# IIR - ITIL Forum 2007

## IT Management Standards for IT Governance

### Das große Spannungsfeld ITIL/COBIT/SOX/EURO-SOX und welche Rolle spielen die ISO-Standards?

**DI. Andreas Nehfort**

andreas@nehfort.at www.nehfort.at



## Die Themen

IT-Prozesse:
- Software Development
- IT Service Management
- Information Security Management

IT Governance:
- Lenkung & Kontrolle → IT Controls

Die zugehörigen relevanten Standards im Überblick

Empfehlungen zur Umsetzung

## Die Fragen der Veranstalter

**Das große Spannungsfeld ITIL / COBIT / SOX / EURO-SOX und welche Rolle spielen die ISO-Standards?**

- Wo liegen deren Schwerpunkte bzw. Unterschiede?
- Welchen Standard benötige ich wofür?
- Schaffe ich es mit ITIL alleine auszukommen oder gibt es Empfehlungen wann man welche Norm bestenfalls einsetzt
- Wie kann ich die Wirtschaftsprüfer mit ITIL zufrieden stellen?
- EURO SOX jeder spricht darüber und keiner weiß Bescheid:
  - Ab wann wird EURO SOX in nationales Recht übergehen?
  - Wo stecken die großen Änderungen und die Unterschiede zu SOX?



## Weitere Themen ...

**Das große Spannungsfeld ITIL/COBIT/SOX/EURO-SOX und welche Rolle spielen die ISO-Standards ... ?**

- Prozessreife CMMI & SPICE/ISO 15504
- ISO 9000 / ISO 20000 / ISO 27000 und die Bedeutung für das IT Management?
  - Wie geht es mit ISO 27000 weiter? Ein Ausblick.
- Gemeinsame Basistechniken für die Implementierung
  - Wie bringe ich all diese Vorgaben unter einen Hut?

## IT Governance & IT Prozessmanagement

**Geschäftsleitung**

**Was soll die IT machen?**

**Macht die IT das, was sie soll?**

**Wie erreichen wir unsere Ziele?**

**IT Governance:**
- Lenkung & Kontrolle
- Control Objectives
- Control Activities
- Control Effectiveness

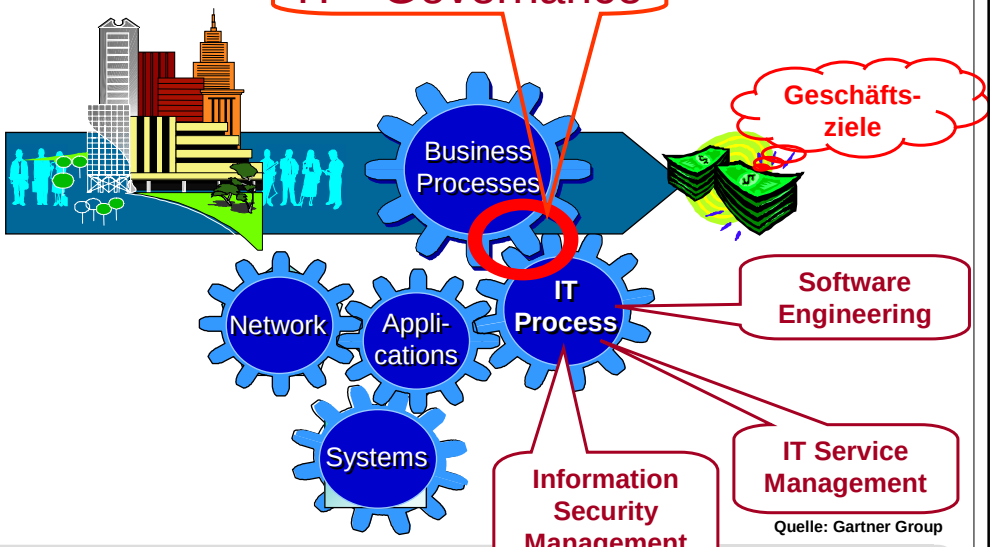
**IT Prozessmanagement:**
- Prozessverbesserung
- Prozessreife Modelle
- Referenz Prozess-modelle
- Best Practice Modelle

**IT Management**

IT Management Standards - 5

DI. Andreas Nehfort
IIR – ITIL Forum - 05.11.2007

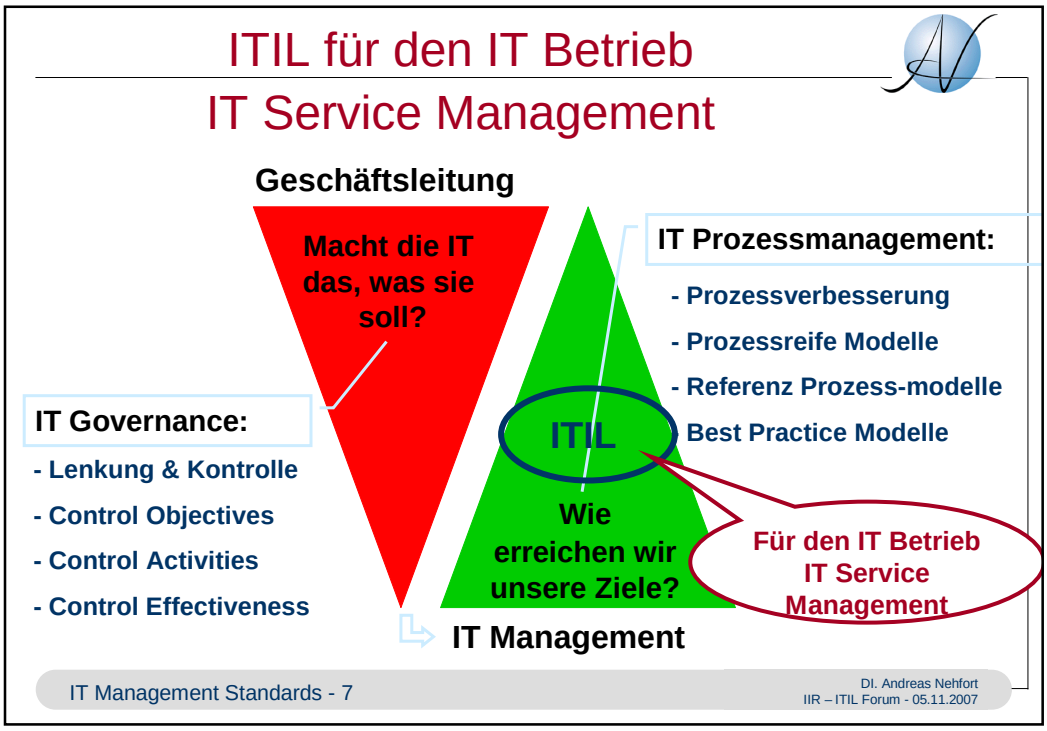
## IT - Prozess Management und IT - Governance

