



Prozessmanagement-Summit 2011

Corporate Governance Eine Frage der Reife!

DI. Andreas Nehfort

andreas@nehfort.at

www.nehfort.at

Prozessreife & Governance - 1

DI. Andreas Nehfort
PzM-Summit 2011

Agenda



- Vorstellung Andreas Nehfort & Nehfort IT-Consulting
- Corporate Governance & IT-Governance
 - Beispiele mangelnder Governance
 - Governance & Compliance
- Die ISO 38500: Corporate Governance of IT
- Governance & Vertrauen
- Prozessreife schafft Sicherheit → zuverlässige Prozesse
 - Das SPICE Prozessreifegrad-Modell (ISO 15504)
 - SPICE Assessments
- SPICE als Werkzeug für Governance

Prozessreife & Governance - 2

DI. Andreas Nehfort
PzM-Summit 2011

Vorstellung Andreas Nehfort



IT-Consultant, Unternehmensberater, Trainer - seit 1986 selbständig:

- Berater für Software Prozesse & Qualität
- Prozessreife → CMMI & SPiCE
- Projektmanagement, Qualitätsmanagement, Requirements Engineering

Erfolg = Qualität x Akzeptanz

Qualifikation & Funktionen:

- SPiCE Principal Assessor & GPard Lead Assessor
- Vorstand der Österreichischen Vereinigung für Software Qualitätsmanagement - STEV-Österreich → www.softwarequalitaet.at

Background:

- TU-Wien – Studium der Technischen Mathematik: 1975 - 1979
- Software Entwicklung seit 1978 und Projektleitung seit 1982

Prozessreife & Governance - 3

DI. Andreas Nehfort
PzM-Summit 2011

Die Nehfort IT-Consulting



Beratungsunternehmen mit folgenden Schwerpunkten:

- Software Prozesse & Software Prozessverbesserung
- Vor dem Hintergrund anerkannter Referenzmodelle:
 - SPiCE - ISO15504 / Automotive SPiCE / CMMI
 - ITIL / ISO 20000 bzw. ISO 27000ff
 - Agile Prozesse (SCRUM, ...)
- Prozess- & Qualitätsmanagement
- GP-Partner & GPard-Assessor
- Network selbständiger Berater, Trainer, Assessoren:
 - Software Engineering & Projektmanagement
 - IT Service Management & Information Security Management
 - Prozessmanagement & Qualitätsmanagement

Prozessreife & Governance - 4

DI. Andreas Nehfort
PzM-Summit 2011

Governance



Governance bedeutet:

- Leiten, Lenken, Herrschen, Regieren, Steuern, Regulieren
- D.h. „**die Dinge im Griff haben**“

Corporate Governance:

- Grundsätze der (guten) Unternehmensführung

Corporate Governance

- The system by which organizations are directed and controlled OECD 1999

Governance bedeutet aber auch:

Für das Ergebnis die Verantwortung zu übernehmen!

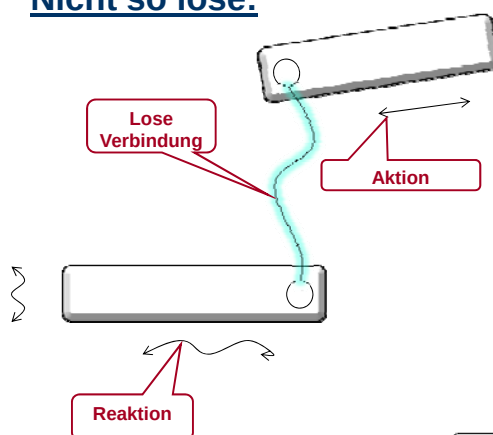
Prozessreife & Governance - 5

DI. Andreas Nehfort
PzM-Summit 2011

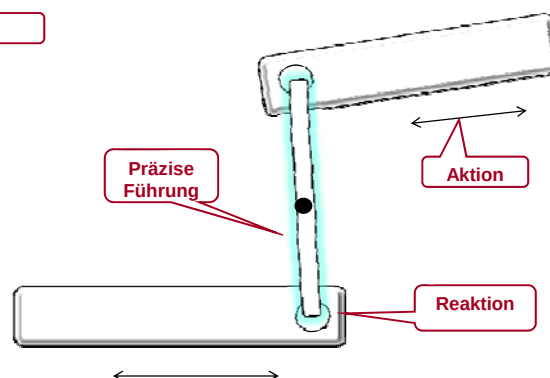
Governance bedeutet Steuern



Nicht so lose:



