



Das Quality ABC: Standards und Begriffe richtig einordnen und verwenden

IIR Fachkonferenz: Software Testing Management

DI. Andreas Nehfort

andreas@nehfort.at

www.nehfort.at

Quality ABC - 1

DI. Andreas Nehfort
IIR Fachkonferenz - 28.02.2008

Agenda



- Vorstellung
- Standards und Begriffe aus der Test Welt
 - ISTQB/ATB: Standards in der Ausbildung von Testern
- Standards und Begriffe aus der Software Prozesswelt und
Ihr Bezug zum Thema Testen
 - Software Prozessmanagement Standards → SPICE/CMMI
 - IT Service Management Standards → ITIL/ISO 20000
 - IT Governance Standards → Cobit / SOX / 8. EU Richtlinie
 - Information Security Management → ISO 27000ff:
 - Sicherheit: Security & Safety
- Resumee

Quality ABC - 2

DI. Andreas Nehfort
IIR Fachkonferenz - 28.02.2008

Vorstellung Andreas Nehfort



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

- Software Prozesse → Assessment Based Process Improvement:
 - Software Engineering: CMMI & SPiCE
 - IT Service Management & Information Security Management
- IT-Projektmanagement, Qualitätsmanagement, Requirements

Qualifikationen / Zertifikate:

- iNTACS Certified Competent Assessor für SPICE & Automotive SPICE
- CMMI V1.2 Upgrade
- /tsmf certified ISO 20000 Consultant

Background:

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

Quality ABC - 3

DI. Andreas Nehfort
IIR Fachkonferenz - 28.02.2008

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 / RUP - Rational Unified Process
- Network selbständiger Berater, Trainer, Assessoren:
 - Software Engineering & Projektmanagement
 - IT Service Management & IT Security Management

Nehfort IT-Consulting vertritt Kugler Maag CIE in Österreich!

Quality ABC - 4

DI. Andreas Nehfort
IIR Fachkonferenz - 28.02.2008

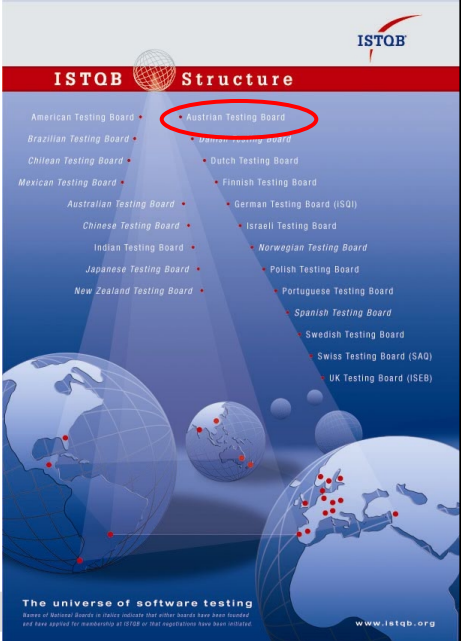


ISTQB – Was ist das?

International **S**oftware **T**esting
Qualification **B**oard

- International anerkanntes Ausbildungskonzept für Tester
→ **ISTQB Certified Tester**
- 36 Nationale Boards
 - Austrian Testing Board

www.austriantestingboard.at



The diagram shows the ISTQB Structure with 36 National Testing Boards listed. The Austrian Testing Board is circled in red. The boards are: American, Brazilian, Chilean, Mexican, Australian, Chinese, Indian, Japanese, New Zealand, Austrian, Dutch, Finnish, German (ISQI), Israeli, Norwegian, Polish, Portuguese, Spanish, Swedish, Swiss (SAQ), and UK (ISEB). The title 'ISTQB Structure' is at the top. At the bottom, it says 'The universe of software testing' and 'www.istqb.org'.

