



Sicherheits- prozesse für SAP- Produkte

Tom Schröder

NetWeaver PM Security, SAP AG

Überblick

Ziele der Qualitätsprozesse

Entwicklungsmodell bei SAP

Interne Richtlinien für sicheres Entwickeln

Interne Produktsicherheitservices

Entwicklungsstandorte



SAP AG *)

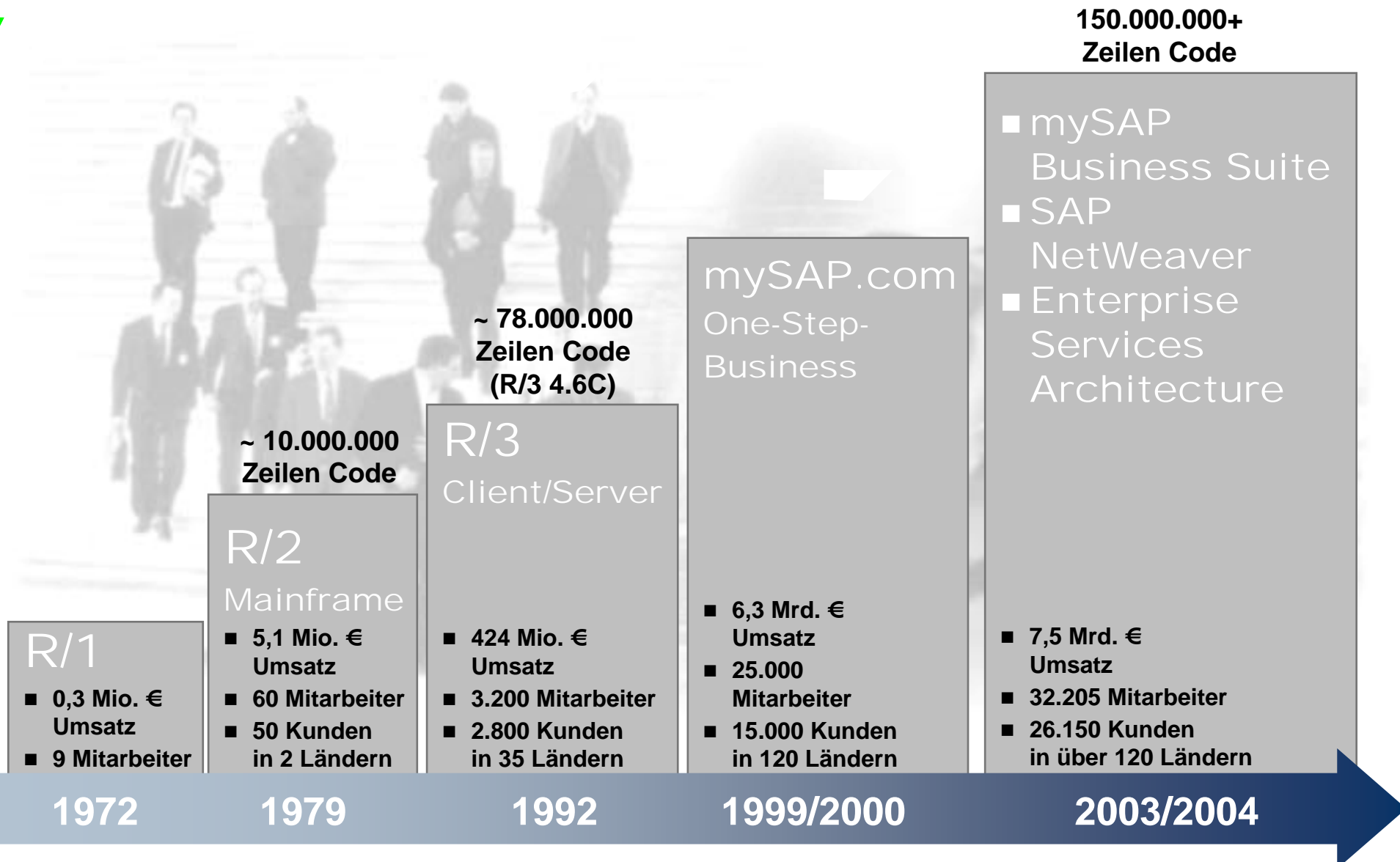
- 31.500 Mitarbeiter
- Vertreten in 50+ Ländern
- Durchschnittsalter 36 Jahre
- 24.450+ Unternehmen nutzen SAP
- 84.000 Installationen
- 12 Millionen Nutzer in 120+ Ländern
- 7,025 Mrd. € Umsatz in 2003
- R&D 13,5% vom Umsatz 2003

*) Stand November 2004

Produkte/Lösungen

- 150+ Produkte und 40+ Lösungen
- davon mehr als 25 Industrielösungen
- 30+ Sprachen unterstützt
- durchschnittlich arbeiten ca. 500 Entwickler parallel an einer Lösung

Geändertes Produktportfolio von SAP



Überblick

Ziele der Qualitätsprozesse

Entwicklungsmodell bei SAP

Interne Richtlinien für sicheres Entwickeln

Interne Produktsicherheitsservices

Ohne Sicherheit kein nachhaltiges E-Business

- **Sicherheit ist ein zentrale Bedingung für erfolgreiches E-Business**

Für SAP ist Sicherheit ein Qualitätsaspekt einer Lösung

- **Integriert in die Planungs,- Entwicklungs- und Qualitätssicherungsprozesse**



6 typische Kernfragen:

- ▶▶ **Wie entwickelt man komplexe Lösungen, die sich flexibel an Kunden- und Marktanforderungen anpassen lassen?**
- ▶▶ **Wie erreicht man einen günstigen TCO beim Kunden? (TCO = Total Cost of Ownership)**
- ▶▶ **Wie stellt man sicher, dass die Entwicklung sowohl zeitgerecht ist als auch die Marktanforderungen trifft?**
- ▶▶ **Wie erreicht man einen hohen Wiederverwendungsgrad der Software?**
- ▶▶ **Wie realisiert man eine verteilte Entwicklung an vielen unterschiedlichen internationalen Standorten?**
- ▶▶ **Wie stellt man bei den o.g. Herausforderungen und Randbedingungen eine hohe Qualität sicher?**

Überblick

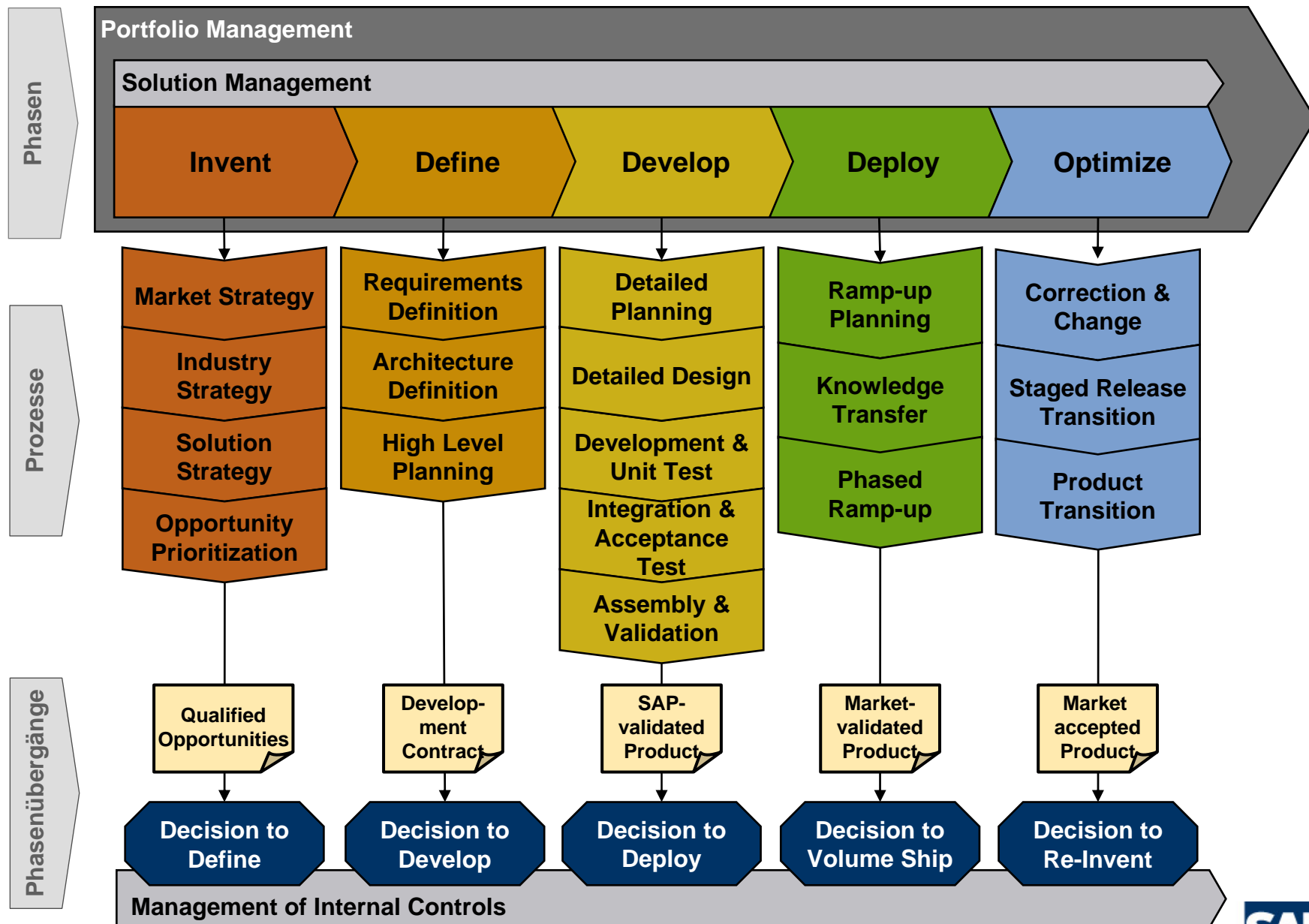
Ziele der Qualitätsprozesse

Entwicklungsmodell bei SAP

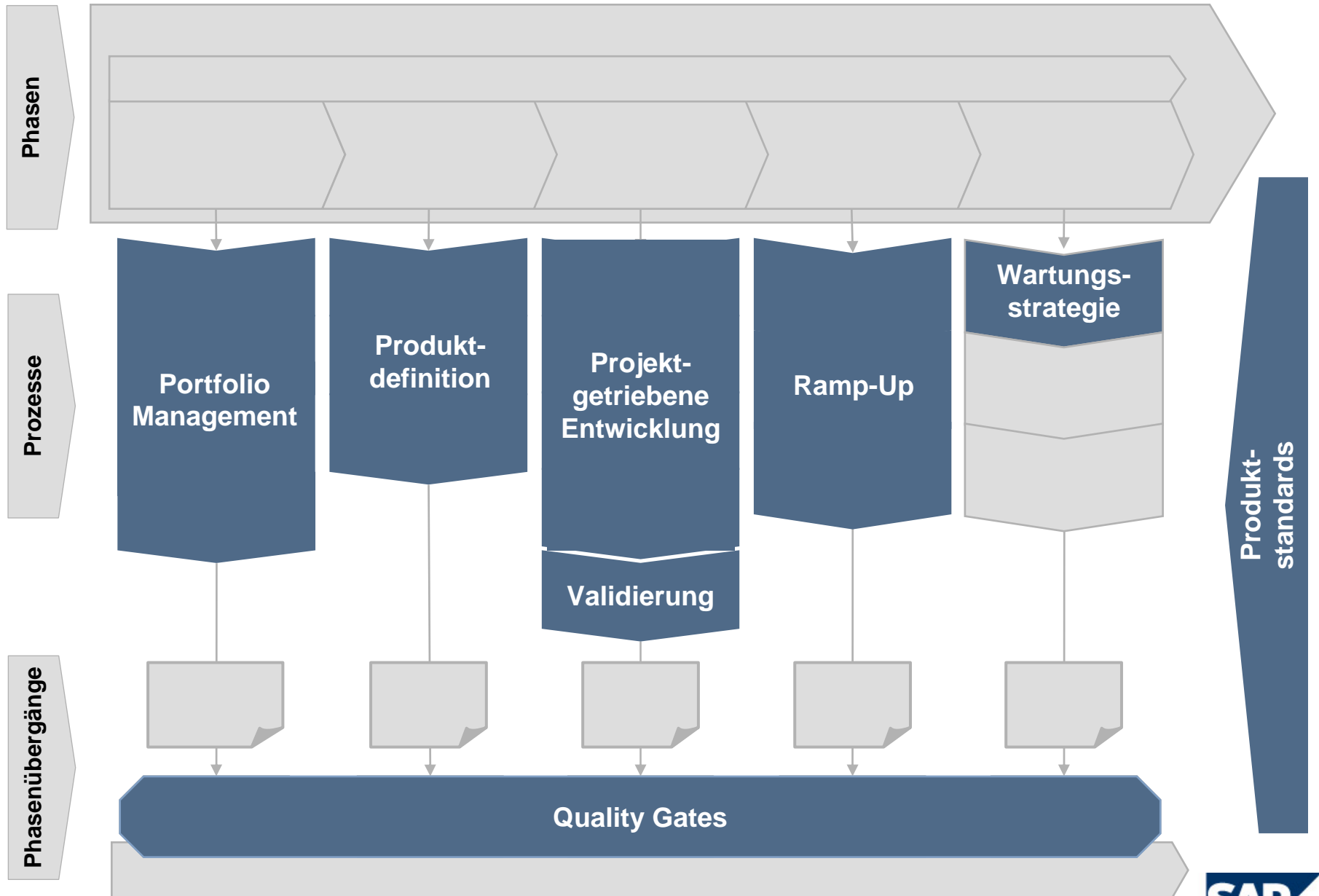
Interne Richtlinien für sicheres Entwickeln

Interne Produktsicherheitsservices

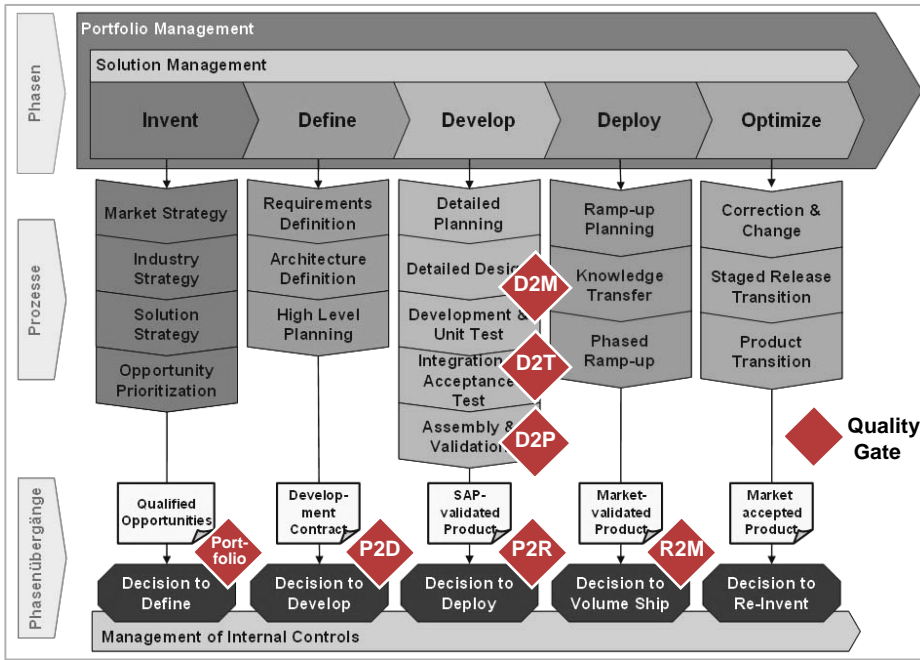
Product Innovation Lifecycle (PIL) im Überblick