Sondern so: eng gekoppelt

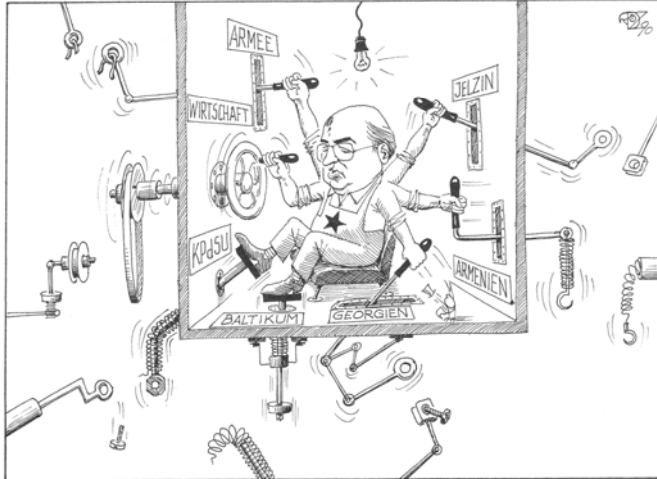


Prozessreife & Governance - 6

DI. Andreas Nehfort
PzM-Summit 2011

Governance?

Ganz sicher nicht so ...



Hebel der Macht - Dieter Zehentmayr – Kurier 1990

Prozessreife & Governance - 7

DI. Andreas Nehfort
PzM-Summit 2011

Management & Governance

Management stands for:

Getting things done by people!

Walter Wintersteiger

Governance stands for :

**Getting things done by people,
following „preassigned rules“!
(compliance rules)**

Prozessreife & Governance - 8

DI. Andreas Nehfort
PzM-Summit 2011

Corporate Governance



Corporate Governance

Quelle: Wikipedia

- bezeichnet den **Ordnungsrahmen** für die Leitung und Überwachung von Unternehmen.
- Der Ordnungsrahmen wird maßgeblich durch **Gesetzgeber** (→ Rahmenbedingungen) und **Eigentümer** (→ Ziele) bestimmt.
- Die konkrete Ausgestaltung obliegt dem Eigentümer und der Unternehmensführung.

Das unternehmensspezifische Corporate Governance-System besteht aus der Gesamtheit relevanter Vorgaben, insbesondere:

- Relevante Gesetze, Richtlinien, Kodizes,
- Unternehmensleitbild & Absichtserklärungen
- und Usus der Unternehmensleitung und –überwachung.

Prozessreife & Governance - 9

DI. Andreas Nehfort
PzM-Summit 2011

Corporate Governance



Unter dem Begriff „**Corporate Governance**“ werden Grundsätze verantwortungsvoller Unternehmensleitung und -überwachung diskutiert.

Ziel guter Corporate Governance ist es,

- die **Wettbewerbsfähigkeit** des Unternehmens **zu sichern**
- und seinen **Wert** nachhaltig **zu steigern**.

Die Diskussion konzentriert sich auf die Leitungsstruktur von börsennotierten Aktiengesellschaften,

- weil bei diesen die Distanz zwischen der Unternehmensführung und den Anteilseignern aufgrund der regelmäßig breiten Streuung der Aktien relativ groß ist.

Quelle: PWC

Prozessreife & Governance - 10

DI. Andreas Nehfort
PzM-Summit 2011

Kennzeichen *guter* Corporate Governance



- Funktionsfähige Unternehmensleitung
- Wahren der Interessen verschiedener Gruppen
 - Eigentümer, Kunden, Mitarbeiter, Gesellschaft
- Zielgerichtete Zusammenarbeit in der Unternehmensleitung und -überwachung
- Transparenz in der Unternehmenskommunikation
- Angemessener Umgang mit Risiken
- Managemententscheidungen sind auf langfristige Wertschöpfung ausgerichtet.

Quelle: Wikipedia

Prozessreife & Governance - 11

DI. Andreas Nehfort
PzM-Summit 2011

Governance Regeln



Für große (insbesondere börsennotierte) Unternehmen:

- SOX Sarbanes Oxley Act
- 8. EU Rahmenrichtlinie,
 - Unternehmensrechtsänderungsgesetz 2008
- Österreichischer Corporate Governance Kodex
 - Österreichischer Arbeitskreis für Corporate Governance

Gemeinsamkeit: Verantwortung des Top-Managements

- für die **Zuverlässigkeit** der Management-Informationen
- für ein **wirksames** Internes Kontroll System (**IKS**).

Prozessreife & Governance - 12

DI. Andreas Nehfort
PzM-Summit 2011

8. EU Rahmenrichtlinie



Fokus: Sicherstellung der korrekten Rechnungslegung

- Bilanzierung, Buchhaltung, externes Berichtswesen
- Durch ein internes Kontroll- & Risikomanagementsystem
- Die Rechnungsprüfer prüfen diese nach internat. Standards

Das verschärft die **Verpflichtung der Geschäftsführung und des Vorstands**, alle Maßnahmen zu setzen,

- um Vermögen zu schützen und
- um **regelkonform** (compliant) zu arbeiten.

