

Praxisforum III Anlassunabhängige und präventive Kontrollen

Luzern, 22. März 2001



Anlassunabhängige und präventive Kontrollen

Alex Ringli



Information Systems Assurance & Advisory Services

Thomas Kohler



Irren ist menschlich.

In vernetzten Umgebungen arbeiten viele Menschen

- ◆ Im Zeitalter der Komponenten lebte man mit der Einsicht „wo gearbeitet wird, werden Fehler gemacht“. Im Zeitalter der vernetzten Systeme wächst die Bedrohung, dass auftretende Fehler häufig dazu führen, dass nicht mehr gearbeitet werden kann. Quelle: BMC Software
- ◆ Die höhere Komplexität in der vernetzten Welt hat weitere und grössere Fehler- und Gefahrenquellen entstehen lassen
- ◆ Es gibt genug Fehler und Probleme, die von aussen kommen und auf die man keinen oder wenig Einfluss hat, umso mehr müssen Fehler dort verhindert werden, wo man präventiv wirken kann
- ◆ Prävention heisst, Fehler verhindern bevor sie geschehen. Durch Motivation, klare Zielsetzung, klare Definitionen, Methodologie mit Route Maps und Checklisten, vorgegebene Standards und Prozeduren, angewandtes Knowledge Management, Controlling, etc.

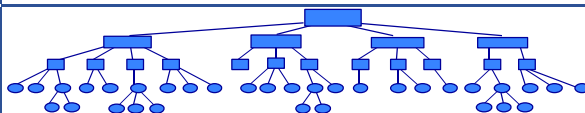


Praxisforum Luzern; Forum III

22. März 2001

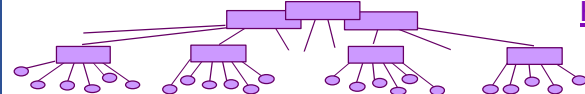
Veränderung wie die Leute arbeiten

60



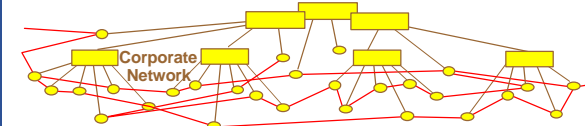
Hierarchisches Modell
Mitarbeiter ist Befehlempfänger

70



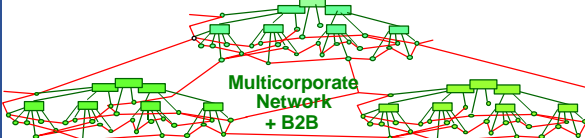
Knowledgeworker Modell
Flache Hierarchie
Mitarbeiter erhält mehr Verantwortung