Quality ABC - 5



ISTQB - Certified Tester

Definierte Qualifikationsprofile → ISTQB - Certified Tester:

- **Foundation Level:** Basisausbildung zum Tester
- **Advanced Level:** Test Analyst, Techn. Test Analyst, Testmanager
- **Expert Level:** ...daran wird gearbeitet ...

Einheitliche Ausbildung:

- Auf Basis des jeweiligen ISTQB-Syllabus
- Durch akkreditierte Trainingsanbieter

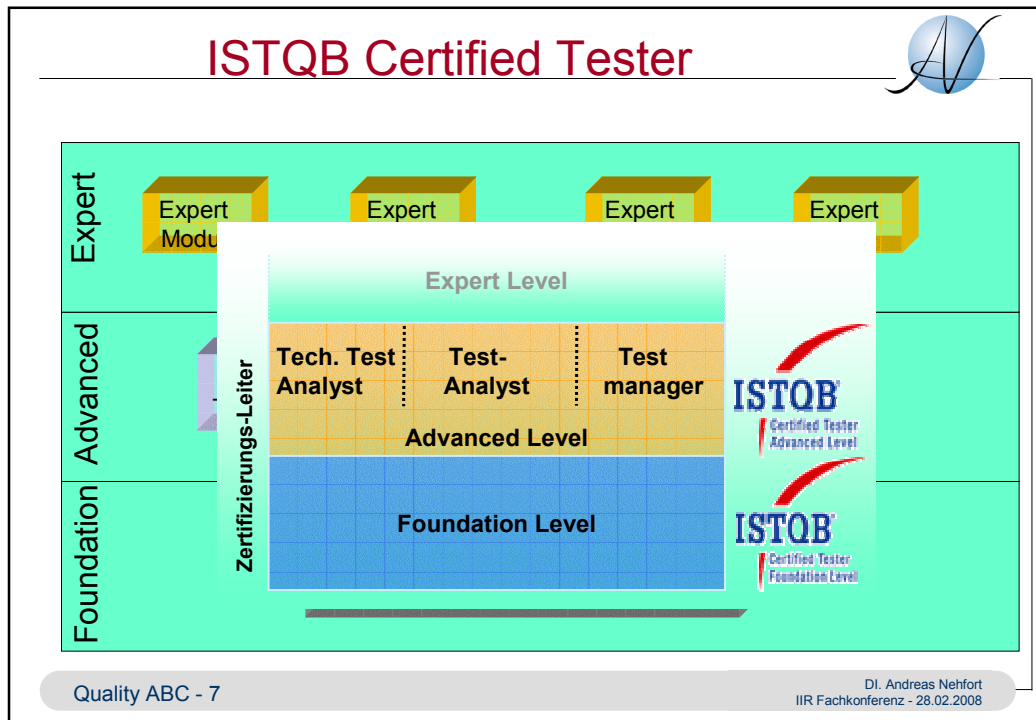
Einheitliche Begriffswelt für das Testen:

- Als Basis für den Syllabus
- „Standard glossary of terms used in Software Testing V2.0“

(Download → **www.austriantestingboard.at**)

Quality ABC - 6

DI. Andreas Nehfort
IIR Fachkonferenz - 28.02.2008



ISTQB - Testlevel & Testtypes



Teststufen (Testlevel):

- Komponententest
- Integrationstest
- Systemtest
- Abnahmetest

Testarten (Testtypes):

- Funktionale Tests
- Nicht funktionale Tests
- Strukturorientierte Tests
- Nachtests & Regressionstests

Quality ABC - 9

DI. Andreas Nehfort
IIR Fachkonferenz - 28.02.2008

Wozu ISTQB Certified Tester?



- Die ISTQB Trainings vermitteln das Handwerkszeug!
- ISTQB schafft eine Tester-Community!
- ISTQB gestaltet das Berufsbild des Testers!
- ISTQB setzt Standards!

Damit wird eine Diskussionsgrundlage geschaffen:

- Was sollte ein Tester können?
- Was sind seine Aufgaben?
- Was ist ein „vernünftiger Testprozess“
- Was ist „Stand der Technik“?