Verantwortung des Top-Managements

- für die **Zuverlässigkeit** der Management-Informationen
- für ein **wirksames** Internes Kontroll System (**IKS**).

Prozessreife & Governance - 13

DI. Andreas Nehfort
PzM-Summit 2011

Beispiele mangelnder Corporate Governance



Heathrow Terminal 5

Nach der Eröffnung des als hochmodern gepriesenen rund fünf Milliarden Euro teuren Terminal 5 Ende März 2008 war dort eine tagelanges Reisechaos ausgebrochen;

- Etwa **30.000 Koffer** blieben liegen, **Hunderte Flüge** fielen aus!

Die Ursache:

- Die automatische Gepäckabfertigungsanlage hat nicht funktioniert.
- Dazu kamen Problem mit dem Zugangskontroll-System für das Personal ...

Das Debakel kostete die Fluggesellschaft British Airways (BA) rund 20 Mio. €

British Airways feuerte daraufhin im April

- Ihren Betriebsmanager **Gareth Kirkwood**
- und den Leiter des Kundenservices **David Noyes**.

Auch der Flughafendirektor geht ...

- **Mark Bullock** habe "sich entschlossen zu gehen" teilte der Flughafenbetreiber BAA heute mit. www.orf.at – Mai 2008

Prozessreife & Governance - 14

DI. Andreas Nehfort
PzM-Summit 2011

Beispiele mangelnder Corporate Governance



September 2011: Zocker-Skandal in der UBS:

- Der Londoner Händler Kweku Adoboli (31) hatte der Bank durch nicht autorisierte Geschäfte einen Verlust von 1,7 Milliarden € eingebracht.

UBS-Vorstand Grübel:

- "Ich habe die Verantwortung für alles, was in der Bank passiert, ich fühle mich aber nicht schuldig"

UBS-Chef Oswald Grübel gibt auf:

- Die Schweizer Großbank UBS trennt sich von ihrem Chef: **Es sei die "Pflicht" Grübels, die Verantwortung für den Betrugsskandal zu übernehmen**, teilt der Verwaltungsrat mit.



Prozessreife & Governance - 15

DI. Andreas Nehfort
PzM-Summit 2011

Die Reaktion auf Mängel in der Corporate Governance



„Unternehmen setzen verstärkt auf „Compliance“ *)

Etablierung der Unternehmensfunktion

„Compliance Management“

Die Selbstverpflichtung, sich an bestimmte Regeln zu halten

Compliance wird zunehmend ein Wettbewerbsfaktor!



*) Quelle: Wirtschaftsblatt 7.11.2011 / Kienbaum Studie

Prozessreife & Governance - 16

DI. Andreas Nehfort
PzM-Summit 2011

Verbindlichkeit von Compliance Regeln



1. Obligatory Requirement (L – Legal):
 - Die Regel ist zwingend einzuhalten.
2. Comply or Explain (C):
 - Regel soll eingehalten werden;
 - Eine Abweichung muss erklärt und begründet werden, um sich Regelkonform zu verhalten.
3. Recommendation (R):
 - Regel mit Empfehlungscharakter;
 - Nichteinhaltung ist weder offenzulegen noch zu begründen.

Prozessreife & Governance - 17

DI. Andreas Nehfort
PzM-Summit 2011

Isolierte Maßnahmen geben in der Praxis oft wenig Sicherheit ...



Prozessreife & Governance - 18

DI. Andreas Nehfort
PzM-Summit 2011

Manche Maßnahmen verfehlen zumindest zeitweise ihren Zweck



Prozessreife & Governance - 19

DI. Andreas Nehfort
PzM-Summit 2011

IT-Governance (Corporate governance of IT)

- **Führung, Organisationsstrukturen und Prozesse,** die sicherstellen, dass die IT die **Unternehmensstrategie** und die **Unternehmensziele** unterstützt.

Wichtiger Bestandteil:

- Business-IT-Alignment

Relevante Standards:

- **Cobit** - Control Objectives for Information and related Technology
- **ISO/IEC 38500:2008:**
Corporate governance of information technology
 - Der erste ISO Standard zum Thema Governance

Prozessreife & Governance - 20

DI. Andreas Nehfort
PzM-Summit 2011

IT-Governance



IT-Governance bedeutet:

- Sicherstellen, dass die IT die Unternehmensziele und die Strategie zu deren Umsetzung unterstützt.
- Sicherstellen, dass die IT die Unternehmensleitung mit korrekten Informationen versorgt:
 - Daten aus dem operative Geschäft
 - Bilanzierung, Buchhaltung, externes Berichtswesen
- Sicherstellen, dass die IT eine gesetzeskonforme Unternehmensführung ermöglicht / unterstützt.