Kernkonzepte des PIL-Prozesses

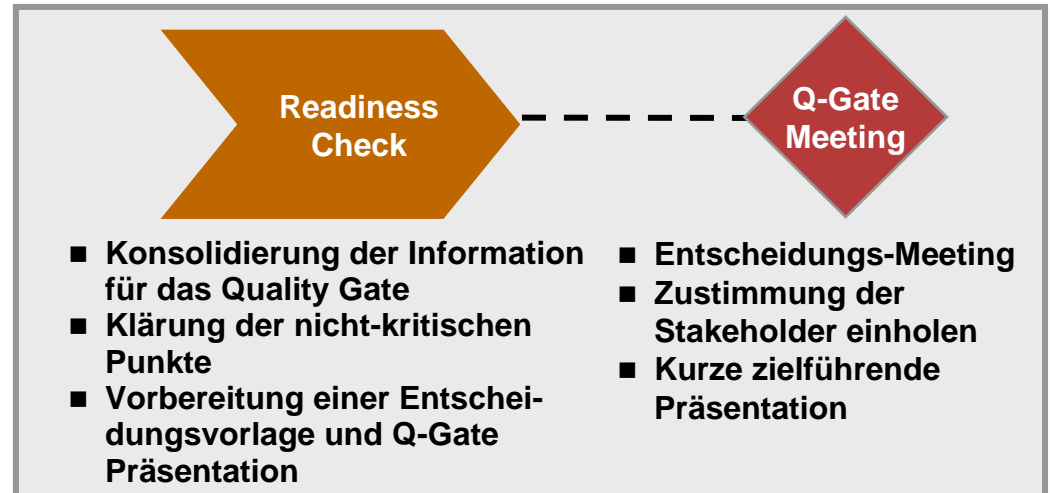


Kernkonzept: Quality Gates



z.B. Standardeinhaltung

Standard	Description
Accessibility	Software accessible to disabled persons
Application Integration and Interfaces	Integration
Customizing and Configuration	Adaptability to customer-specific business processes
Data Archiving	Archivability of business data
Development Environments	Use of dev. environments and programming languages
Documentation	Documentation for customers
Functional Correctness	Functionality
Globalization	Multilingual capability and internationalization
Multiple Clients	Multiple client capability
Open Source	Controlled use of open source software
Performance	System performance and scalability
Security	Support to reach a baseline product security level
IT Service & Appl. Mgmt. Services	Smooth operation at the customer site
Implementation and Change Mgmt. (ICM)	Simple implementation and upgrade capability
Third Party	Integration of software products from other providers
Usability	User-friendliness



Kernkonzept: Produktstandards

Standard	Beschreibung
Accessibility	Bedienbare Software für behinderte Menschen
Application Integration and Interfaces	Software-Integration und standardisierte Schnittstellen
Business Solution Configuration	Adaption an kundenspezifische Geschäftsprozesse
Data Archiving	Archivierbarkeit von Geschäftsdaten
Development Environments	Verwendung von Entwicklungsumgebungen und Programmiersprachen
Dokumentation	Dokumentation für Kunden
Functional Correctness	Korrekte Funktionalität
Globalization	Mehr-Sprachen-Unterstützung und Internationalisierung
Multiple Clients	Eigenschaft "viele Mandanten in einem System"
Open Source	Kontrollierte Verwendung von Open Source Software
Performance	Systemperformance und Skalierbarkeit
Security	Unterstützung zur Erfüllung eines angemessenen Sicherheitsniveau
IT Service & Appl. Mgmt.	Reibungsloser Betrieb beim Kunden
Technical Implementation and Change Mgmt. (TICM)	Einfache Implementierung und Upgrade Eigenschaften
Third Party	Integration von Fremdsoftware anderer Hersteller
Usability	Benutzerfreundlichkeit