80



Knowledgeworker Netzwerkmodell
Mitarbeiter erhält Querinformation

90



Knowledgeworker wird zum Decisionworker
Unternehmens- und weltweite Vernetzung

00+

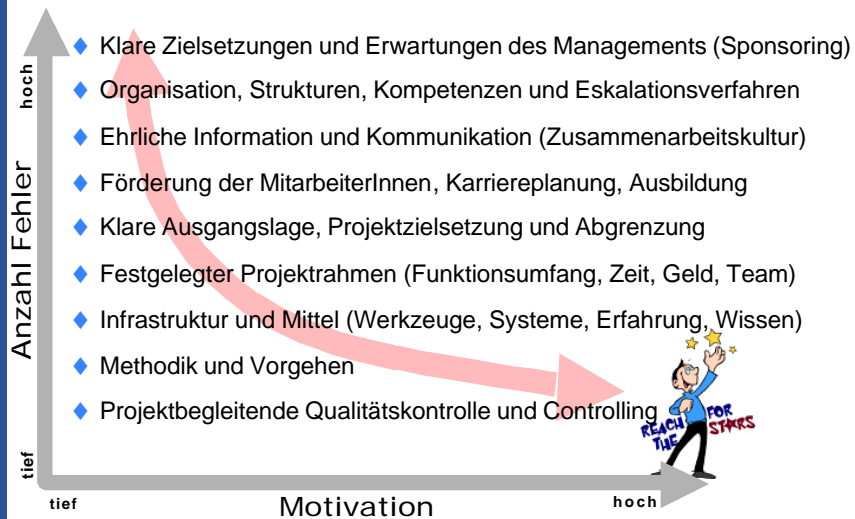


Knowledgeworker wird zum mobilen Decisionworker
weltweite Mobilität

Praxisforum Luzern; Forum III

Motivierte Mitarbeiter machen weniger Fehler

Qualitätssteigerung durch Motivation



Praxisforum Luzern; Forum III

22. März 2001

Vertrauen ist gut, Kontrolle ist besser

Präventive Kontrollen – der Zeitpunkt ist wichtig!

- ◆ Einbezug von IT-Audit bereits in der Detailspezifikationsphase
- ◆ Grob- und Detailkonzepte
 - auf Vorhandensein
 - auf Richtigkeit, Konsistenz
 - auf Machbarkeit
 - Risikoanalyse
- ◆ Komplexität vs. Einfachheit
 - Rolls Royce Lösung
 - alles auf einmal
 - viele Partner (Kommunikationsfalle)



Praxisforum Luzern; Forum III

22. März 2001

Vertrauen ist gut, Kontrolle ist besser

Präventive Kontrollen

◆ Sicherheit

- Sicherheitsstrategie
- Sicherheitskonzept
- Sicherheitsstandards und Prozeduren
- Umsetzung



◆ Tests

- Testkonzept
- Testdaten, Vertraulichkeit
- RFC Request for Change Konzept
- Releasemanagement

Vertrauen ist gut, Kontrolle ist besser

Präventive, anlassunabhängige Kontrollen

◆ Outsourcing

- Vertrag
- SLA Service Level Agreement
- Sicherheit
- strategische Weiterentwicklung
- Kostenentwicklung



◆ Ausbildung und Unterstützung

- Benutzerausbildung
- Dokumentation
- Supportorganisation und -qualität
- Benutzer-Problem- und Changemanagement

Vertrauen ist gut, Kontrolle ist besser

Präventive Kontrollen mit externer Unterstützung

- ◆ IT-Audit
- ◆ Gezielte, anlassunabhängige Kontrollen
 - z.B. ERP Prozessuntersuchung
 - Prozess-Integrität
 - Infrastruktur
 - Netzwerksicherheit, Zugriffsschutz
 - Katastrophenplanung
 - Restart- und Recoveryprozeduren
 - Datenkonversion
 - Internes Kontrollsystem



Vertrauen ist gut, Kontrolle ist besser

Präventive Kontrollen mit externer Unterstützung

- ◆ Neutralität
 - um die Betriebsblindheit zu überwinden
 - um Widerstände und Seilschaften zu umgehen
 - um die internen Kontrolleure zu kontrollieren
 - um Meinungen zu validieren (Second Opinion)
- ◆ Chinesische Mauer
 - Problematik Beratung vs. Audit
 - Problematik Reporting (z.B. an EBK)
 - Problematik Auditor



Beispiel eines konkreten A&P Set-ups

Präventive Kontrollen mit externer Unterstützung

◆ Attack & Penetration (Tiger Team)

— klare Zielsetzung, Vorgaben und Rahmenbedingungen:

- Management Engagement
- Vertrag (Letter of Understanding)
- Zielsetzung und Erwartung
- Organisation und Vorgehen
- Rollen und Verantwortlichkeiten
- Projektteam
- Master- und Detailplanung
- Vertraulichkeit
- Projektkultur
- Rechtliche Absicherung (Terms & Conditions)



A&P – Attack & Penetration Experiences

Some Lessons learned

- ◆ Roles and Responsibilities
- ◆ Legal and Regulatory Aspects
- ◆ Code of Conduct
- ◆ Management Involvement
- ◆ Controls
- ◆ Data Handling (Life Cycle)
- ◆ Risks
- ◆ Deliverables