Prozessreife & Governance - 21

DI. Andreas Nehfort
PzM-Summit 2011

IT-Governance



Das Hauptziel:

- Die IT ist „**fit for purpose**“

Verantwortlichkeiten im Rahmen der IT-Governance:

- Informationssicherheit & Schutz personenbezogener Daten
- E-Commerce-Richtlinien
- Urheberrecht inclusive Software Licensing
- Aufzeichnungspflichten
- Umweltschutz,
- Gesundheit & Sicherheit
- Zugriffsschutz & Vertraulichkeit betrieblicher Informationen

Prozessreife & Governance - 22

DI. Andreas Nehfort
PzM-Summit 2011

ISO 38500 - Framework for good Corporate Governance of IT



Governance Model:

- Regelschleife: Evaluate - Direct – Monitor

Six Principles for good corporate governance of IT

- Definiert sechs Themenbereiche der IT-Governance:
 - Responsibility, Strategy, Acquisition,
 - Performance, Conformance, Human behaviour

Guidance for the corporate governance of IT

- Erläuterungen zur Umsetzung der 6 Prinzipien mittels des Governance Models → Evaluate - Direct – Monitor

Bietet eine gute „High-Level“ Anleitung

Prozessreife & Governance - 23

DI. Andreas Nehfort
PzM-Summit 2011

ISO 38500 - Governance Model



Directors should govern IT through three main tasks:

- **Evaluate** - Bewerten
 - Evaluate the current and future use of IT.
- **Direct** – Lenken
 - Direct preparation and implementation of plans & policies
 - to ensure that use of IT meets business objectives.
- **Monitor** – Beobachten, beaufsichtigen, überwachen
 - Monitor conformance to policies, and performance against the plans.

Prozessreife & Governance - 24

DI. Andreas Nehfort
PzM-Summit 2011

ISO 38500 - Governance Principles



Principle 1: Responsibility

- Individuals and groups within the organization understand and accept their responsibilities in respect of both supply of, and demand for IT.
- Those with responsibility for actions also have the authority to perform those actions.

Principle 2: Strategy

- The organization's business strategy takes into account the current and future capabilities of IT;
- the strategic plans for IT satisfy the current and ongoing needs of the organization's business strategy.

Prozessreife & Governance - 25

DI. Andreas Nehfort
PzM-Summit 2011

ISO 38500 - Governance Principles



Principle 3: Acquisition

- IT acquisitions are made for valid reasons, on the basis of appropriate and ongoing analysis, with clear and transparent decision making.
- There is appropriate balance between benefits, opportunities, costs, and risks, in both the short term and the long term.

Principle 4: Performance

- IT is **fit for purpose** in supporting the organization, providing the services, levels of service and service quality required to meet current and future business requirements.

Prozessreife & Governance - 26

DI. Andreas Nehfort
PzM-Summit 2011

ISO 38500 - Governance Principles



Principle 5: Conformance

- IT complies with all mandatory legislation and regulations. Policies and practices are clearly defined, implemented and enforced.

Principle 6: Human Behaviour

- IT policies, practices and decisions demonstrate respect for Human Behaviour, including the current and evolving needs of all the 'people in the process'.

Prozessreife & Governance - 27

DI. Andreas Nehfort
PzM-Summit 2011

Governance im Privatleben



Governance in der Familie:

- Aufsichtspflicht der Erziehungsberechtigten
- Umsetzung Familien-interner Spielregeln

IT-Governance in der Familie:

- **Wirksame Spielregeln** zur Nutzung der familiären IT-Infrastruktur:
 - Schutz Minderjähriger vor ungeeigneten Inhalten
 - Schutz der Persönlichkeitsrechte Dritter → social media
 - Schutz der Urheberrechte → Tauschbörsen

Der Anspruch ist klar und nachvollziehbar

- Die Umsetzung ist nicht immer einfach ...

