Prozessmanagement-Summit 2009

Prozessreife
und
Informationssicherheit

DI. Andreas Nehfort

andreas@nehfort.at www.nehfort.at

Agenda

- Vorstellung Andreas Nehfort & Nehfort IT-Consulting
- Informationssicherheit – ein gesellschaftliches Bedürfnis
  - Sicherheitslücken und ihre Folgen
  - Informationssicherheit in der Logistik
- Prozessreife und Zuverlässigkeit → Sicherheit
- Das SPICE Prozessreifegrad-Modell (ISO 15504)
  - Die Anforderungen an einen „Defined Process“
  - SPICE als Best Practice für Prozessmanagement
- SPICE 1-2-1 for IT-Governance - Assessment
- Informationssicherheit & Prozessreife

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

Qualifikation & Funktionen:

- SPICE Principal Assessor (iNTACS)
- GPard Lead Assessor
- *It*smf certified ISO 20000 Consultant,
- Vorstandsmitglied im STEV-Österreich → www.softwarequalitaet.at

Background:

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

Prozessreife & Informationssicherheit - 3 — DI. Andreas Nehfort PzM-Summit 2009

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, …)
- GP-Partner
- Network selbständiger Berater, Trainer, Assessoren:
  - Software Engineering & Projektmanagement
  - IT Service Management & IT Security Management

Nehfort IT-Consulting vertritt KUGLER MAAG CIE in Österreich!

Prozessreife & Informationssicherheit - 4 — DI. Andreas Nehfort PzM-Summit 2009

Informationssicherheit bedeutet …

Sicherstellen der Integrität, Verfügbarkeit & Vertraulichkeit von Informationen … und damit verbunden, dass man sich

- auf Korrektheit & Zuverlässigkeit der Informationen verlassen kann …

Integrität:

- Richtig, vollständig, genau

Verfügbarkeit:

- Für Befugte **bei Bedarf** zugreifbar & brauchbar

Vertraulichkeit:

- Schutz vor unbefugtem Zugriff & unbefugter Nutzung

Prozessreife & Informationssicherheit - 5
DI. Andreas Nehfort
PzM-Summit 2009

Die Bedeutung der Informationssicherheit nimmt zu …

Informationssicherheit ist zum gesellschaftlichen Bedürfnis geworden!

- Information: die Werte der Informationsgesellschaft
- Was einen Wert hat, gehört geschützt

Gesetzliche Regelungen entsprechen diesem Bedürfnis

- Datenschutzgesetz,
- e-commerce Richtline,
- SOX / 8. EU Rahmenrichtlinie (für Abschlussprüfer), …

Prozessreife & Informationssicherheit - 6
DI. Andreas Nehfort
PzM-Summit 2009

8. EU Rahmenrichtlinie

Fokus: Sicherstellung der korrekten Rechnungslegung

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

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

- 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**).

Sicherheitslücken und ihre Folgen

Dezember 2008: Datenleck bei LBB

- Kreditkartenabrechnungen zehntausender Kunden quer durch die BRD werden einer Frankfurter Zeitung zugespielt.
- Die Ursache: Sicherheitslücke eines IT-Dienstleisters

Dezember 2008: Milliardenbetrug an der Wallstreet

- Investmenthaus “erwirtschaftet” tolle Renditen aus den Einlagen neuer Kunden → Schaden etwa 65 Milliarden US $
- Die Ursache:
  Bilanzfälschungen blieben über viele Jahre unentdeckt!

Sicherheitslücken im Geschäftsalltag …

10. Oktober 2009: Datenpanne bei AWD

- Daten von 27.000 AWD-Kunden werden NDR zugespielt.
  - Kundendaten, Art & Dauer der Verträge, Vertragssummen

11. Oktober 2009: Datenleck bei schülerVZ gemeldet

- Der deutschen Bürgerrechtsplattform Netzpolitik.org sind über eine Million Datensätze von jugendlichen Nutzern des Sozialen Netzwerks schülerVZ zugespielt worden. Die Betreiber bestätigten mittlerweile die "illegale Datenkopie" und prüfen derzeit, wie die Daten gesammelt wurden …
- Bereits **2006** hatte der deutsche Blogger Don Alphonso mehrfach auf Datenlecks bei der schülerVZ-Mutter studiVZ hingewiesen …

Prozessreife & Informationssicherheit - 9

DI. Andreas Nehfort
PzM-Summit 2009

Sicherheitsbedürfnisse im Geschäftsalltag …

20. Oktober 2009: Spielregeln für smarte Stromzähler

In den nächsten Jahren sollen Stromzähler "intelligenter" werden und damit beim Energiesparen helfen.

Doch die neue Technologie bringt nicht nur Vorteile mit sich:

- Die automatische ferngesteuerte Auslesung der Verbraucherdaten könnte das Datenschutzgesetz verletzen.

Österreichische Netzbetreiber, die Pilotprojekte betreiben, weisen mögliche Probleme zurück …

Prozessreife & Informationssicherheit - 10

DI. Andreas Nehfort
PzM-Summit 2009

Die Konsequenzen im Geschäftsalltag …
Deutsche Bahn akzeptiert Bußgeld

23.Oktober 2009: 1,12 Millionen Euro Forderungen

Die Deutsche Bahn zahlt eine Strafe von 1,12 Millionen € für **Verstöße gegen den Datenschutz** im Unternehmen.

Das teilte der Berliner Datenschutzbeauftragte Alexander Dix am Freitag in Berlin mit.

Geahndet werden damit mehrere Vorfälle der Affäre, bei denen die Daten von Mitarbeitern heimlich mit denen von Lieferanten der Bahn abgeglichen wurden …

Verleihung des Big Brother Awards Austria

25. Oktober im Wiener Rabenhoftheater

In Österreich findet die Verleihung der Big Brother Awards bereits zum elften Mal traditionell am 25. Oktober statt.