Quality ABC - 10

DI. Andreas Nehfort
IIR Fachkonferenz - 28.02.2008

Prozessreifegradmodelle Die aktuellen Referenzmodelle



CMMI: Capability Maturity Model Integrated

- CMMI-DEV V1.2: CMMI for Development
- Herausgeber:
Carnegie Mellon University – Software Engineering Institute

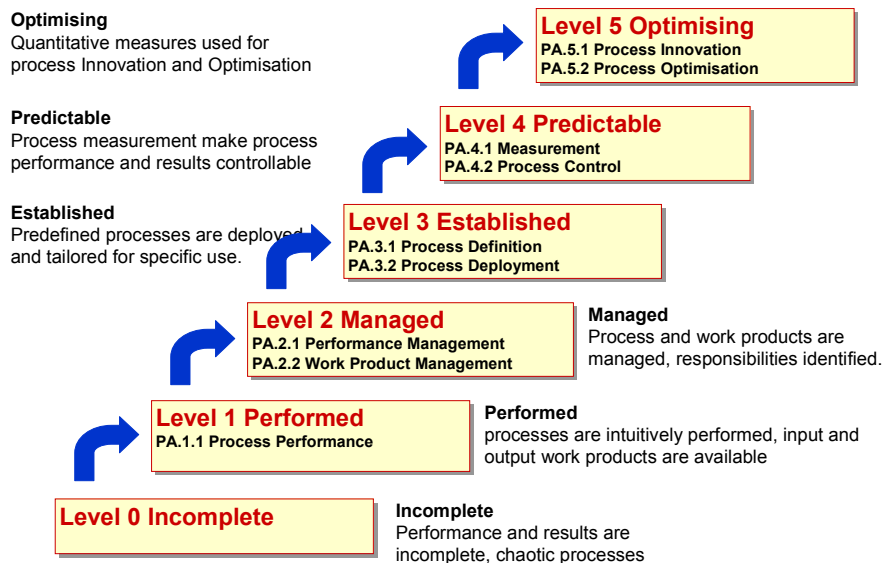
SPICE: Software Process Improvement & Capability determination

- ISO/IEC 15504: Information Technology –
Process Assessment
- Herausgeber: ISO – International Standards Organisation