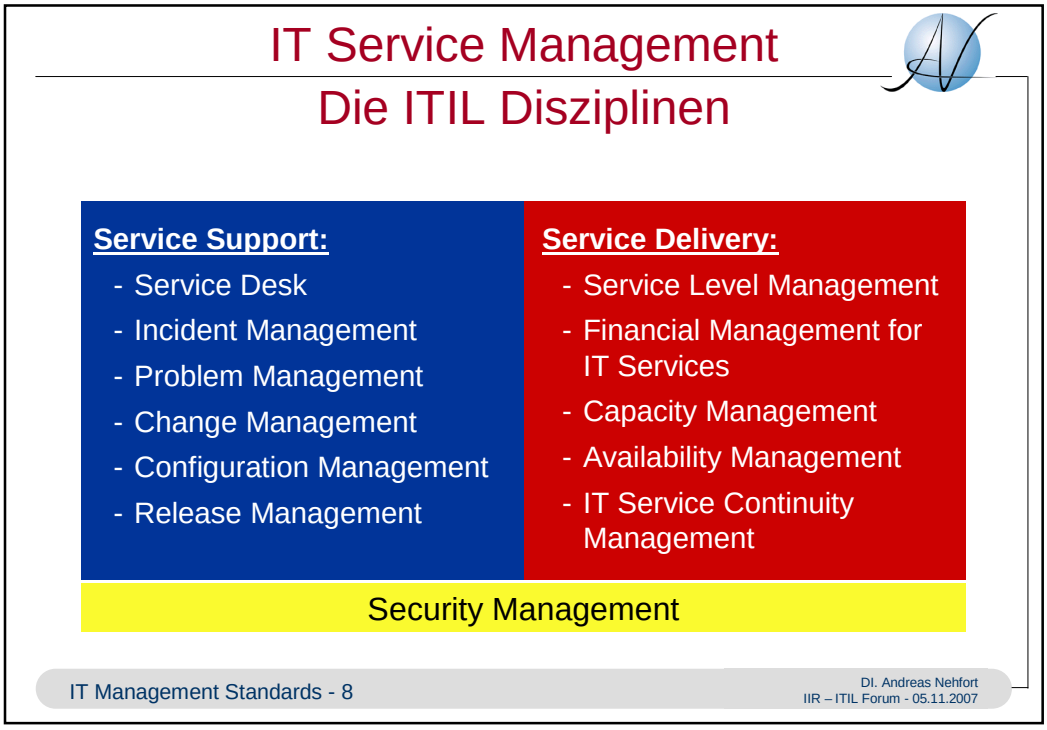



Quelle: Gartner Group

IT Management Standards - 6

DI. Andreas Nehfort
IIR – ITIL Forum - 05.11.2007


ITIL für den IT Betrieb
IT Service Management
Geschäftsleitung
Macht die IT das, was sie soll?
IT Prozessmanagement:
- Prozessverbesserung
- Prozessreife Modelle
- Referenz Prozess-modelle
- Best Practice Modelle
IT Governance:
- Lenkung & Kontrolle
- Control Objectives
- Control Activities
- Control Effectiveness
ITIL
Wie erreichen wir unsere Ziele?
Für den IT Betrieb IT Service Management
IT Management
IT Management Standards - 7
DI. Andreas Nehfort
IIR – ITIL Forum - 05.11.2007


IT Service Management
Die ITIL Disziplinen
Service Support:
- Service Desk
- Incident Management
- Problem Management
- Change Management
- Configuration Management
- Release Management
Service Delivery:
- Service Level Management
- Financial Management for IT Services
- Capacity Management
- Availability Management
- IT Service Continuity Management
Security Management
IT Management Standards - 8
DI. Andreas Nehfort
IIR – ITIL Forum - 05.11.2007

## ISO 20000 – der ISO Standard für IT Service Management

Die ISO 20000 erweitert das ITIL best practice Framework um das Konzept der integrierten Managementsysteme:

- ISO 20000-1: Information Technology – Service Management Part 1: Specification
- ISO 20000-2: Information Technology – Service Management Part 2: Code of Practice

Zweck der ISO 20000 ist die Zertifizierung

- Zertifizierung von Unternehmen auf der Basis Ihrer IT Service Management Prozesse
- Die Zertifizierung nach ISO 20000 wird für IT Service Organisationen das ISO 9001-Zertifikat ersetzen oder ergänzen



## ITIL & ISO 20000

ITIL bildet den inhaltlichen Kern des Standards ISO 20000

Die ISO 20000 hat somit zwei konzeptuelle Wurzeln:

- ISO 9001: Integrierte Managementsysteme
- BS 15000: Der bisherige ITIL-Standard

## ISO 20000 → Manged Services

ISO/IEC 20000 defines the **requirements for a service provider** to deliver **managed services** of an acceptable quality for its customers.