Die Gewinner bekommen einen Preis und einen Platz in der **"Hall of Shame"**, so wie ihre Vorgänger der letzten zehn Jahre.

Die Preisträger des Jahres 2009 finden Sie unter

→ http://www.bigbrotherawards.at/2009/Preistraeger

November 2009: Probleme mit Kreditkarten

16.11.2009: Sicherheitsloch in Spanien:

- Kreditkarten-Datenklau trifft alle deutschen Banken
- Nach bisherigen Erkenntnissen des Kreditausschusses sind in diesem Jahr Daten bei einem Finanzdienstleister in Spanien abhanden gekommen …

Größte Rückrufaktion aller Zeiten

- Aus Angst vor Datenmissbrauch haben Banken die bisher größte Umtauschaktion von Kreditkarten in Deutschland begonnen.
- Die Zahl der eingezogenen Kreditkarten beträgt bereits mehr als 100.000 ! **"Financial Times Deutschland"**

Die Folgen dieses Security Incidents im Kreditkartengeschäft

Vertrauensverluste der Kunden:

- Zurückhaltung in der Nutzung von Kreditkarten
- Umsatzverluste für VISA & MasterCard

Die direkten Kosten:

- Info & Servicehotlines
  - für mehr als 100.000 betroffene Kunden
  - und für Millionen nicht direkt betroffene Kunden.
- Der Austausch von mehr als 100.000 Karten
- Die Überprüfung von Millionen Buchungen, …

Informationssicherheit in der Logistik

März 2008: Heathrow Terminal 5

- Nach der Eröffnung des rund fünf Milliarden Euro teuren Terminal 5 Ende März war dort eine tagelanges Reise-chaos ausgebrochen, vor allem weil die **automatische Gepäck-Abfertigungsanlage** nicht funktionierte.
- Etwa 30.000 Koffer blieben liegen,
- Hunderte Flüge fielen aus → **20 Mio. € Schaden !!!**
- Tausende (!!) Koffer wurden mit LKWs nach Mailand gebracht … zum sortieren und verteilen …

Mängel in der Integrität & Verfügbarkeit …
→ der Logistik – Betrieb steht !

Vertraulichkeit der Daten in der Logistik

Logistik-Dienstleister benötigen viele Daten:

- Daten der Kunden
- Auftragsdaten
- Daten der Lieferanten

} **In ihren Verknüpfungen!**

Logistik-Dienstleister halten damit sehr sensible Daten:

- Wer liefert was an wen?
- Wer kauft was bei wem?
- Warenflüsse & Mengengerüste, … ihrer Kunden & Partner

Handelsketten zahlen viel für die Daten **ihrer** Kunden → Karten

- Was wären die Daten der Mitbewerber wert?

→ Logistik-Dienstleister müssen ihre Daten schützen

Elemente der Informationssicherheit

- Sichere Nutzung der IT-Anwendungen

- Sicherer IT-Betrieb

- Sichere Software (Anwendungen)

Information Security auf Seiten der IT-User

Information Security Im IT Service Management

Information Security in der SW Entwicklung

Prozessreife & Informationssicherheit - 17

DI. Andreas Nehfort PzM-Summit 2009

Informationsicherheit Stand der Technik

ISO Standards bilden die inhaltliche Grundlage

- ISO 20000 → IT Service Management
- ISO 27000 → Information Security Management System

Zweck dieser Standards ist die Zertifizierung von Unternehmen auf der Basis Ihrer Prozesse:

- für IT Service Management → Betriebssicherheit
- für Informationssicherheit

Die Botschaft: zertifizierte Sicherheit

Prozessreife & Informationssicherheit - 18

DI. Andreas Nehfort PzM-Summit 2009

ISO 27000ff
Information Security Management

ISO 27000ff: Information Technology Security Management

- Normenserie zum Information Security Management
- Integriert Information Security Management in ein integriertes Managementsystem

Die ISO 27000ff hat somit zwei konzeptuelle Wurzeln

- ISO 9001: Qualitätsmanagementsysteme (als Basis für ein integrieres Mangementsystem)
- ISO 17799: der bisherige ISO IS-Standard (früher auch BS7799)

ISO 27000ff: Information Technology
Information Security Management

- ISO 27000 – ISMS - Overview and Vocabulary
- ISO 27001 – ISMS – Requirements
- ISO 27002 – Code of Practice for ISMS (→ information security controls)
- ISO 27003 – ISMS Implementation Guidance (FDIS)
- ISO 27004 – ISM Measurment (FDIS)
- ISO 27005 – ISMS Risk Management
- ISO 27006 – ISMS Req. for Bodies providing Audits
- ISO 27006 – Guidelines for ISMS Auditing

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: ISMS - Control Objectives and Controls:
Verweis auf die ISO 27002

Inhalte der ISO 27002:2005 "Information Security Controls"

4. Risk assessment & Treatment
5. Security policy
6. Organization of information security
7. Asset management
8. Human resources security
9. Physical and environmental security
10. Communications & operations management
11. Access control
12. Information system acquisition, development, maintenance
13. Information security incident management
14. Business continuity management
15. Compliance

Service Level Agreements aus Sicht des Kunden

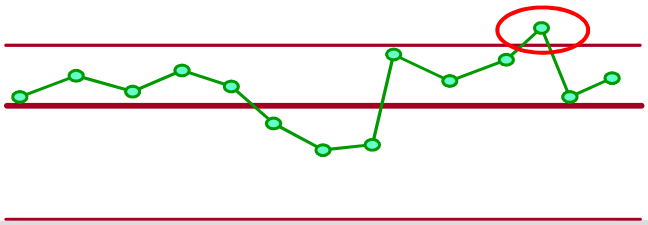
Service Level Agreements bedeuten:

- Definierte bedarfsgerechte Services
  - Mit einer definierten Leistung (WAS?)
  - Mit definierten Leistungsparametern (WIE GUT?)
- Betriebssicherheit → reduziertes Betriebsrisiko
- Informationssicherheit → reduziertes Sicherheitsrisiko

Service Level Agreements aus Sicht des Lieferanten

Definierte bedarfsgerechte Services:

- Mit einer definierten Leistung (WAS?)
- Mit definierten Leistungsparametern (WIE GUT?)
- Mit einer Dokumentation der Performance (IST)
  - Dokumentation allfälliger Abweichungen vom SLA.
- Maßnahmen bei Abweichungen



Sichere Prozesse?