Prozessreife & Governance - 28

DI. Andreas Nehfort
PzM-Summit 2011

Governance erfordert Vertrauen



Governance (im Sinne von Steuern) erfordert Vertrauen:

- **Vertrauen** in die eigene Kompetenz als Steuermann
- **Vertrauen** in die Handlungs-Kompetenz meines Teams
- **Vertrauen** in die Strukturen zur Steuerung der Organisation

Governance (im Sinne von Kontrolle) erfordert ebenfalls Vertrauen:

- **Vertrauen** in die eigene Kontroll-Kompetenz
- **Vertrauen** in die Kontroll-Kompetenz meines Teams
- **Vertrauen** in die Kontroll-Strukturen der Organisation

Prozessreife & Governance - 29

DI. Andreas Nehfort
PzM-Summit 2011

Governance & Vertrauen



**Governance hat das Ziel Vertrauen zu schaffen
durch Transparenz & Nachvollziehbarkeit**

Konkret: Vertrauen schaffen

- durch transparente, zuverlässige Prozesse
- durch transparente, zuverlässige Prozesssteuerung
- durch transparente, zuverlässige Prozesskontrolle
- **durch nachvollziehbare & zuverlässige Ergebnisse**

Prozessreife & Governance - 30

DI. Andreas Nehfort
PzM-Summit 2011

Product

People

Technology

Methodology

Processes

Fokus auf alle Einflussfaktoren

DI. Andreas Nehfort
PzM-Summit 2011

[illegible]

DI. Andreas Nehfort
PzM-Summit 2011

Qualität = Fit for Purpose



Jedoch:

- Nicht immer ist eine fehlerfreie Spezifikation ausreichend ...

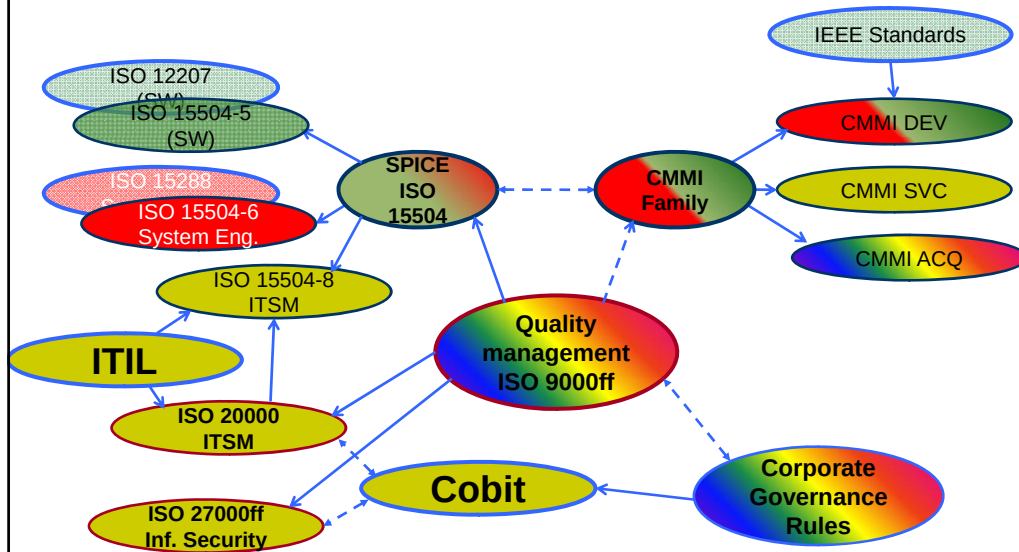


Prozessreife & Governance - 33

DI. Andreas Nehfort
PzM-Summit 2011

Qualitätsstandards in der IT

(ein kleiner Ausschnitt für unsere Zwecke, d.h. vereinfacht ...)



Prozessreife & Governance - 34

DI. Andreas Nehfort
V4.0 / 12.11.2009

Zuverlässige Prozesse?



Referenzmodelle definieren typischerweise **inhaltliche Anforderungen** an unsere Prozesse → **Was ist zu tun?**

Die offene Frage:

- **Wie** müssen sichere/zuverlässige Prozesse beschaffen sein?

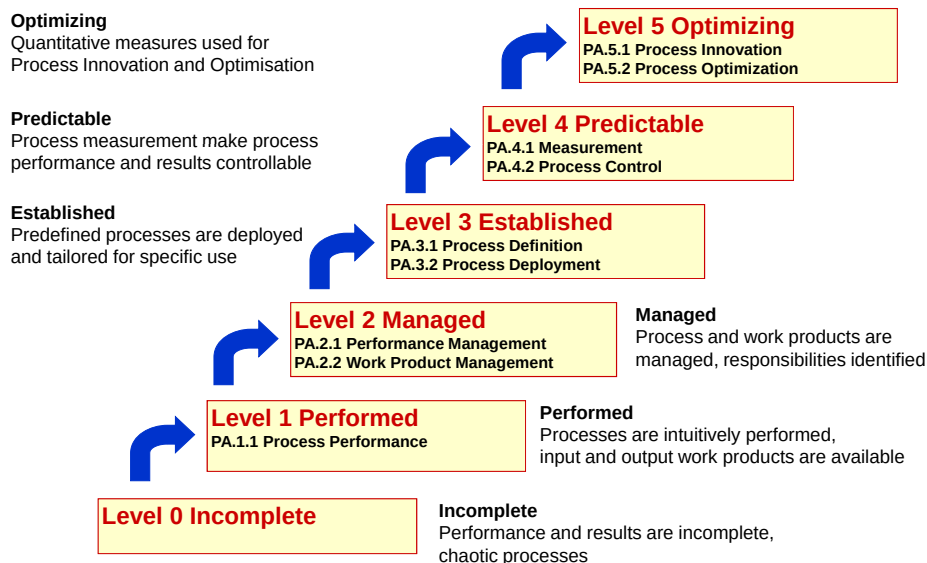
Prozessreifegradmodelle geben eine Antwort:

- Die Kriterien der Prozessreife bieten eine methodische Grundlage für Prozess-Sicherheit!
- CMMI und SPICE / ISO 15504 sind Werkzeuge
 - für sichere/zuverlässige Prozesse und
 - für die Wirksamkeit eines IKS

Prozessreife & Governance - 35

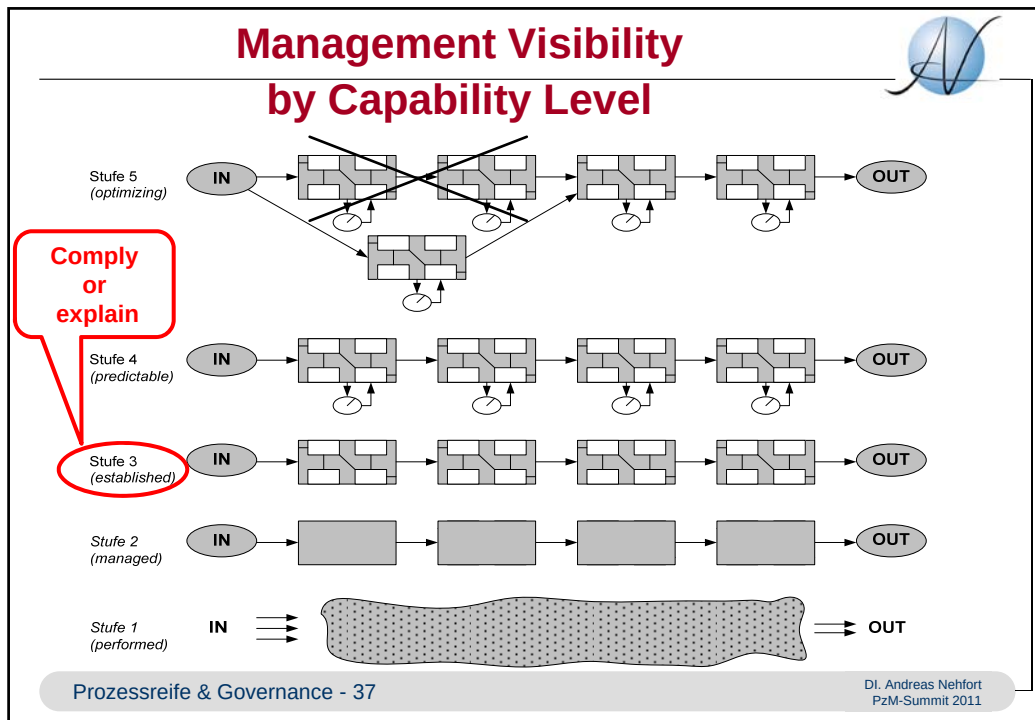
DI. Andreas Nehfort
PzM-Summit 2011

SPICE-Capability Levels



Prozessreife & Governance - 36

DI. Andreas Nehfort
PzM-Summit 2011



SPICE als Best Practice für Prozessmanagement

Das SPICE Prozessreifegradmodell liefert einen generischen Baukasten für reife Prozesse:

- Geeignete Basispraktiken, damit der Prozess seinen Zweck erfüllen kann.
- Kriterien für Planung & Lenkung der Prozessdurchführung → CL2
- Kriterien für Planung & Lenkung der Prozessergebnisse → CL2
- Kriterien für die Definition von Standardprozessen → CL3
 - Inklusive Überwachung auf Eignung & Angemessenheit
- Kriterien für den Einsatz von Standardprozessen → CL3
 - Inklusive Analyse des Prozessverhaltens
- Kriterien für quantitative Prozess-Steuerung → CL4