It may be used:

a) by businesses that are going out to tender for their services;

b) by businesses that require a consistent approach by all service providers in a supply chain;

c) by service providers to benchmark their IT service management;

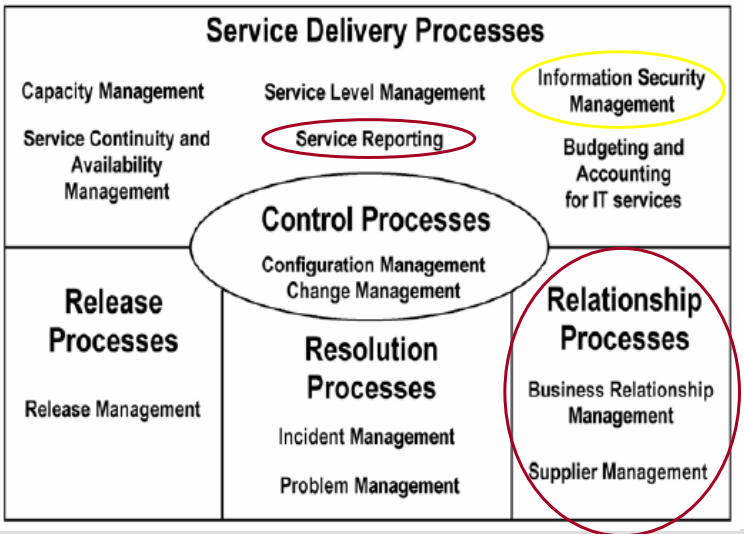
d) as the basis for an independent assessment;

e) by an organization which needs to demonstrate the ability to provide services that meet customer requirements; and

f) by an organization which aims to improve service through the effective application of processes to monitor and improve service quality.



## Service Management Prozesse nach ISO 20000



## ISO 27000ff & ISO 17799:
## Information Security Management

ISO 27000ff: Information Technology – Security Management

- Neue Normenserie zum Information Security Management
- Integriert Information Security Management in integrierte Managementsysteme

Die ISO 27000ff hat somit zwei konzeptuelle Wurzeln

- ISO 9001: Integrierte Managementsysteme
- ISO 17799: der bisherige ISO Standard (früher auch BS7799)



## ISO 27000 und Zertifizierung:

Zweck einer ISO 27000 Zertifizierung:

- Zertifizierung von Unternehmen auf der Basis Ihres Information Security Management Systems
- Die Zertifizierung nach ISO 27000 wird für IT Service Organisationen das Zertifikat nach ISO 9001 bzw. nach ISO 20000-1 ergänzen

Die Bedeutung der Information Security nimmt zu:

- In einer Informationsgesellschaft wird „Information Security“ zu einem gesellschaftlichen Grundbedürfnis
- Die Anforderungen an „Information Security“ steigen ...

## ISO 27000ff: Information Technology Security Management

- **ISO 27000** – principles and vocabulary (in Arbeit - CD)
- **ISO 27001** – ISMS – requirements
- **ISO 27002** – Code of Practice for ISMS (inhaltlich ident mit ISO 17799:2005)
- **ISO 27003** – ISMS Implementation guidelines (geplant)
- **ISO 27004** – ISMS Metrics and measurement (in Arbeit - CD)
- **ISO 27005** – ISMS Risk Management (in Arbeit - FCD)
- **ISO 27006 – 27010** – „allocation for future use“



## Inhalte der ISO 27001: ISMS – requirements

Chapter 4: Information Security Management Systems

- Establish the ISMS
  - Define a ISMS policy
  - Define a risk assessment approach
  - Identify the risks
  - Select control objective and controls for the treatment of risks
- Implement & operate the ISMS
- monitor & review the ISMS
- Maintain & improve the ISMS

## Inhalte der ISO 27001:
## ISMS – requirements

Chapter 5: Management Responsibility

Chapter 6: Internal ISMS Audits

Chapter 7: Management Review of the ISMS

Chapter 8: ISMS Improvement

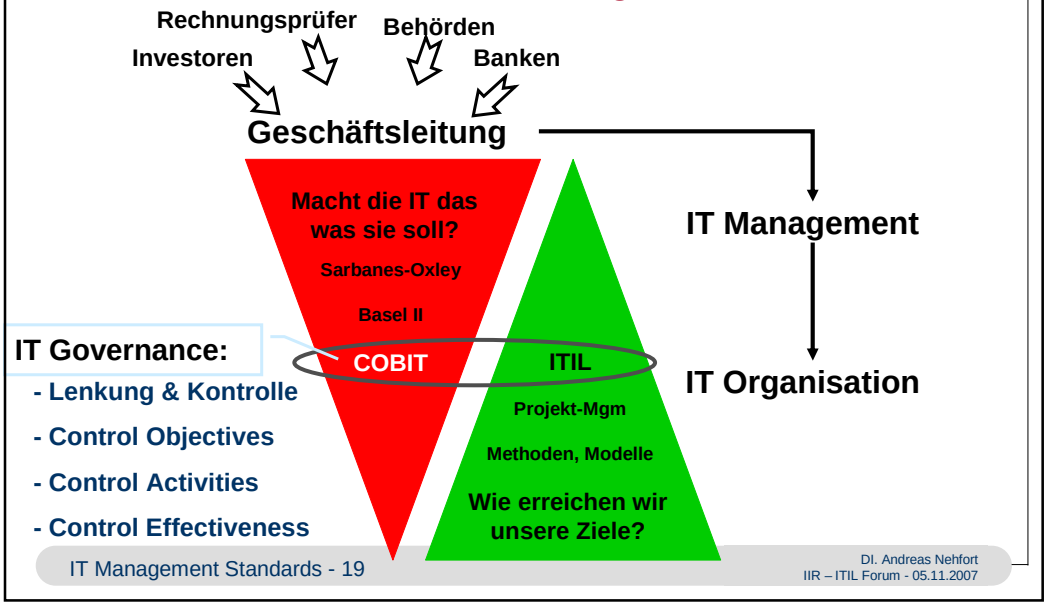
Annex A: Control Objectives and Controls:
Verweis auf die ISO 17799 / ISO 27002