ISO 20000 & ISO 27000 definieren inhaltliche Anforderungen an unsere IT-Prozesse

Die offene Frage:

- Wie müssen sichere Prozesse beschaffen sein?

Prozessreifegradmodelle geben eine Antwort:

- Prozessreife bieten eine methodische Grundlage für Prozess-Sicherheit!
- CMMI und SPICE / ISO 15504 sind enabler
  - für sichere Prozesse
  - für die Wirksamkeit eines IKS.

Das SPICE-Prozessreifemodell

Optimising
Quantitative measures used for
Process Innovation and Optimisation

Level 5 Optimising
PA.5.1 Process Innovation
PA.5.2 Process Optimisation

Predictable
Process measurement make process
performance and results controllable

Level 4 Predictable
PA.4.1 Measurement
PA.4.2 Process Control

Established
Predefined processes
are deployed
and tailored for specific use.

Level 3 Established
PA.3.1 Process Definition
PA.3.2 Process Deployment

Level 2 Managed
PA.2.1 Performance Management
PA.2.2 Work Product Management

Managed
Process and work products are
managed, responsibilities identified.

Level 1 Performed
PA.1.1 Process Performance

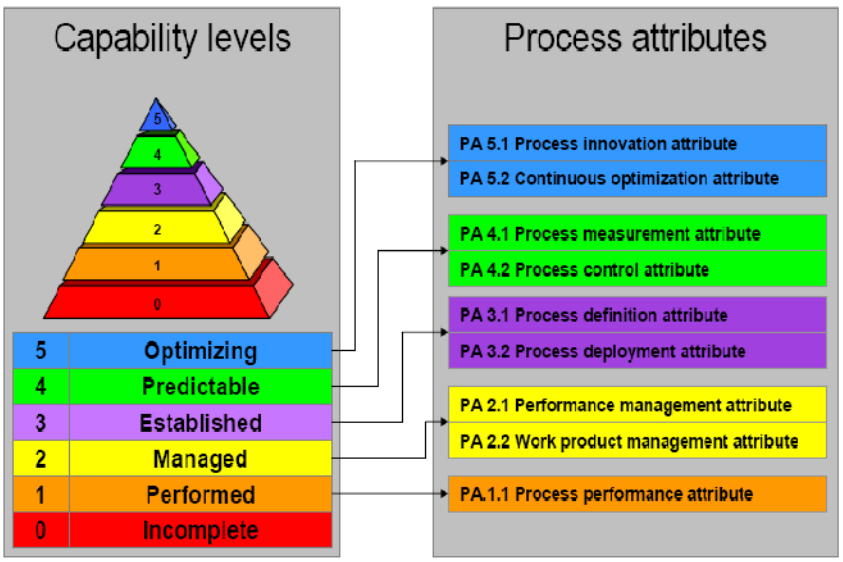
Performed
processes are intuitively performed, input
and
output work products are available

Level 0 Incomplete

Incomplete
Performance and results are
incomplete, chaotic processes

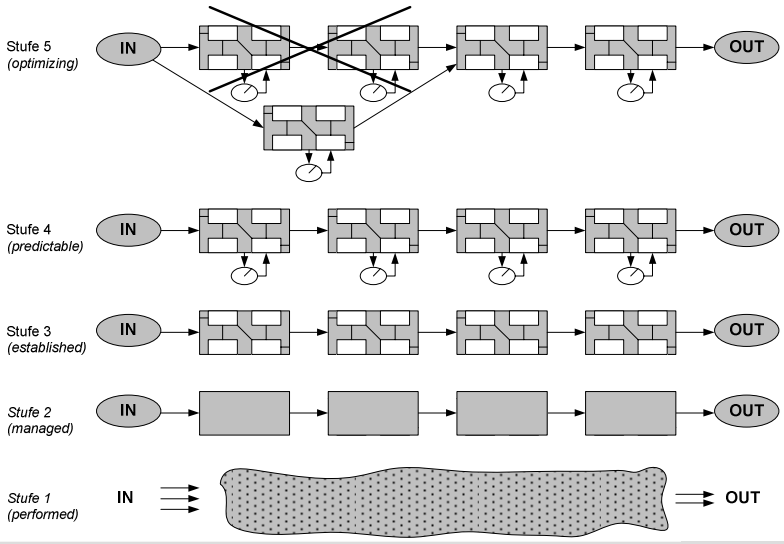
Prozessreife & Informationssicherheit - 27
DI. Andreas Nehfort
PzM-Summit 2009

Das SPICE-Prozessreifemodell



Prozessreife & Informationssicherheit - 28
DI. Andreas Nehfort
PzM-Summit 2009

Management Visibility by Capability Level



SPICE

Die zwei Konzepte der ISO 15504

Referenzprozess-Modelle:

- Definieren die Anforderungen an die **Prozessdurch-führung** zur Ziel-Erreichung → **WAS ist zu tun?**

Das SPICE Reifegradmodell:

- Definiert Kriterien für unterschiedliche Stufen der **Prozessfähigkeit** → Process Capability → **Wie gut?**

Prozessfähigkeit / Process Capability

Die Fähigkeit eines Prozesses seine Ziele zu erreichen!

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

Mit **zunehmender Prozessfähigkeit** werden die Ergebnisse des Prozesses **besser vorhersagbar**!