Prozessreife & Governance - 38

DI. Andreas Nehfort
PzM-Summit 2011

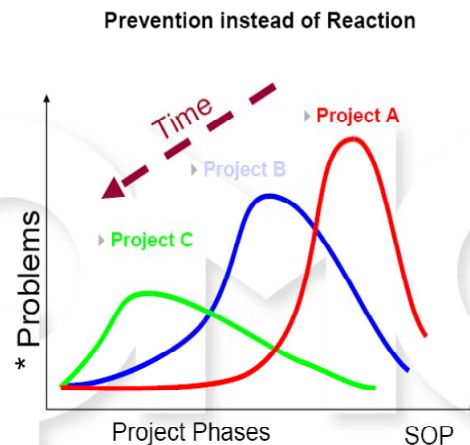
Prozessreife eliminiert Unsicherheit



Mit zunehmender Prozessreife wird der Prozess für Außenstehende

- besser steuerbar
- besser nachvollziehbar
- besser kontrollierbar

Mit zunehmender Prozessreife wird der Prozess zuverlässiger!



Prozessreife & Governance - 39

DI. Andreas Nehfort
PzM-Summit 2011

Prozessreife – Warum?



If you don't attack a risk actively ...



... the risk will attack you!

Prozessreife & Governance - 40

DI. Andreas Nehfort
PzM-Summit 2011

Prozessreife & Risiko



Prozessreife:

- Reduziert das Risiko unerwünschter Ergebnisse ...
- Trägt dazu bei, mehr Sicherheit zu gewährleisten

Prozessreife:

- Erhöht die Transparenz von Prozessen
- Ermöglicht es damit dem Management, Verantwortung (wirklich) zu übernehmen

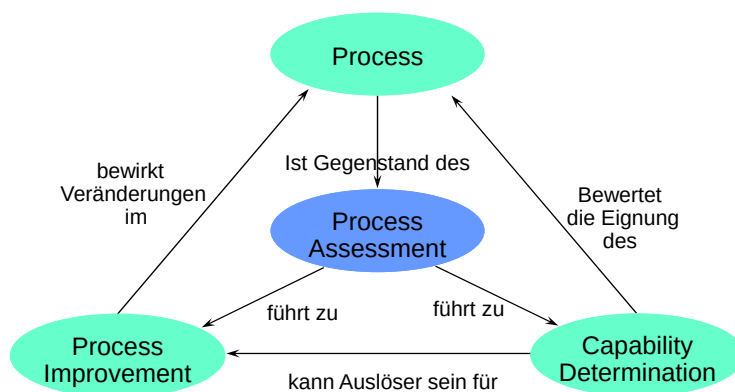
Process Assessments:

- Bestätigen die Reife der Prozesse
- Decken allfällige Lücken auf ... und damit Risiken ...

Prozessreife & Governance - 41

DI Dr. Andreas Nehfort
PzM-Summit 2011

Process Assessments



Prozessreife & Governance - 42

DI Dr. Andreas Nehfort
PzM-Summit 2011

Das Motto



**Messen was messbar ist,
messbar machen,
was noch nicht messbar ist.**

Galileo Galilei

(lang vor Watts Humphrey & CMM/CMMI & SPICE)

**Prozessqualität messbar machen!
Fortschritte messbar machen!**

Prozessreife & Governance - 43

DI. Andreas Nehfort
PzM-Summit 2011

Assessment Tools



Die SPICE 1-2-1 Tool-Familie

Assessment Tools unterstützen

- die Assessment Vorbereitung
- die Assessment Durchführung
- die Assessment Auswertung
- die Erstellung des Assessment Reports

SPICE 1-2-1 for IT-Governance:

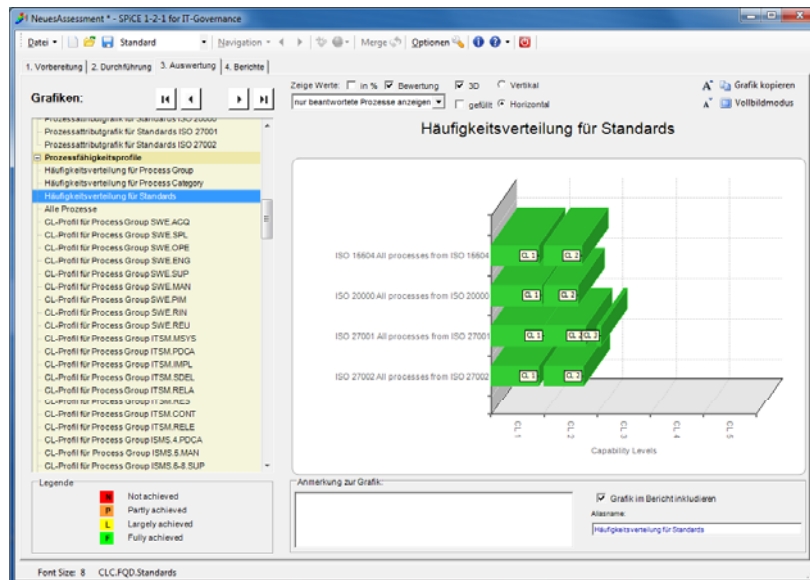
- Software Entwicklung → ISO 15504-5
- IT Service Management → ISO 20000-1 & ISO 20000-4
- Information Security Management → ISO 27001 & ISO 27002