Quality ABC - 11

DI. Andreas Nehfort
IIR Fachkonferenz - 28.02.2008

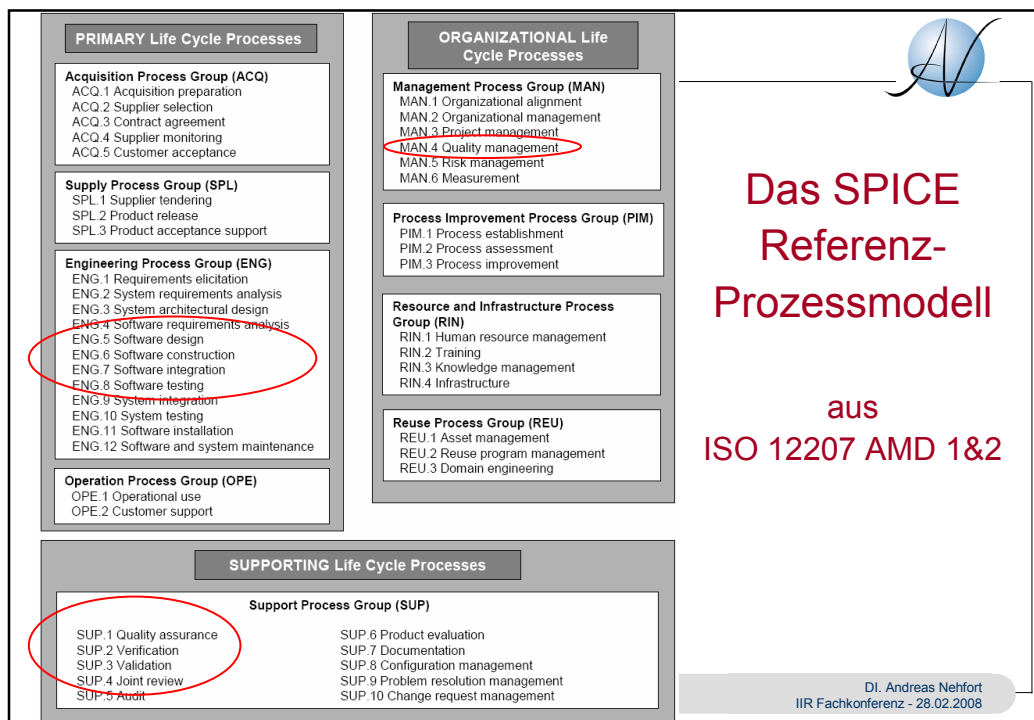
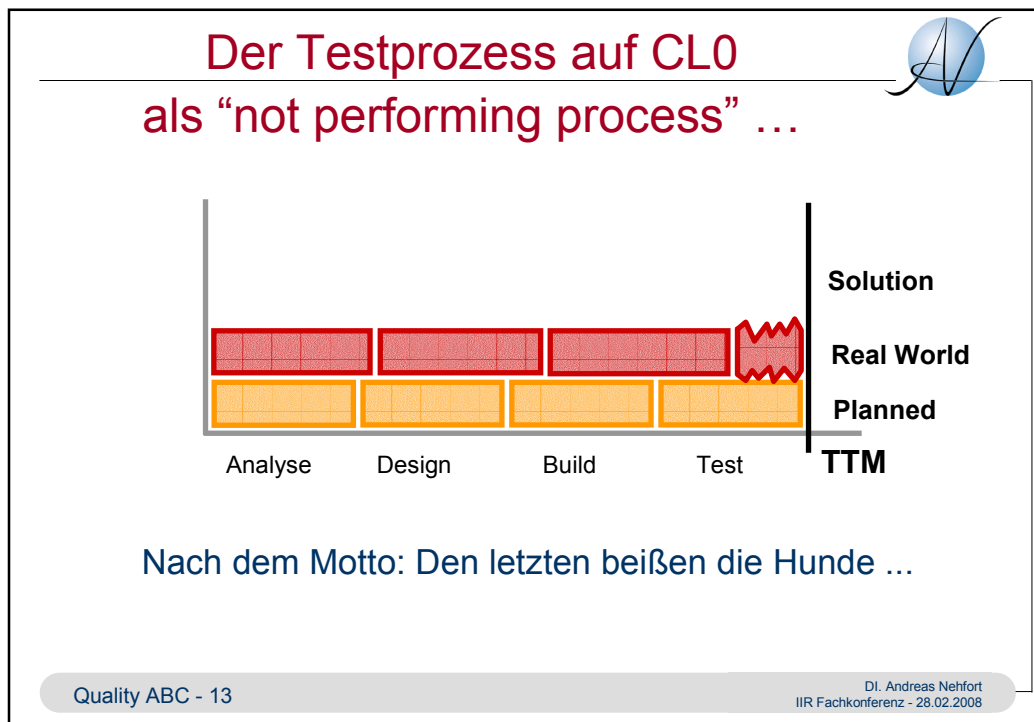
SPICE-Capability Levels



Quality ABC - 12

Die Referenzmodelle

DI. Andreas Nehfort
IIR Fachkonferenz - 28.02.2008



Verifikation & Validierung



Verifikation:

- Bestätigung durch Bereitstellung eines objektiven Nachweises, dass **festgelegte Anforderungen** erfüllt worden sind

ISO 9000:2000

Validierung:

- Bestätigung durch Bereitstellung eines objektiven Nachweises, dass die **Anforderungen** für einen **spezifischen beabsichtigten Gebrauch** oder eine **spezifische beabsichtigte Anwendung** erfüllt worden sind.