Bewertet wird die Process Capability

- mittels Process Assessment
- anhand der Kriterien eines Assessmentmodells

SPiCE - Capability Level 2

Managed Process

- **PA 2.1: Performance Management Attribute**
  - Prozessziele vorgeben,
  - Prozess planen & lenken,
  - Verantwortlichkeiten definieren & Ressourcen bereitstellen
- **PA 2.2: Work Product Management Attribute**
  - Anforderungen an WPs definieren
  - Anforderungen and die Dokumentation der WPs definieren
  - WPs erstellen und lenken
  - WPs reviewn, damit sie die Anforderungen erfüllen

SPiCE – Capability Level 3
Established (Standard) Process

- **PA 3.1: Process Definition Attribute**
  - Definierte Standardprozesse & ihr Zusammenspiel
  - Definierte Kompetenzen und Rollen
  - Definierte Methoden zur **Überwachung auf Eignung & Angemessenheit**
- **PA 3.2: Process Deployment Attribute**
  - Die definierten Standardprozesse werden eingesetzt
  - Rollen und Kompetenzen werden wahrgenommen
  - Ressourcen und Infrastruktur: bereitgestellt & genutzt
  - Datensammlung & **Analyse des Prozessverhaltens**

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.
- Planung & Lenkung der Prozessdurchführung → CL2
- 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 Prozesssteuerung → CL4

Informationssicherheit & Prozessreife

Prozessreife:

- Reduziert das Risiko unerwünschter Ergebnisse …
- Trägt dazu bei, Informationssicherheit zu gewährleisten

Prozessreife:

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

Process Assessments:

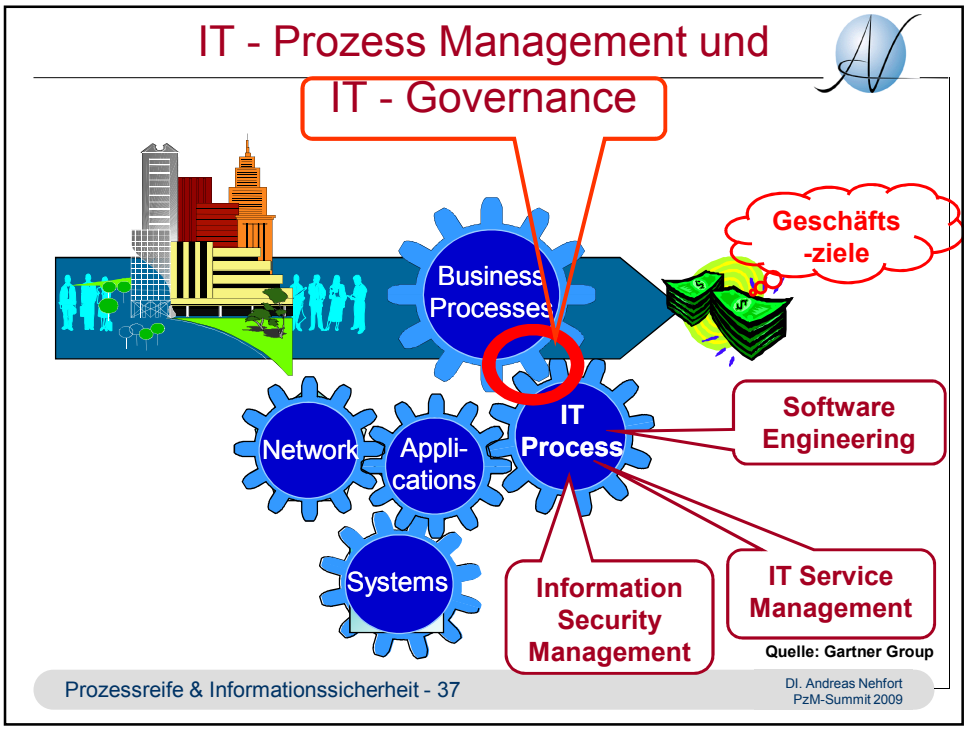
- Bestätigen die Reife der Prozesse
- Decken allfällige Lücken auf …

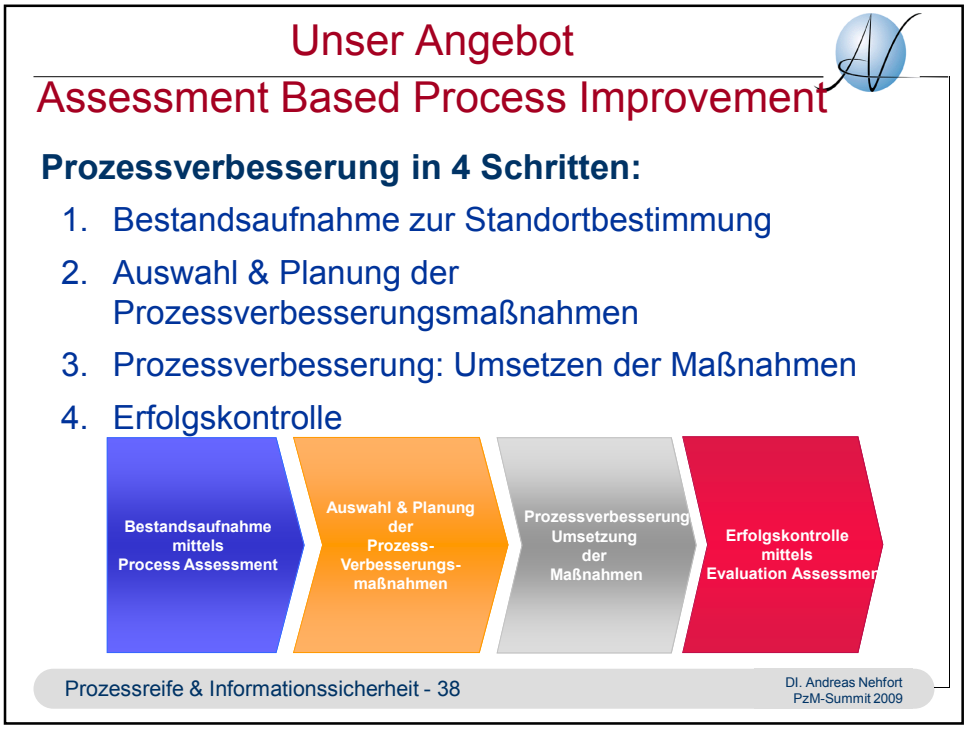
Informationssicherheit & Prozessreife

Definierte Standardprozesse:

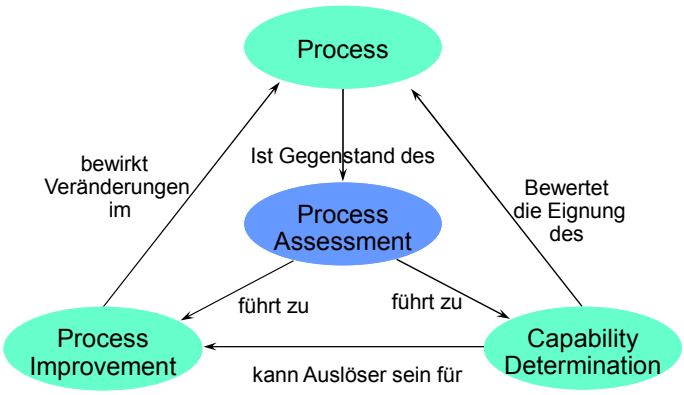
- Definierte Standardprozesse → etablierte Standards
  - Etablierte Standards → ermöglichen definierte Leistung
  - Etablierte Standards → ermöglichen Vergleichbarkeit
  - Etablierte Standards → ermöglichen Prozessmessung
- Prozessmessung → ermöglicht Soll-Ist Vergleich
- Prozessmessung → ermöglicht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

Diese Verantwortung nennt man heute **IT Governance!**


IT - Prozess Management und
IT - Governance
Business Processes
Geschäfts -ziele
Network
Appli-cations
Systems
IT Process
Software Engineering
Information Security Management
IT Service Management
Quelle: Gartner Group
Prozessreife & Informationssicherheit - 37
DI. Andreas Nehfort
PzM-Summit 2009


Unser Angebot
Assessment Based Process Improvement
Prozessverbesserung in 4 Schritten:
1. Bestandsaufnahme zur Standortbestimmung
2. Auswahl & Planung der Prozessverbesserungsmaßnahmen
3. Prozessverbesserung: Umsetzen der Maßnahmen
4. Erfolgskontrolle
Bestandsaufnahme mittels Process Assessment
Auswahl & Planung der Prozess-Verbesserungs-maßnahmen
Prozessverbesserung Umsetzung der Maßnahmen
Erfolgskontrolle mittels Evaluation Assessmen
Prozessreife & Informationssicherheit - 38
DI. Andreas Nehfort
PzM-Summit 2009

Die Rolle des Process Assessments



Alle Leistungen aus einer Hand

Unser Spezialistenteam für Ihren Erfolg:

- Prozess Experten: Berater, Trainer, Assessoren
- Entwickler von Assessment Methoden, Modellen & Tools
- Experten für SW-Engineering, Projekt- & Qualitätsmanagement , …

Assessments für Ihr integriertes Management System

SPICE als Basis für Ihr integriertes Management System

SPICE 1-2-1 als zugehöriges Assessment Tool

SPICE 1-2-1 integriert schrittweise folgende Standards:

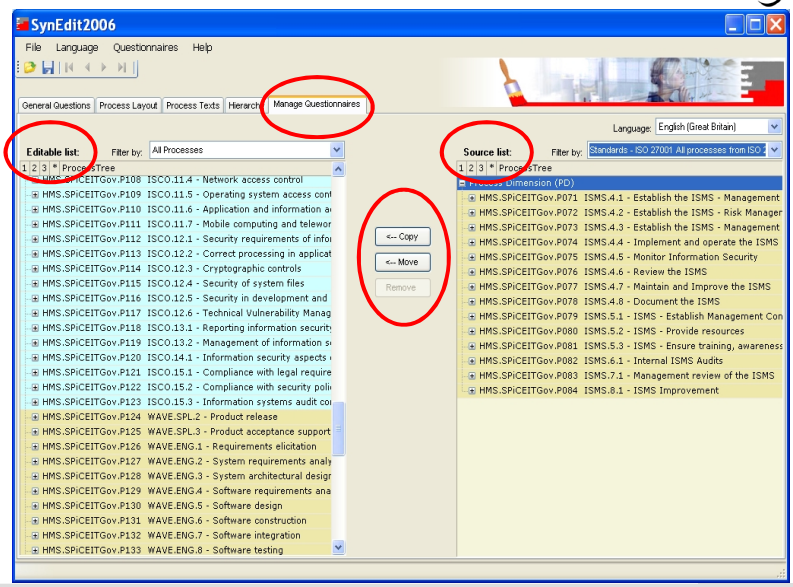
- ISO 15505-5 → Software Engineering
- ISO 15504-6 →Systems Engineering
- ISO 20000-1 → IT Service Management
- ISO 27001 → Information Security Management
- ISO 27002 → IT Security Controls
- Ihre spezifischen Prozesse & Controls