## Inhalte der ISO 17799:2005
## “controls” für “Information Security”

- Security policy
- Organization of information security
- Asset management
- Human resources security
- Physical and environmental security
- Communications and operations management
- Access control
- Information systems acquisition, development and maintenance
- Incident management
- Business continuity management
- Compliance

## Das COBIT Konzept ist auf die Prüfung der IT im Unternehmen ausgerichtet






## COBIT

COBIT ist ein Prozessmodell zur Steuerung und Kontrolle von IT Organisationen

Die 4 „High Level Control Objectives“:

- Plan & Organise
- Acquire & Implement
- Deliver & Support
- Monitor & Evaluate

Cobit ist DAS anerkannte Werkzeug der Wirtschaftsprüfer zur Prüfung von IT Organisationen

## SOX – Sarbanes-Oxley Act

Der Sarbanes-Oxley Act regelt

- Verantwortlichkeiten und Haftungen
- von Unternehmensleitung und Wirtschaftsprüfern
- für die Vollständigkeit und Richtigkeit der Angaben bei der quartalsweisen und jährlichen Berichterstattung:

Verpflichtend für Unternehmen an der NYSE
→ New York Stock Exchange



## SOX – Sarbanes-Oxley Act – Section 404

Der Sarbanes-Oxley Act Section 404 verlangt:

- die Einrichtung eines funktionsfähigen internen Kontrollsystems (Scope: Sämtliche interne Kontrollen, die im Zusammenhang mit der Rechnungslegung stehen)
- dessen Dokumentation
- die Einschätzung und Bewertung der Zweckmäßigkeit dieses Kontrollsystems

Der Jahresabschlussprüfer bestätigt und berichtet über die regelmäßige Einschätzung der Unternehmensleitung.

- D.h .er muss die Wirksamkeit des Kontrollsystems bewerten!

## SOX & IT Governance (2)

Die Finanzdaten entstehen aus der Aggregation der Ergebnisse von IT Services ... die Umsetzung von SOX erfordert daher:

- die Einrichtung eines funktionsfähigen internen Kontrollsystems hinsichtlich der Vollständigkeit und Richtigkeit dieser IT-Ergebnisse
- Die laufende Bewertung der Zweckmäßigkeit und Wirksamkeit dieses Kontrollsystems

Der Sarbanes-Oxley Act Section 404 erfordert daher die Einrichtung eines wirksamen IT-Controllings → IT Governance



## Die 8. EU Richtlinie

**RICHTLINIE 2006/43/EG DES EUROPÄISCHEN PARLAMENTS UND DES RATES vom 17. Mai 2006 über Abschlussprüfungen von Jahresabschlüssen und konsolidierten Abschlüssen**

„ ... Für alle nach Gemeinschaftsrecht vorgeschriebenen Abschlussprüfungen sollte eine gleich bleibend hohe Qualität gewährleistet werden. Alle Abschlussprüfungen sollten deshalb nach **internationalen Prüfungsstandards** durchgeführt werden."

„ ... Ein gutes Mittel zur Erreichung einer gleich bleibend hohen Prüfungsqualität sind regelmäßige Kontrollen. Abschlussprüfer und Prüfungsgesellschaften sollten deshalb einem von den überprüften Abschlussprüfern und Prüfungsgesellschaften unabhängigen Qualitätssicherungssystem unterliegen."

## Die 8. EU Richtlinie

Inhalte der 8. EU Richtlinie (Abschlussprüfer-Richtlinie):

- Scope: Sämtliche qualitätsrelevanten Bereiche der Abschlussprüfung, einschließlich der EDV
- Sicherstellung der Neutralität & Unabhängigkeit der Wirtschaftsprüfer
- Anwendung Internationaler Prüfungsstandards (ein Ziel: internationale Harmonisierung → SOX, Cobit, ...)
- Überwachung des gesamten Rechnungslegungsprozesses
- Überprüfung auf Wirksamkeit des Internen Kontroll Systems (IKS) und ggf. der Innenrevision
- Überprüfung auf Wirksamkeit des Risiko-Management-Systems



## SOX und die 8. EU Richtlinie (2)

Mit der 8. EU Richtlinie (Abschlussprüfer-Richtlinie) werden SOX-ähnliche Regelungen auch in der EU verpflichtend!

Damit wird sich jeder Vorstand einer AG mit folgenden Themen beschäftigen (müssen):

- IT Governance & IT-Controlling
- Risiko Management

Wann wird die 8. EU-Richtlinie wirksam?

- Umsetzung in nationales Recht bis 29. Juni 2008
- Ab dann gelten entsprechende Prüfungsstandards

# EU - Prüfungsstandards

**RICHTLINIE 2006/43/EG DES EUROPÄISCHEN PARLAMENTS UND DES RATES vom 17. Mai 2006 über Abschlussprüfungen von Jahresabschlüssen und konsolidierten Abschlüssen**

Artikel 26 **Prüfungsstandards**

Die Mitgliedstaaten verpflichten die Abschlussprüfer und Prüfungsgesellschaften, Abschlussprüfungen unter Beachtung der von der Kommission nach dem in Artikel 48 Absatz 2 genannten Verfahren **angenommenen internationalen Prüfungsstandards** durchzuführen.