ISO 9000:2000

Quality ABC - 15

DI. Andreas Nehfort
IIR Fachkonferenz - 28.02.2008

Testen ⇔ Qualitätssicherung



Quality Assurance Process (ISO 15540-5):

„The purpose of the quality assurance process is to **provide assurance** that work products and processes comply with **predefined provisions and plans**“

Verifikation & Validierung:

→ Prüfung gegen „**Anforderungen**“

Qualitätssicherung:

→ Prüfung gegen „**vorab definierte Vorschriften & Pläne**“

Quality ABC - 16

DI. Andreas Nehfort
IIR Fachkonferenz - 28.02.2008

Testen im IT Service Management ITIL & ISO 20000



In ITIL und ISO 20000 spielt der Begriff „Testen“ eine untergeordnete Rolle.

Testen kommt meist nur indirekt vor:

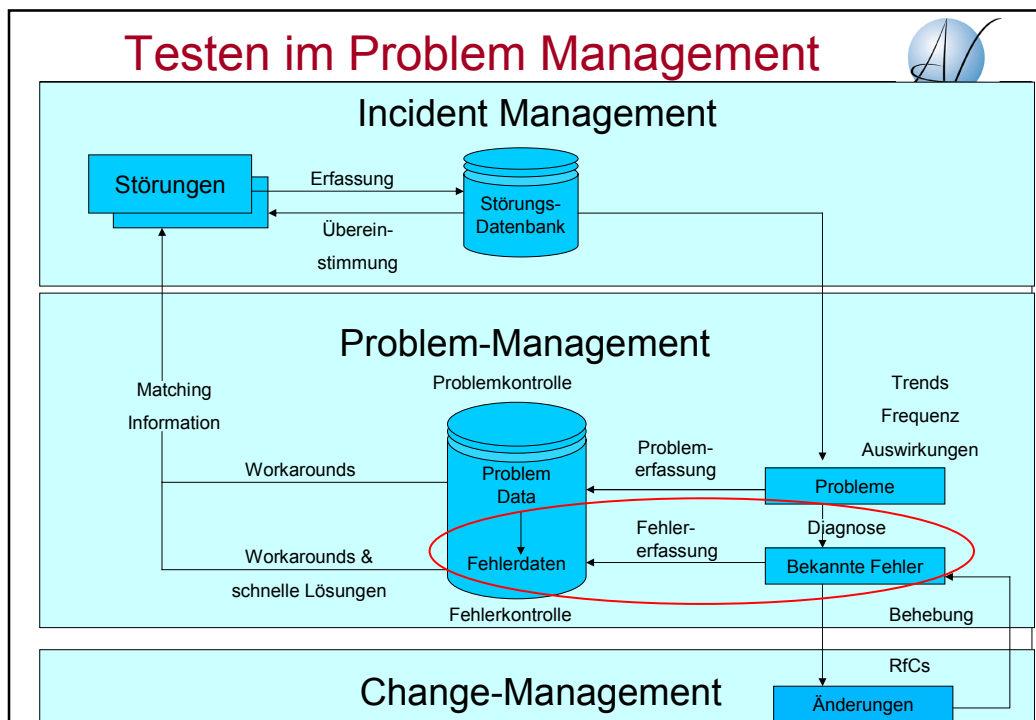
- als Tätigkeit im „**Problem Management**“ → **Diagnose**
- Als Tätigkeit in „**Change Management**“ → **Freigabe**
- Als Tätigkeit im „**Release Management**“ → **Freigabe**