Weitere Infos → www.nehfort.at/assessmenttools/

Prozessreife & Governance - 44

DI. Andreas Nehfort
PzM-Summit 2011

SPICE 1-2-1 for IT-Governance



Prozessreife & Governance - 45

DI. Andreas Nehfort
PzM-Summit 2011

Prozessreife schafft Sicherheit

Definierte Standardprozesse:

- Definierte Standardprozesse → etablierte Standards
 - Etablierte Standards → ermöglichen definierte Leistung
 - Etablierte Standards → ermöglichen Vergleichbarkeit
 - Etablierte Standards → ermöglichen Prozessmessung
- Prozessmessung → ermöglicht Soll-Ist Vergleich
- Prozessmessung → ermöglicht Prozess Reporting
 - Prozess Reporting → ermöglicht Transparenz
- Transparenz → ermöglicht es dem Management **Verantwortung** wahrzunehmen

Diese Verantwortung nennt man heute Governance!

Prozessreife & Governance - 46

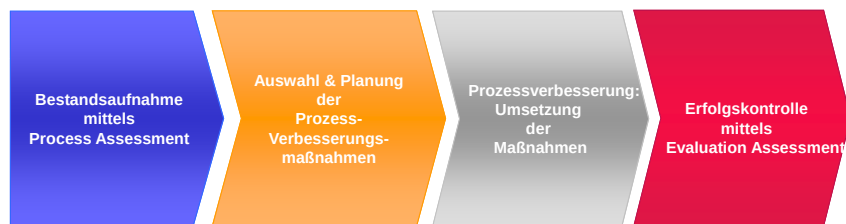
DI. Andreas Nehfort
PzM-Summit 2011

Assessment Based Process Improvement A-B-P-I



Prozessverbesserung in 4 Schritten:

1. Bestandsaufnahme zur Standortbestimmung
2. Auswahl & Planung der Prozessverbesserungsmaßnahmen
3. Prozessverbesserung: Umsetzen der Maßnahmen
4. Erfolgskontrolle



Prozessreife & Governance - 47

DI. Andreas Nehfort
PzM-Summit 2011

SPICE for Corporate Governance



- Identifizieren Sie Ihre Ziele
- Identifizieren Sie Ihre Strategien zur Erreichung dieser Ziele
- Identifizieren Sie Ihre kritischen Prozesse
- Gestalten Sie diese Prozesse nach den Kriterien des SPICE Reifegradmodells:
 - Geeignete Basispraktiken, damit der Prozess seinen Zweck erfüllen kann → CL1
 - Planung & Lenkung → CL2
 - Ausgestaltung als definierter Standardprozess → CL3
- Lassen Sie Assessments durchführen (als Teil Ihres IKS)
- Eliminieren Sie die identifizierten Schwachstellen

Prozessreife & Governance - 48

DI. Andreas Nehfort
PzM-Summit 2011



**"Reif ist,
wer auf sich selbst nicht mehr hereinfällt!"**

Heimito von Doderer

Governance bedeutet:

**Sicherzustellen, dass eine Organisation
sich nicht selber austrickst!**

SPICE unterstützt Sie dabei!

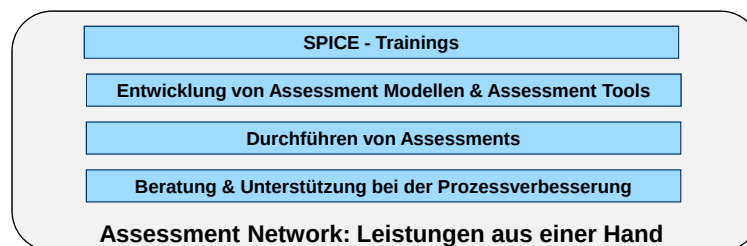
Prozessreife & Governance - 49

DI. Andreas Nehfort
PzM-Summit 2011



**SPICE gibt Ihnen die Werkzeuge
um Governance
mittels reifer Prozesse
systematisch zu implementieren!**

Wir unterstützen Sie dabei mit unserer Expertise!



Prozessreife & Governance - 50

DI. Andreas Nehfort
PzM-Summit 2011



Danke für Ihre Aufmerksamkeit!

Fragen & Anmerkungen

Diskussion ...