Die Mitgliedstaaten können einen **nationalen Prüfungsstandard** so lange anwenden, wie die Kommission keinen internationalen Prüfungsstandard, der für denselben Bereich gilt, angenommen hat.

Angenommene internationale Prüfungsstandards werden vollständig in jeder der Amtssprachen der Gemeinschaft im *Amtsblatt der Europäischen Union* veröffentlicht.



# EU – Prüfungsstandards ...

„Aufgrund der Erfahrungen mit der Umsetzung von SOX 404 bleibt jedoch zu wünschen, dass der europäische Standardsetter aus den amerikanischen Lektionen seine eigenen Schlüsse zieht und einen weniger stur Compliance-orientierten Ansatz wählt, dafür aber stärker in Richtung Performance zielt“

**Aus einem KPMG-Artikel**

**... Wir werden sehen ...**

## Wir haben eine Fülle an Standards ...

## Was sagen Andere dazu?

The main point is, that even though all of these frameworks and standards are quite useful and helpful for security controls purposes, no single one of them alone is absolute and complete guidance.

- CobiT lacks implementation guidance.
- ISO 27001 probably has some flaws as well.
- ITIL does not address security and governance as one would wish.
- SAS 70 while letting organizations know whether their existing controls are working doesn't tell them if all the right controls are in place.

So, none of the frameworks and standards alone provide full security.

I think the best practice would be to use the combination of different frameworks, choosing the best practices from each and fitting it to the company needs!

**Bob Violino – Computerworld, April 2006**



## Was machen Andere?

We use:

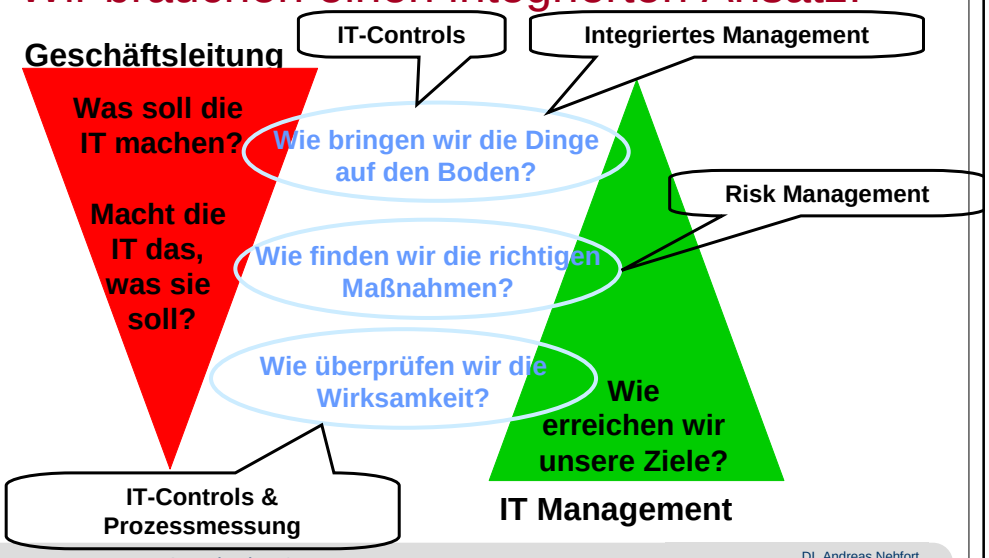
- ITIL to improve internal IT services,
- ISO 27001 for IT governance, and
- CobiT for measuring and assessing IT controls

**Kimberly Sawyer, Lockheed Martin Corp.'s**, Orlando, vice president of computing and network services

- "All of these frameworks supply IT with repeatable processes that are consistent across the various IT functions" and help technology executives provide better service.“
- „But none of the standards alone provides full security“
- "They contain various information security concepts that must be interpreted, integrated and incorporated into the daily operations“
- "Comprehensive security requires discipline and integration across all aspects of planning, service delivery, risk management architecture, tool selection, policy development and audits."

## Die Botschaft:

## Wir brauchen einen integrierten Ansatz!






## Basistechniken für IT-Management & IT Governance (enabler - 1)

Integrierte Managementsysteme:

- Die Verbindung von der Leitung zur Umsetzung (Vorgabe)
- Die Verbindung von der Umsetzung (Ergebnisse) zur Leitung

Risk Management

- Erkennen des Risikos → Akteptanz & Vorbeugung
- Zielgerichtete Auswahl von Maßnahmen

## Basistechniken für IT-Management & IT Governance (enabler - 2)

Process-Controls und Prozess-Messung:

- „controls“ = „Steuerung“, „Stellvorrichtung“
  - „to be at the controls“ = „an den Hebeln der Macht sitzen“
- Zur Steuerung → Zielvorgabe & Lenkung
- Zur Kontrolle der Wirksamkeit → Erfolgskontrolle

Projektmanagement:

- Zur Beherrschung der Veränderungssprozesse → Projekte



## Integrierte Managementsysteme:

Elemente eines integrierten Management Systems:

- Verantwortung der Leitung
- Definition der Politik & Vorgabe von Zielen (z.B.: Qualitäts-Politik / Sicherheits-Politik, ...)
- Definition der Verantwortlichkeiten
- Bereitstellung von Ressourcen
- Planung und Umsetzung
- Erfolgskontrolle
- Kontinuierliche Verbesserung

Diese Elemente sind das 1x1 des erfolgreichen Managements

## Risikomanagement

Risikomanagement ist die Schlüsseltechnologie

- für die rationale und zielgerichtete Lenkung der Ressourcen
- auf der Basis unternehmerischer Entscheidungen.