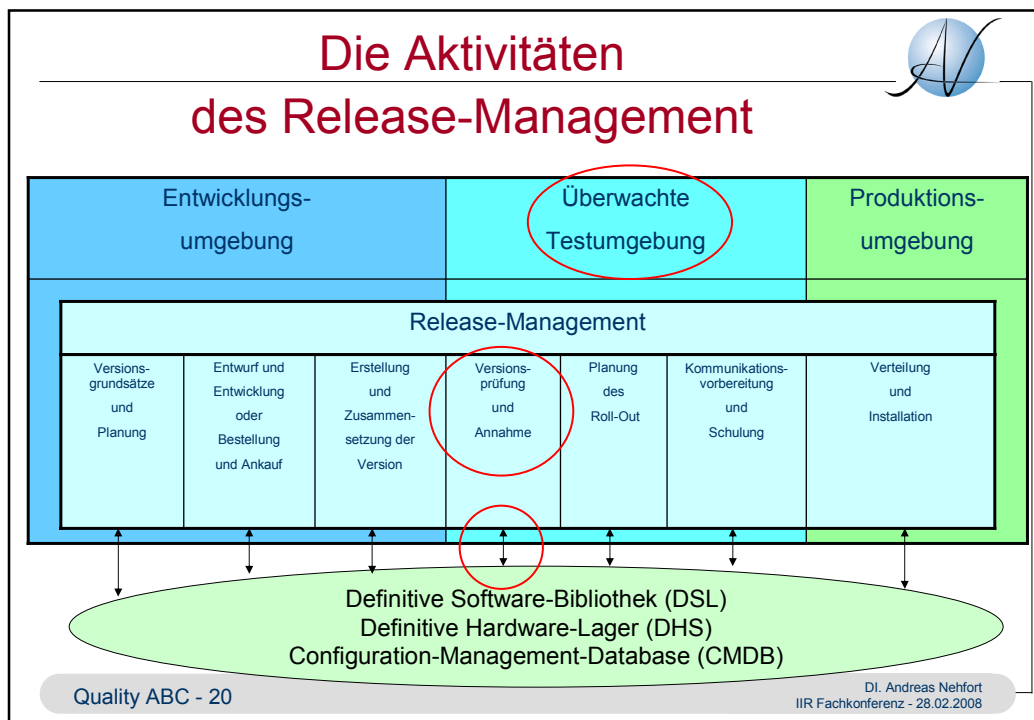
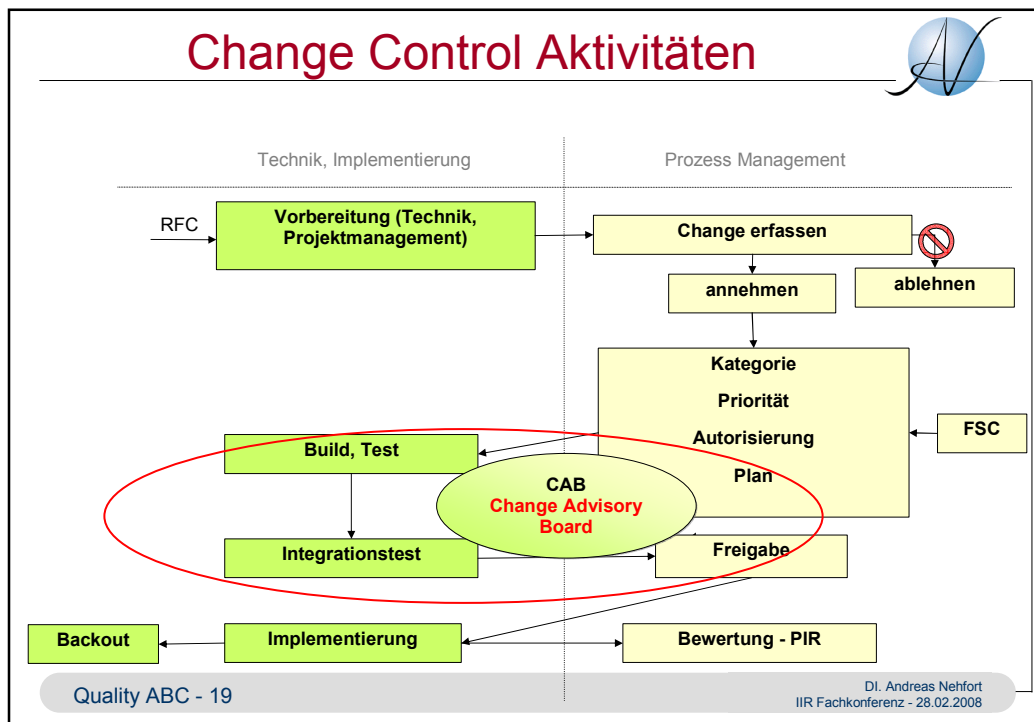
Die Anforderungen des IT Service Managements ans Testen entstehen aus der geforderten Integration in die IT Service Management Prozesse ...