Überblick

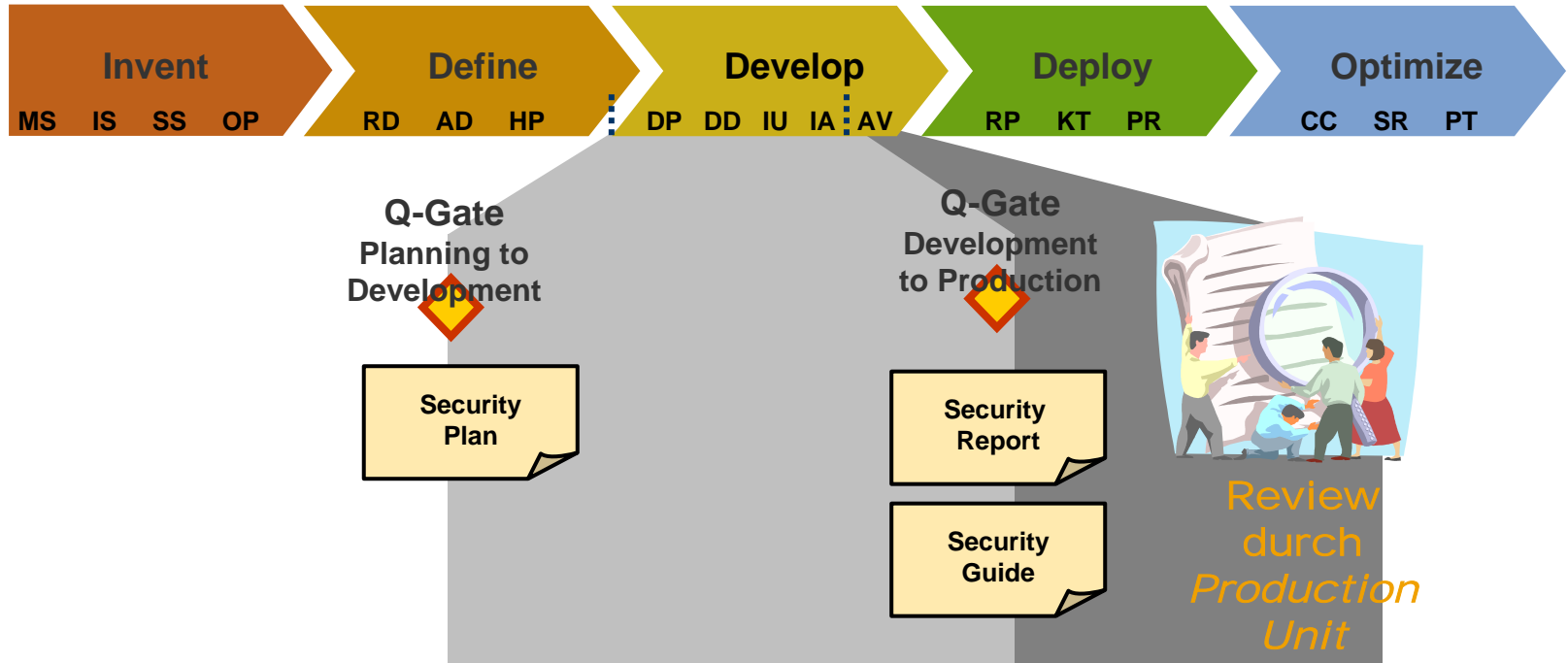
Ziele der Qualitätsprozesse

Entwicklungsmodell bei SAP

Interne Richtlinien für sicheres Entwickeln

Interne Produktsicherheitsservices

SAP müssen heute folgende Dokumente für den Sicherheitsstandard während der Entwicklung erstellen:

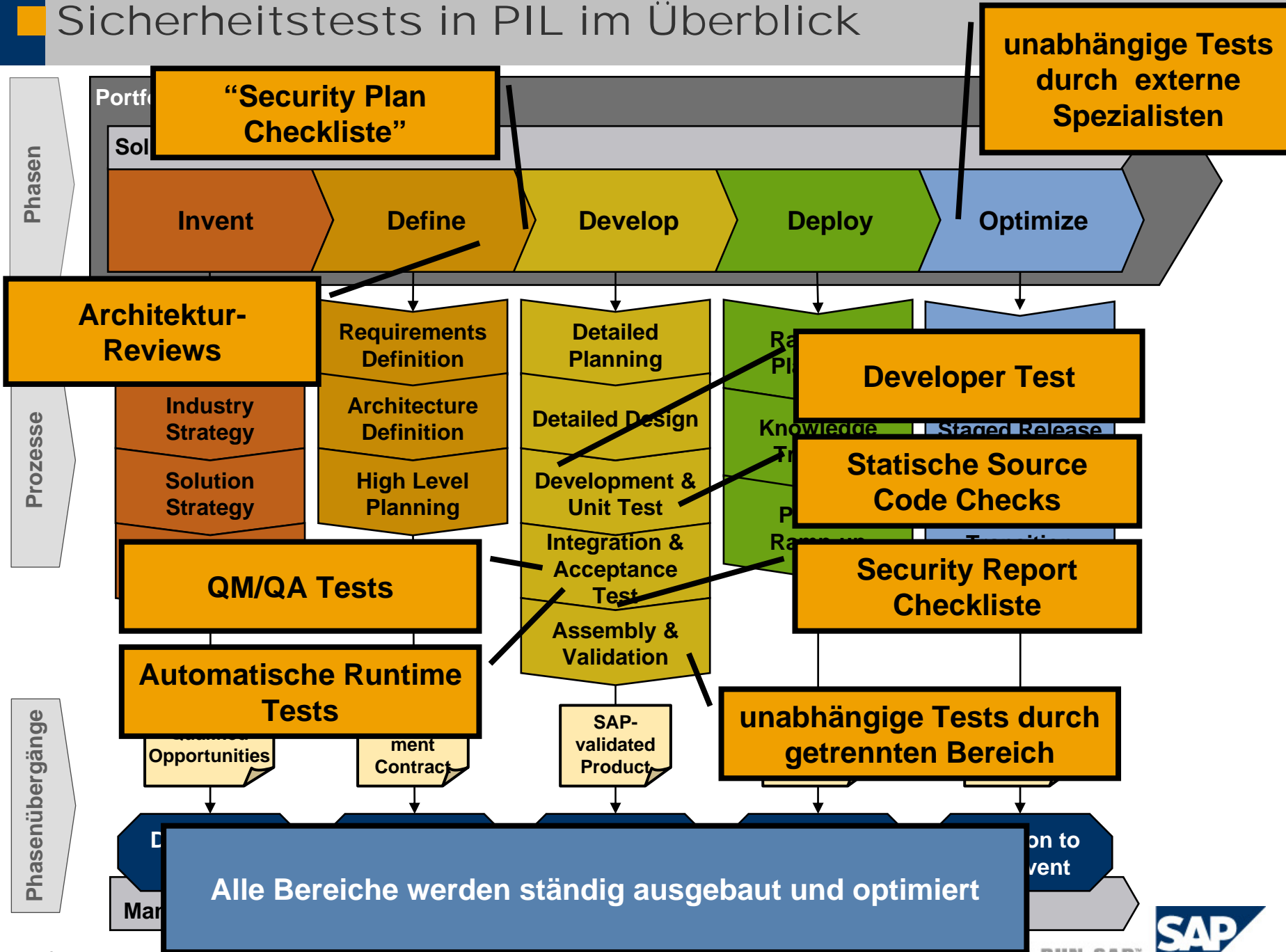


Security Solution Map: Struktur der Anwendungssicherheit

Application Security	Regulatory compliance	Role and authorization concepts	Data protection and privacy	Auditing
Secure Collaboration	Identity federation	Message security	Security interoperability	Trust management
Secure User Access	Identity management	Authentication and single sign-on	Access control	
Infrastructure Security	Network and communications security	Platform security	System security	Front-end security
Software Life-Cycle Security	Secure development	Secure default configuration	Secure delivery	Secure change management

Details auf dem SAP Service Marketplace [/security](https://www.sap.com/service-marketplace/security)