SPICE 1-2-1 for IT Governance

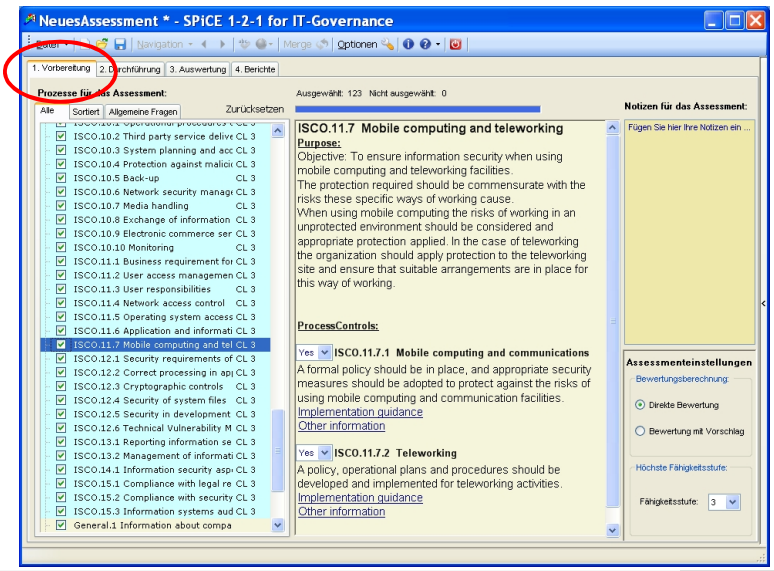
Multi-Standard Assessment Tool für IT Governance:

- Software Engineering → ISO 15504-5
- IT-Service Management → ISO 20000-1
- Information Security Management → ISO 27001
- Information Security Controls → ISO 27002
- Information Security Risk Management → ISO 27005 (geplant)
- **Ihr Assessment Modell …** → konfigurierbar mit **SynEdit**
  - Prozesse & Basis Praktiken
  - Control Objectives & Controls