Quality ABC - 17

DI. Andreas Nehfort
IIR Fachkonferenz - 28.02.2008

Testen im Problem Management





Testen in der ISO 20000



Configuration management:

- Configuration Items shall be referenced to Testing Products

Service continuity and availability management:

- The availability and service continuity plans shall be **re-tested** at every major change to the business environment.
- The service continuity plan shall be **tested** in accordance with business needs.
- All **continuity tests** shall be recorded and **test failures** shall be formulated into action plans.

Releasemanagement:

- A **controlled acceptance test environment** shall be established to build and test all releases prior to distribution.

Quality ABC - 21

DI. Andreas Nehfort
IIR Fachkonferenz - 28.02.2008



Quality ABC - 22

DI. Andreas Nehfort
IIR Fachkonferenz - 28.02.2008

Sicherheit: Security & Safety



Security:

- The capability of the software product **to protect information and data** so that **unauthorised persons** or systems cannot read or modify them and authorised persons or systems are not denied access to them.
- **Schutz der Informationen vor unbefugten Zugriff**

Safety:

- The capability of the software product **to achieve acceptable levels of risk of harm to people**, business, software, property or the environment in a specified context of use.
- **Schutz der Umwelt vor den Ergebnissen der Software**

ISO 9126-1

Quality ABC - 23

DI. Andreas Nehfort
IIR Fachkonferenz - 28.02.2008

IEC 61 508 Funktionssicherheit ...



IEC 61 508 betrifft sogenannte **E/E/EP-Systeme**:
Elektrische / Elektronische / Elektronische programmierbare Systeme

Der Safety-Lifecycel:

- Gefährdungs- und Risikoanalyse → Sicherheitsrisiken
- Ermittlung der **Sicherheitsklasse** des Produkts
 - **SIL - Safety Integrity Level: SIL 0 bis SIL 4**
- Daraus werden die **Sicherheitsanforderungen** an das Produkt abgeleitet → Versagenswahrscheinlichkeit
- Diese werden mit **produktorientierten Maßnahmen** umgesetzt.

Letztendlich gilt es diese Maßnahmen durch geeignete Prozesse sicherzustellen.

Quality ABC - 24

DI. Andreas Nehfort
IIR Fachkonferenz - 28.02.2008

IT-Governance & Information Security

Verantwortung der Leitung

SOX / SAS70: Sarbanes Oxley Act

- US Vorschriften für die Sicherstellung der Vertrauenswürdigkeit von Unternehmensdaten

8. EU Rahmenrichtlinie: Wirtschaftsprüferrichtlinie

- Mindestanforderungen an Qualitätssicherungssysteme für die Abschlussprüfung in der EU

Cobit: Control Objectives for IT and related Technology

- Referenzmodell zur Prüfung von Abläufen in der IT eines Unternehmen (→ IT Governance)

Quality ABC - 25

DI. Andreas Nehfort
IIR Fachkonferenz - 28.02.2008

IT-Governance & Information Security

Sicherstellung der **Integrität**, **Verfügbarkeit** & **Vertraulichkeit** von Unternehmensdaten

Integrity / Integrität:

- Richtigkeit und Vollständigkeit

Availability / Verfügbarkeit:

- für Befugte zugreifbar und brauchbar

Confidentiality / Vertraulichkeit:

- für Unbefugte nicht verfügbar

Information Security Management → **ISO 27000ff**

Quality ABC - 26

DI. Andreas Nehfort
IIR Fachkonferenz - 28.02.2008

Information Security



Das Security Bedürfnis:

- Schutz vor Fehlern in der Datenverarbeitung
- Schutz vor unbefugter Verfälschung der Ergebnisse

Die Maßnahmen (Security Controls):

- Anforderungen an das Management & die Prozesse
- Anforderungen an die Applikationen
- Anforderungen an die IT-Systeme
- Anforderungen an den Betrieb der IT-Systeme

Die Konsequenzen:

- **Anforderungen an die Entwicklung und das Testen!**

Quality ABC - 27

DI. Andreas Nehfort
IIR Fachkonferenz - 28.02.2008

Ein paar Hauptthemen



→ Applikationen:

- Security Anforderungen definieren
- Gegen die Security Anforderungen verifizieren / testen
- Für einen sicheren Betrieb sorgen.

→ Zugriffsschutz & Rechte:

- System, Netzwerk, Applikation, Daten

→ Betriebsüberwachung:

- Unbefugter Zugriff → Security Incidents, ...

Quality ABC - 28

DI. Andreas Nehfort
IIR Fachkonferenz - 28.02.2008

Ein Beispiel



Control Objective 12.2 Correct processing in applications

- Objective: To prevent errors, loss, unauthorized modification or misuse of information in applications.

A.12.2.1 Input data validation

- Data input to applications shall be validated to ensure that this data is correct and appropriate.

A.12.2.2 Control of internal processing

- Validation checks shall be incorporated into applications to detect any corruption of information through processing errors or deliberate acts.

A.12.2.3 Message integrity

- Requirements for ensuring authenticity and protecting message integrity in applications shall be identified, and appropriate controls identified and implemented.

A.12.2.4 Output data validation

- Data output from an application shall be validated to ensure that the processing of stored information is correct and appropriate to the circumstances.

Quality ABC - 29

DI. Andreas Nehfort
IIR Fachkonferenz - 28.02.2008

Wichtig für die IT-Governance



Internes Kontroll System:

- Einrichten und Aufrecht erhalten
- Sicherstellung der Wirksamkeit

Nachvollziehbarkeit der Maßnahmen für Außenstehende:

- Für Manager
- Für Auditoren / Assessoren
- Für Wirtschaftsprüfer

Dokumentation und Aufzeichnungen:

- Nachvollziehbare Ausführung von Control Aktivitäten
- Nachvollziehbare Ergebnisse der Control Aktivitäten

Quality ABC - 30

DI. Andreas Nehfort
IIR Fachkonferenz - 28.02.2008

Resumee



Der IT Betrieb hat zusätzliche Test-Anforderungen:

- IT Service Management
- IT Governance & Information Security Management

Die Anforderungen an IT-Applikationen steigen!

- Je stärker IT-Applikationen in das alltägliche Leben eingreifen, desto mehr werden sie durch (gesetzlichen) Anforderungen reglementiert ...

Damit steigen auch

- Die Anforderungen an die **Entwicklung!**
- die Anforderungen an das **Testen!**
- die Anforderungen an die **Qualifikation der Tester!**

Quality ABC - 31

DI. Andreas Nehfort
IIR Fachkonferenz - 28.02.2008

Resumee (2)



Die Rahmenbedingungen:

- Der Gesetzgeber verlangt „**Stand der Technik**“
- Nicht „Stand der Technik“ ist **fahrlässig!**
- Wer fahrlässig handelt ist **strafrechtlich haftbar!**

Nötige Maßnahmen:

- Ausbildung der Tester → z.B. ISTQB Certified ...
- Kenntnis & Anwendung der relevanten Regularien
- Nachweis der Sorgfaltspflicht → Aufzeichnungen
 - z.B. der Testpläne, Der Testdaten & der Testergebnisse

Quality ABC - 32

DI. Andreas Nehfort
IIR Fachkonferenz - 28.02.2008