## Die wichtigsten Schritte des Risk Managements:

- Identifikation der Ziele
  (Ein Risiko ist die Gefahr, ein Ziel nicht zu erreichen)
- Risk Assessment → Standortbestimmung:
  - Wie groß ist unser Risiko-Potential?
  - Welche Risiken haben wir?
- Mit welchen Risiken können wir leben, mit welchen nicht?
  → Identifikation von Handlungsbedarf
- Auswahl von Maßnahmen anhand klarer Kriterien
- Planung und Umsetzung der Maßnahmen
- Erfolgskontrolle

# Risikomanagement in den betrachteten Modellen

Risikomanagement ist:

- Ein Management Prozess in CMMI & SPICE
- Ein Teil eines Service Management Systems nach ISO 20000
- Der Schlüsselprozess im Information Security Management nach ISO 27001 & ISO 17799
- Die Maßnahme in der IT-Governance (COBIT) zur Identifikation der Control Objectives und zur Selection der Controls
- Der Schlüsselprozess in SOX und SAS70 zur Identifikation der relevanten Control Objectives und zur Selection der Controls
- Im modernen Projektmanagement nicht mehr weg zu denken!

Risk Management ist ein Lenkungsprozess in allen relevanten Standards

Risikomanagement & Sicherheitsmanagement: zwei Seiten einer Medaille!



# IT-Controls & Prozessmessung (1)

IT-Controls & Prozessmessung sind die Schlüsseltechnologien

- für die Beobachtung & Kontrolle von Risiken
- Für die Prozesslenkung → Zielvorgaben
- Für die Erfolgskontrolle

IT-Controls & Prozessmessung spielen in **allen** relevanten Modellen und Standards eine wichtige Rolle!

## IT-Controls & Prozessmessung (2)

IT-Controls & Prozessmessung sind

- In den Reifegradmodellen ein Merkmal der Prozessreife
  - In unterschiedlichen Ausprägungen auf Capability Level 2, CL3 & CL4
  - Für Projektmanagement schon auf CL 2 erforderlich
- In den Best Practice Modellen ein Merkmal der Erfolgskontrolle
- Die zentrale Maßnahme in der IT-Governance (COBIT)
- Notwendige Begleitmaßnahmen für SOX
- Das zentrale Element für ein SAS 70 Audit



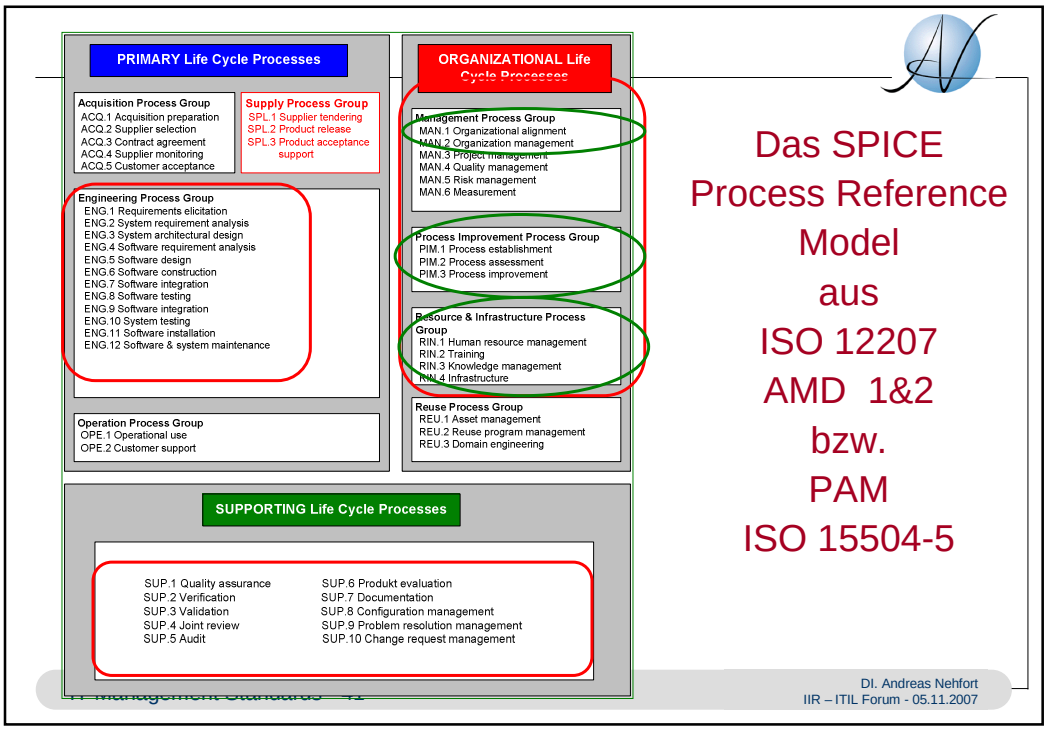
## CMMI & SPICE / ISO 15504

Referenzmodelle für Software & Systems Engineering

- Anforderungen an die Prozessdurchführung
  - Capability Level 1 → spezifische Praktiken