Sicherheitstests in PIL im Überblick

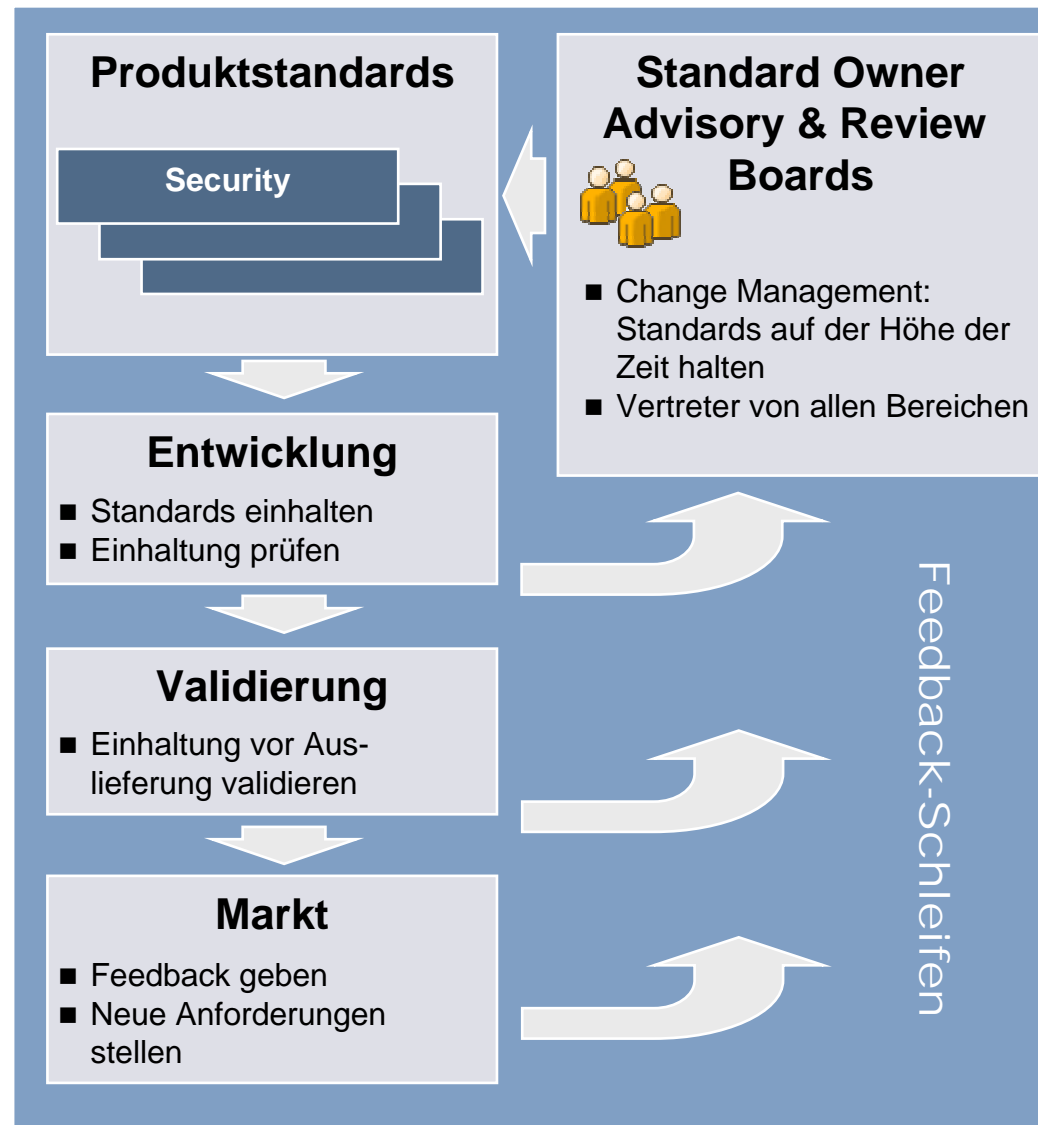


Organisation

- Standard Owner
- ARB
- „Security Coordinator/Expert Network“ als dezentrales Netzwerk (Roll-in und Roll-out)

Roll-in

- Kundenanforderungen
- Externe Untersuchungen
- Kunden
- Markt (State-of-the-Art)
- SAP Strategie
- rechtliche Anforderungen



Überblick

Ziele der Qualitätsprozesse

Entwicklungsmodell bei SAP

Interne Richtlinien für sicheres Entwickeln

Interne Produktsicherheitservices

Entwicklungsgruppen bei SAP haben Zugriff auf Unterstützung:

- interne Sicherheitsberatung (für Planung und Entwicklung)
- interne Sicherheitsreviews
- Sicherheitstraining
 - ◆ Zielgruppenspezifisch
 - ◆ Unterschiedliche Medien (E-Learning, Schulungen, Dokumente)
 - ◆ Unterschiedliche Lernstufen
- Awarenesskampagnen und Vorträge
- Sicherheitsuntersuchungen durch externe Sicherheitsspezialisten
- Security Response Prozess

Sicherheitsmaßnahmen bei der Softwareherstellung

- 4-Augen-Prinzip für Code-Auslieferung
- 4-Augen-Prinzip für SAP Hinweise
- Sichere Entwicklungsumgebung
- Sichere Auslieferung durch Code-Signing (teilweise)
- Externe Penetrationstests der Entwicklungsumgebung
- ...

<http://service.sap.com/security>
[/securitypartners](http://service.sap.com/security/securitypartners)
[/securityguide](http://service.sap.com/security/securityguide)
[/securityconsulting](http://service.sap.com/security/securityconsulting)
[/sos](http://service.sap.com/security/sos)
[/education](http://service.sap.com/security/education)

<http://sdn.sap.com> -> NetWeaver -> Security

<http://help.sap.com>

<http://www.sap-si.com/security>

service.sap.com

- No part of this publication may be reproduced or transmitted in any form or for any purpose without the express permission of SAP AG. The information contained herein may be changed without prior notice.
 - Some software products marketed by SAP AG and its distributors contain proprietary software components of other software vendors.
 - Microsoft, Windows, Outlook, and PowerPoint are registered trademarks of Microsoft Corporation.
 - IBM, DB2, DB2 Universal Database, OS/2, Parallel Sysplex, MVS/ESA, AIX, S/390, AS/400, OS/390, OS/400, iSeries, pSeries, xSeries, zSeries, z/OS, AFP, Intelligent Miner, WebSphere, Netfinity, Tivoli, and Informix are trademarks or registered trademarks of IBM Corporation in the United States and/or other countries.
 - Oracle is a registered trademark of Oracle Corporation.
 - UNIX, X/Open, OSF/1, and Motif are registered trademarks of the Open Group.
 - Citrix, ICA, Program Neighborhood, MetaFrame, WinFrame, VideoFrame, and MultiWin are trademarks or registered trademarks of Citrix Systems, Inc.
 - HTML, XML, XHTML and W3C are trademarks or registered trademarks of W3C®, World Wide Web Consortium, Massachusetts Institute of Technology.
 - Java is a registered trademark of Sun Microsystems, Inc.
 - JavaScript is a registered trademark of Sun Microsystems, Inc., used under license for technology invented and implemented by Netscape.
 - MaxDB is a trademark of MySQL AB, Sweden.
 - SAP, R/3, mySAP, mySAP.com, xApps, xApp, SAP NetWeaver and other SAP products and services mentioned herein as well as their respective logos are trademarks or registered trademarks of SAP AG in Germany and in several other countries all over the world. All other product and service names mentioned are the trademarks of their respective companies. Data contained in this document serves informational purposes only. National product specifications may vary.
-
- The information in this document is proprietary to SAP. No part of this document may be reproduced, copied, or transmitted in any form or for any purpose without the express prior written permission of SAP AG.
 - This document is a preliminary version and not subject to your license agreement or any other agreement with SAP. This document contains only intended strategies, developments, and functionalities of the SAP® product and is not intended to be binding upon SAP to any particular course of business, product strategy, and/or development. Please note that this document is subject to change and may be changed by SAP at any time without notice.
 - SAP assumes no responsibility for errors or omissions in this document. SAP does not warrant the accuracy or completeness of the information, text, graphics, links, or other items contained within this material. This document is provided without a warranty of any kind, either express or implied, including but not limited to the implied warranties of merchantability, fitness for a particular purpose, or non-infringement.
 - SAP shall have no liability for damages of any kind including without limitation direct, special, indirect, or consequential damages that may result from the use of these materials. This limitation shall not apply in cases of intent or gross negligence.
 - The statutory liability for personal injury and defective products is not affected. SAP has no control over the information that you may access through the use of hot links contained in these materials and does not endorse your use of third-party Web pages nor provide any warranty whatsoever relating to third-party Web pages.