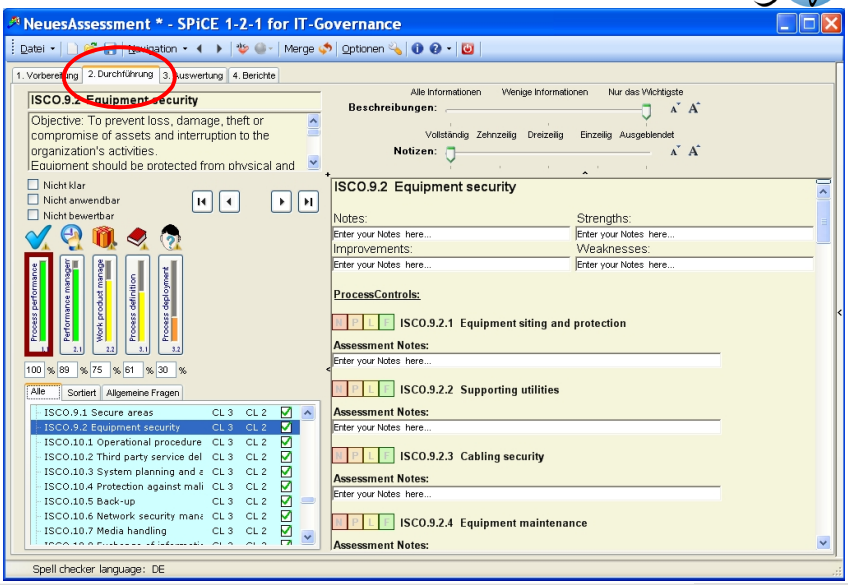
SynEdit: Configure your Questionnaire



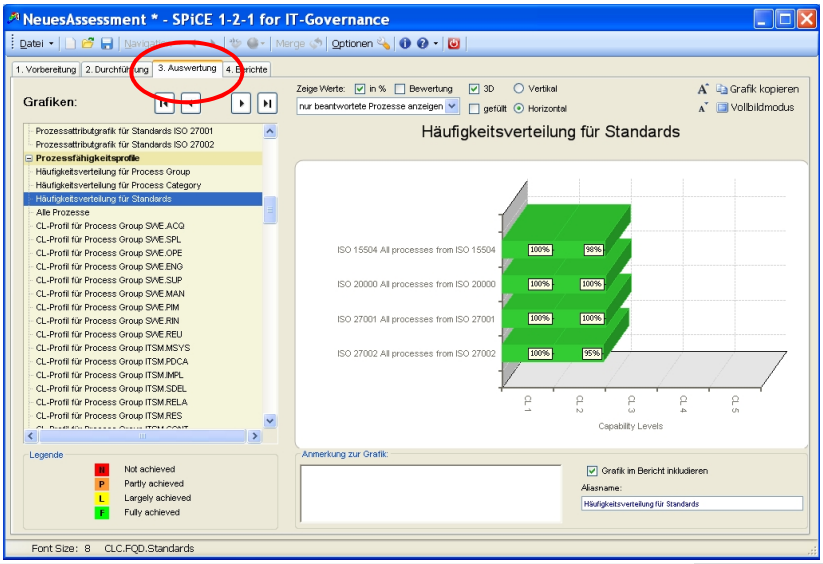
SPICE 1-2-1: Prepare



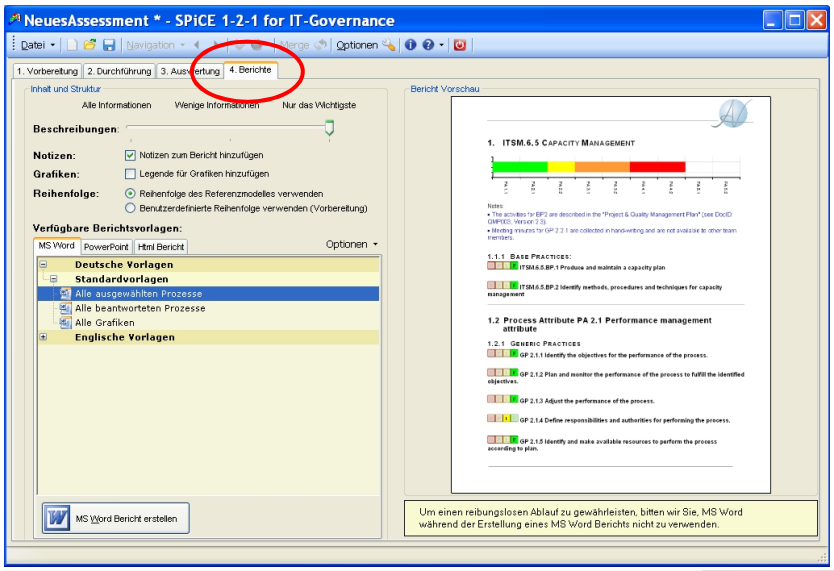
SPICE 1-2-1: Fill-In



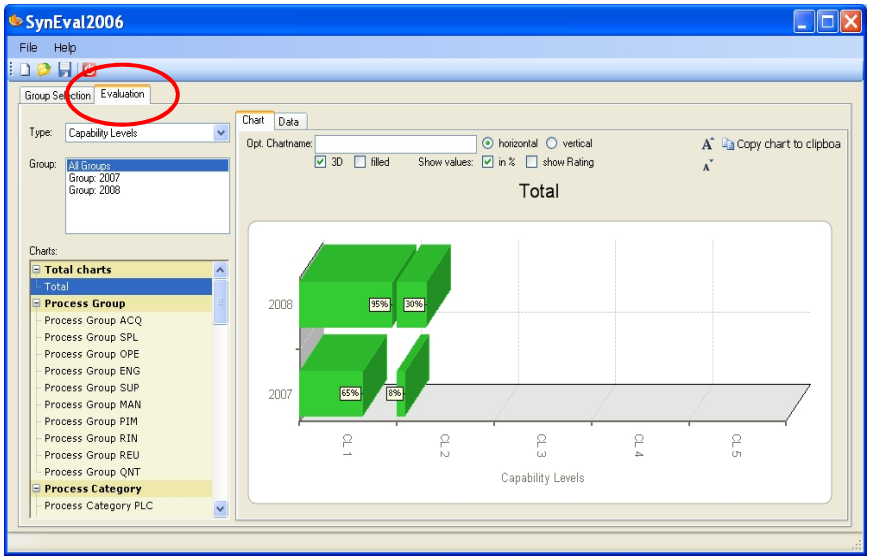
SPICE 1-2-1: Analyze



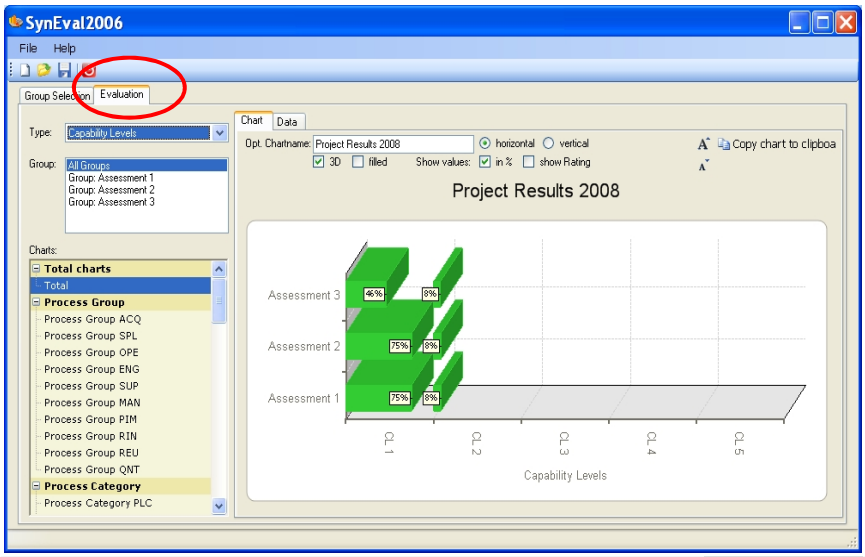
SPICE 1-2-1: Reports



SynEval: Erfolgskontrolle in der Zeitreihe



SynEval: Vergleich mehrerer Assessments



Information Security Management ist zu einem gesellschaftliches Anliegen geworden

„The best way to strengthen Information Security is to treat it as a corporate governance issue that requires the attention of boards and CEOs."

Dazu gibt es mittlerweile klare gesetzlicher Vorgaben:

- **SOX in den USA** - **Die 8. EU Richtlinie in Europa …**

Aus nachvollziehbaren Gründen werden manche Regelwerke ernster genommen als andere ...

Danke für Ihre Aufmerksamkeit!

Ihr Beitrag zu Diskussion ...

Download der aktuellen Präsentation
→ www.nehfort.at → Download → Referate & Vorträge

Information Security Incidents in den Medien

Beobachtungszeitraum: Oktober 2009

- 10.10.2009: Datenpanne bei AWD
- 11.10.2009: Datenleck bei schülerVZ gemeldet
- 23.10.2009: Deutsche Bahn akzeptiert Bußgeld von 1,12 Millionen Euro
- 24.10.2009: Neue Datenpanne bei Lidl
- 25.10.2009: Millionenpanne bei HSH Nordbank
- 25.10.2009: Verleihung des Big Brother Awards Austria
- 29.10.2009 Datenpanne bei deutschem Online-Buchhändler
- 30.10.2009: Datenleck bei Libri.de größer als angenommen

Sicherheitslücken im Geschäftsalltag …

10. Oktober 2009: Datenpanne bei AWD

- Daten von 27.000 AWD-Kunden werden NDR zugespielt.
  - Kundendaten, Art & Dauer der Verträge, Vertragssummen

11. Oktober 2009: Datenleck bei schülerVZ gemeldet

- Der deutschen Bürgerrechtsplattform Netzpolitik.org sind über eine Million Datensätze von jugendlichen Nutzern des Sozialen Netzwerks schülerVZ zugespielt worden. Die Betreiber bestätigten mittlerweile die "illegale Datenkopie" und prüfen derzeit, wie die Daten gesammelt wurden …
- Bereits 2006 hatte der deutsche Blogger Don Alphonso mehrfach auf Datenlecks bei der schülerVZ-Mutter studiVZ hingewiesen …

Prozessreife & Informationssicherheit - 53

DI. Andreas Nehfort
PzM-Summit 2009

Sicherheitsbedürfnisse im Geschäftsalltag …

20. Oktober 2009: Spielregeln für smarte Stromzähler

In den nächsten Jahren sollen Stromzähler "intelligenter" werden und damit beim Energiesparen helfen.