Referenzmodelle für die Prozessreife / Prozessqualität

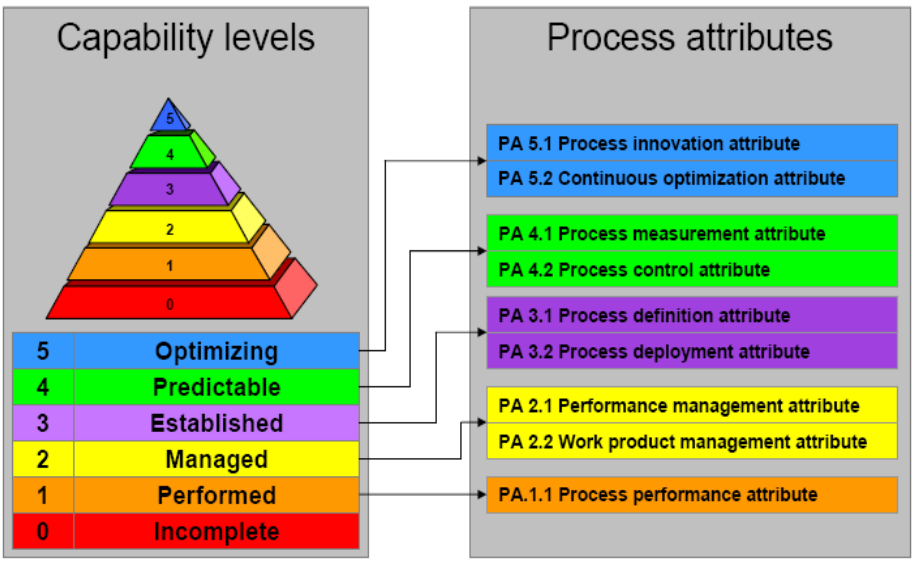
- Capability Level 2 → Managed Processes
- Capability Level 3 → Defined Standard Processes
- Capability Level 4 → Quantitatively Managed Processes




Das SPICE Process Reference Model aus ISO 12207 AMD 1&2 bzw. PAM ISO 15504-5

DI. Andreas Nehfort
IIR – ITIL Forum - 05.11.2007

## Die SPICE-Prozessattribute




IT Management Standards - 42

DI. Andreas Nehfort
IIR – ITIL Forum - 05.11.2007

## Prozessreife / Process Capability

**Beschreibt die Fähigkeit eines Prozesses seine Ziele zu erreichen, mittels:**

- Prozessplanung
- Prozessdurchführung & definierte Ergebnisse
- Prozesslenkung & Prozessmessung
- Prozessverbesserung

Mit **zunehmender** Process Capability

- werden die Ergebnisse des Prozesses **besser vorhersagbar**!
- **Sinkt das Risiko** unterwarteter / unerwünschter Ergebnisse

→ **Prozessreife als Instrument für IT-Governance!**



## Welche Standards / Zauberwörter sind damit interessant?

IT-Service Management → ISO 20000

- Managed Services als Basis für den Erfolg

Information Security Management → ISO 27000

- Das ist ein gesellschaftliches Anliegen geworden!

Risk Management → ISO 17799

- Risikomanagement und Sicherheitsmanagement sind zwei Seiten der selben Medaille!

Control Objectives & IT Controls:

- Standards nach Bedarf: COBIT, ISO 17799, ...

ISO 15504 / SPICE → Prozessreife

## Empfehlungen → Basistechniken

Forcierung eines Integrierten Managementsystems nach den Modellen der ISO 9001, ISO 20000, ISO 27000

Etablierung eines Risiko Management Systems

- Wie für ISO 27001 & ISO 17799 benötigt
- Hilfreich dafür ist auch die ONR 49000ff: Risikomanagement

Etablierung eines Control- & Messprozesses

- Hilfreich dafür ist die ISO 15939: Software Measurement Process

Diese Maßnahmen machen uns fit und beweglich!



## Empfehlungen → Prozessmanagement und IT Governance (1)

Management der Leistungsprozesse:

- SW-Entwicklung → CMMI oder SPICE
- IT Service Management → ITIL & ISO 20000

Etablierung eines Information Security Management Systems

- Nach ISO 27001 & ISO 17799

Etablierung der IT Controls zur Deckung der internen IT Governance Bedürfnisse

- Auf Basis eines Risk Assessments
- Orientiert an COBIT bzw. an den ISO 17799 - Controls

## Empfehlungen → Prozessmanagement und IT Governance (1)

Etablierung der IT Controls zur Deckung der externen IT Governance Bedürfnisse

- Orientiert an COBIT, ISO 17799,
- Orientierung an den externen Vorschriften (EU-Prüfungsstandards, SOX, SAS 70, ... what ever, ..)

Prüfung welche Zertifizierungen Sinn machen ...

- Aufwand & Kosten der Zertifizierung
- Interner Nutzen der Zertifizierung
- Außenwirkung des Zertifikats, ...



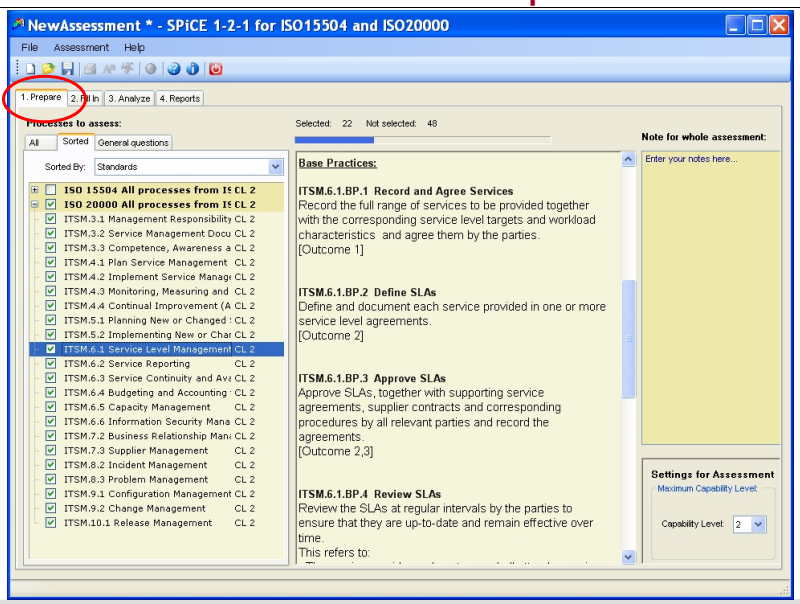
## Assessment Based Process Improvement A-B-P-I