- Weitergabe und Vervielfältigung dieser Publikation oder von Teilen daraus sind, zu welchem Zweck und in welcher Form auch immer, ohne die ausdrückliche schriftliche Genehmigung durch SAP AG nicht gestattet. In dieser Publikation enthaltene Informationen können ohne vorherige Ankündigung geändert werden.
 - Die von SAP AG oder deren Vertriebsfirmen angebotenen Softwareprodukte können Softwarekomponenten auch anderer Softwarehersteller enthalten.
 - Microsoft, Windows, Outlook, und PowerPoint sind eingetragene Marken der Microsoft Corporation.
 - IBM, DB2, DB2 Universal Database, OS/2, Parallel Sysplex, MVS/ESA, AIX, S/390, AS/400, OS/390, OS/400, iSeries, pSeries, xSeries, zSeries, z/OS, AFP, Intelligent Miner, WebSphere, Neffinity, Tivoli, und Informix sind Marken oder eingetragene Marken der IBM Corporation in den USA und/oder anderen Ländern.
 - Oracle ist eine eingetragene Marke der Oracle Corporation.
 - UNIX, X/Open, OSF/1, und Motif sind eingetragene Marken der Open Group.
 - Citrix, ICA, Program Neighborhood, MetaFrame, WinFrame, VideoFrame, und MultiWin sind Marken oder eingetragene Marken von Citrix Systems, Inc.
 - HTML, XML, XHTML und W3C sind Marken oder eingetragene Marken des W3C®, World Wide Web Consortium, Massachusetts Institute of Technology.
 - Java ist eine eingetragene Marke von Sun Microsystems, Inc.
 - JavaScript ist eine eingetragene Marke der Sun Microsystems, Inc., verwendet unter der Lizenz der von Netscape entwickelten und implementierten Technologie.
 - MaxDB ist eine Marke von MySQL AB, Schweden.
 - SAP, R/3, mySAP, mySAP.com, xApps, xApp, SAP NetWeaver und weitere im Text erwähnte SAP-Produkte und -Dienstleistungen sowie die entsprechenden Logos sind Marken oder eingetragene Marken der SAP AG in Deutschland und anderen Ländern weltweit. Alle anderen Namen von Produkten und Dienstleistungen sind Marken der jeweiligen Firmen. Die Angaben im Text sind unverbindlich und dienen lediglich zu Informationszwecken. Produkte können länderspezifische Unterschiede aufweisen.
-
- Die in dieser Publikation enthaltene Information ist Eigentum der SAP. Weitergabe und Vervielfältigung dieser Publikation oder von Teilen daraus sind, zu welchem Zweck und in welcher Form auch immer, nur mit ausdrücklicher schriftlicher Genehmigung durch SAP AG gestattet.
 - Bei dieser Publikation handelt es sich um eine vorläufige Version, die nicht Ihrem gültigen Lizenzvertrag oder anderen Vereinbarungen mit SAP unterliegt. Diese Publikation enthält nur vorgesehene Strategien, Entwicklungen und Funktionen des SAP®-Produkts. SAP entsteht aus dieser Publikation keine Verpflichtung zu einer bestimmten Geschäfts- oder Produktstrategie und/oder bestimmten Entwicklungen. Diese Publikation kann von SAP jederzeit ohne vorherige Ankündigung geändert werden.
 - SAP übernimmt keine Haftung für Fehler oder Auslassungen in dieser Publikation. Des Weiteren übernimmt SAP keine Garantie für die Exaktheit oder Vollständigkeit der Informationen, Texte, Grafiken, Links und sonstigen in dieser Publikation enthaltenen Elementen. Diese Publikation wird ohne jegliche Gewähr, weder ausdrücklich noch stillschweigend, bereitgestellt. Dies gilt u. a., aber nicht ausschließlich, hinsichtlich der Gewährleistung der Marktgängigkeit und der Eignung für einen bestimmten Zweck sowie für die Gewährleistung der Nichtverletzung geltenden Rechts.
 - SAP haftet nicht für entstandene Schäden. Dies gilt u. a. und uneingeschränkt für konkrete, besondere und mittelbare Schäden oder Folgeschäden, die aus der Nutzung dieser Materialien entstehen können. Diese Einschränkung gilt nicht bei Vorsatz oder grober Fahrlässigkeit.
 - Die gesetzliche Haftung bei Personenschäden oder Produkthaftung bleibt unberührt. Die Informationen, auf die Sie möglicherweise über die in diesem Material enthaltenen Hotlinks zugreifen, unterliegen nicht dem Einfluss von SAP, und SAP unterstützt nicht die Nutzung von Internetseiten Dritter durch Sie und gibt keinerlei Gewährleistungen oder Zusagen über Internetseiten Dritter ab.