/Fragen



Paradigmenwechsel?
... Weg von Technik? ... Hin zu Systemen? ...

Sicherheit (und Unweltschutz und ...)
werden immer mehr durch VERHALTEN in ORGANISATIONEN bestimmt?

Der Nutzen technischer Verbesserungen ist begrenzt!



Unternehmensdimension

Managementsysteme spiegeln die individuelle Situation eines Unternehmens wieder

- **...die Ausgestaltung des MS‘s hängt stark von den Bedürfnissen der Mitarbeiter und der speziellen Kernkompetenzen/Prozesse des jeweiligen Unternehmens ab**

Unternehmen tragen nur ein Managementsystem

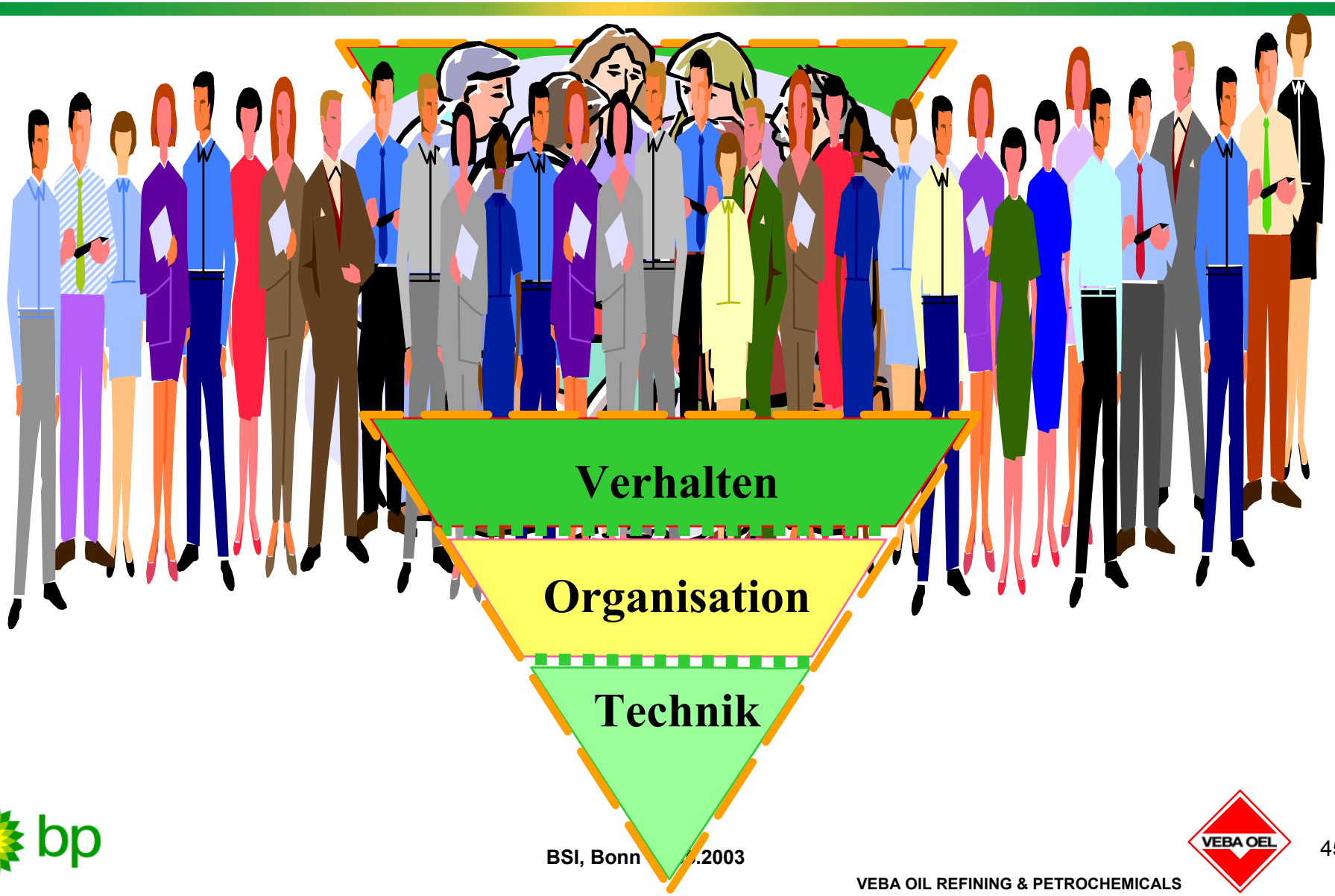
- **...mehrere MS‘e sind ineffizient und kontraproduktiv und schaden den übergeordneten Unternehmenszielen**

Managementsysteme müssen einen Beitrag zur Erreichung der Unternehmenszielen leisten

- **...ein wesentliches Ziel ist der Unternehmensgewinn**

... Auf dem Weg zu ganzheitlichem Unternehmens- und zu umfassenden RISK-Management ...?

Menschen entscheiden über den Erfolg von Systemen!



Offene Fragen?

Jürgen Herrmann

- **+49 209 6043 8644**
- **juergen.herrmann@vorp.de**