**Prozessverbesserung in 4 Schritten:**

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

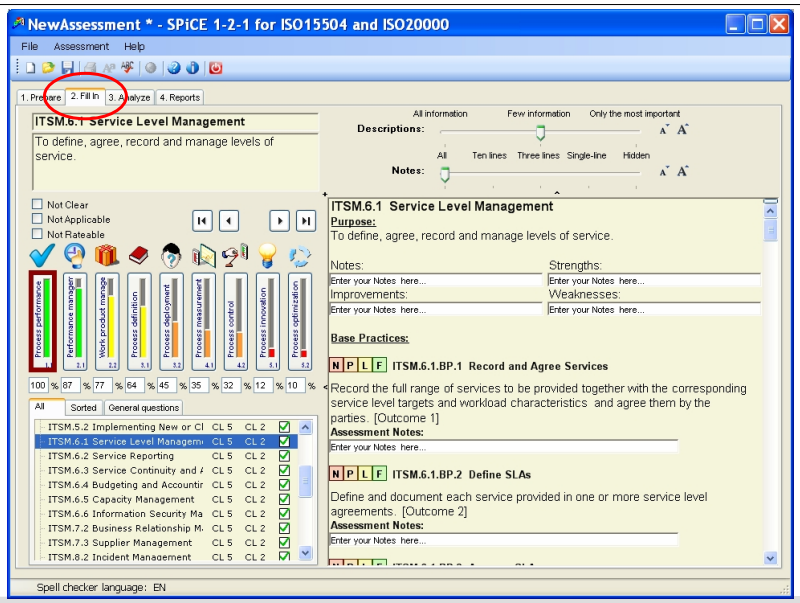
Auf der Basis der ISO/IEC 15504 / SPICE

# SPICE 1-2-1: Prepare

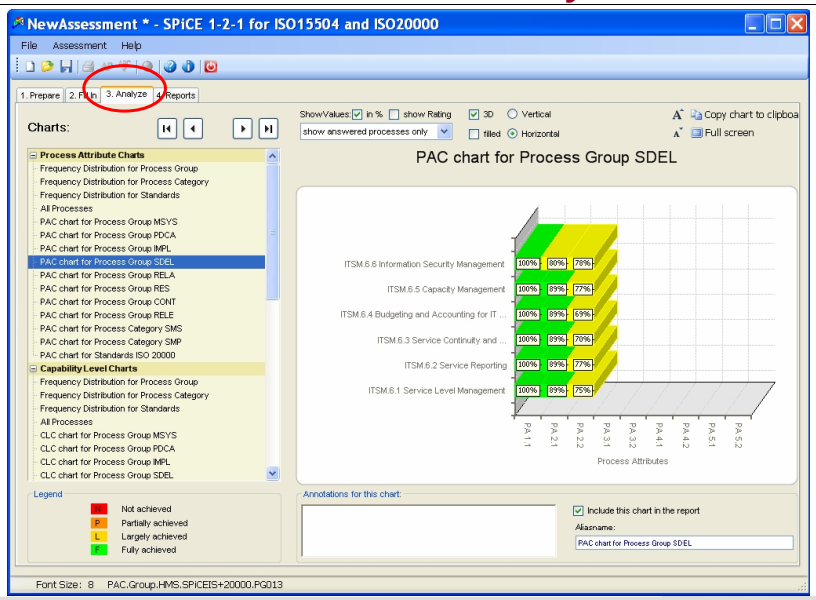





# SPICE 1-2-1: Fill-In

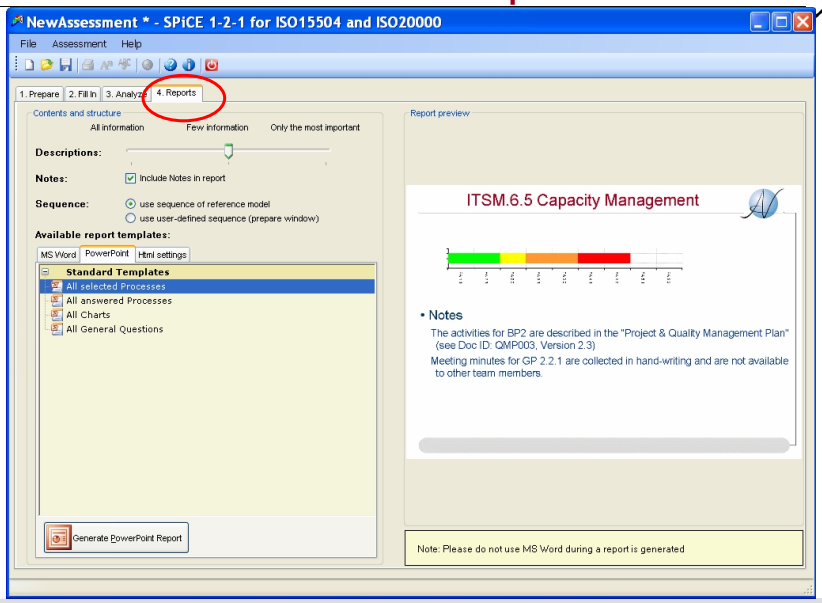


# SPICE 1-2-1: Analyze






# SPICE 1-2-1: Reports



## Assessments für Ihr integriertes Management System

SPICE 1-2-1 integriert schrittweise folgende Standards:

- ISO 15505-5 → Software Engineering
- ISO 15504-6 →Systems Engineering
- ISO 20000-1 → IT Service Management
- ISO 27001 → Information Security Management
- ISO 27002 → IT Security Controls
- **Ihre spezifischen Prozesse & Controls**



## Danke für Ihre Aufmerksamkeit!

Fragen & Anmerkungen

Diskussion ...