Doch die neue Technologie bringt nicht nur Vorteile mit sich:

- Die automatische ferngesteuerte Auslesung der Verbraucherdaten könnte das Datenschutzgesetz verletzen.

Österreichische Netzbetreiber, die Pilotprojekte betreiben, weisen mögliche Probleme zurück …

Prozessreife & Informationssicherheit - 54

DI. Andreas Nehfort
PzM-Summit 2009

Die Konsequenzen im Geschäftsalltag …
Deutsche Bahn akzeptiert Bußgeld

23.Oktober 2009: 1,12 Millionen Euro Forderungen

Die Deutsche Bahn zahlt eine Strafe von 1,12 Millionen € für **Verstöße gegen den Datenschutz** im Unternehmen.

Das teilte der Berliner Datenschutzbeauftragte Alexander Dix am Freitag in Berlin mit.

Geahndet werden damit mehrere Vorfälle der Affäre, bei denen die Daten von Mitarbeitern heimlich mit denen von Lieferanten der Bahn abgeglichen wurden …

Sicherheitslücken im Geschäftsalltag …

24.Oktober 2009: Neue Datenpanne bei Lidl

- **Laut "Spiegel" hat es diesmal eine Panne beim Zentralserver von Lidl Irland gegeben.**
- Auf einem Zentralserver von Lidl Irland seien extrem sensible Daten für Unbefugte innerhalb des Konzerns zeitweise komplett einsehbar gewesen.
- Dazu zählten Umsatzzahlen, Einkaufsplanungen, Schriftverkehr zwischen dem Unternehmen und Ärzten der Mitarbeiter sowie Krankmeldungen, Diagnosen und Abmahnungen von Beschäftigten, heißt es in dem Bericht.
- **Eine Kopie der Daten sei einem deutschen Ex-Mitarbeiter zugespielt worden.**

Verleihung des Big Brother Awards Austria

25. Oktober im Wiener Rabenhoftheater

In Österreich findet die Verleihung der Big Brother Awards bereits zum elften Mal traditionell am 25. Oktober statt.

Die Gewinner bekommen einen Preis und einen Platz in der **"Hall of Shame"**, so wie ihre Vorgänger der letzten zehn Jahre.

Im Vorjahr erhielt etwa Daniela Strassl für **Wiener Wohnen** den Big Brother Award in der Kategorie "Behörden und Verwaltung".

Grund waren Funkchips für die zentrale Verwaltung von Waschküchen und ein als "anonym" beschriebener Fragebogen mit intimen Fragen zu den Nachbarn und dem Sicherheitsgefühl, auf dem die Kundennummer als Strichcode der automatisierten Zuordnung diente, so die Veranstalter der Big Brother Awards.

25.10.2009: Millionenpanne bei HSH Nordbank

Die HSH Nordbank hat laut Bericht des deutschen Nachrichtenmagazins "Focus" 30 Millionen Dollar durch den Fehler eines Mitarbeiters verloren.

- Ein Händler in Kopenhagen habe am 6. Oktober 2008 einen Währungstausch mit der schlingernden isländischen Kaupthing Bank vereinbart.
- Die Nordbank habe die Summe in Schweizer Franken überwiesen.
- Als die Kaupthing Bank den Gegenwert wenige Tage später in Dollar überweisen sollte, war sie bereits zahlungsunfähig.

Die HSH habe 20 Millionen Euro abschreiben müssen.

- Bereits am 2. Okt. 2008 hatte die Bank einen Handelsstopp mit Island verhängt.
- Der inzwischen gefeuerte Banker habe sein Vorgehen mit einer Ausnahmegenehmigung erklärt.
- Belege existieren dem Bericht zufolge nicht mehr.

Das Blatt zitiert die HSH-Sprecherin Michaela Fischer-Zernin so:

- Der Händler hat sich nicht an den Handelsstopp gehalten.
- Die Dokumentationspflicht sei inzwischen verbessert worden.

29.10.2009 Datenpanne bei deutschem Online-Buchhändler

Rechnungen Tausender Libri.de-Kunden waren online

Beim deutschen Online-Buchhändler Libri.de hat es eine Datenpanne gegeben.

- Rechnungen Tausender Kunden waren über einen Umweg für jeden Internet-Nutzer einsehbar.

Das Unternehmen räumte den Fehler ein.

- "Wir konnten unverzüglich reagieren und die Lücke schnell schließen, bevor ein Schaden entstand",

teilte Libri am Donnerstag in Hamburg mit.

30.10.2009: Datenleck bei Libri.de größer als angenommen

Wir hatten Zugriff auf die **kompletten Bestellstatistiken,** die **Bestell-historie, Beleghistorie und Kundenliste mit Mail- und Postadresse**", berichtete Netzpolitik.org am Freitag.

"Dazu hätten wir die Möglichkeit gehabt, einen Shop zu 'übernehmen', indem wir die Zugangs- und Kontaktdaten ändern, und selbstverständlich hätten wir auch gleich allen Kunden eine Mail schicken können mit der Empfehlung eines ähnlichen Buches." Mit leicht veränderten Log-in-Daten konnten sich die Betreiber mit dem immer gleichen Passwort in weitere Shops bei Libri.de einloggen.

"Die neuerlichen Weiterungen des Falles dokumentieren ein erschreckendes Ausmaß an Unkenntnis und Nachlässigkeit im Umgang mit Daten und der Datensicherheit", kritisierte der Hamburger Datenschutzbeauftragte Johannes Caspar den Fall.