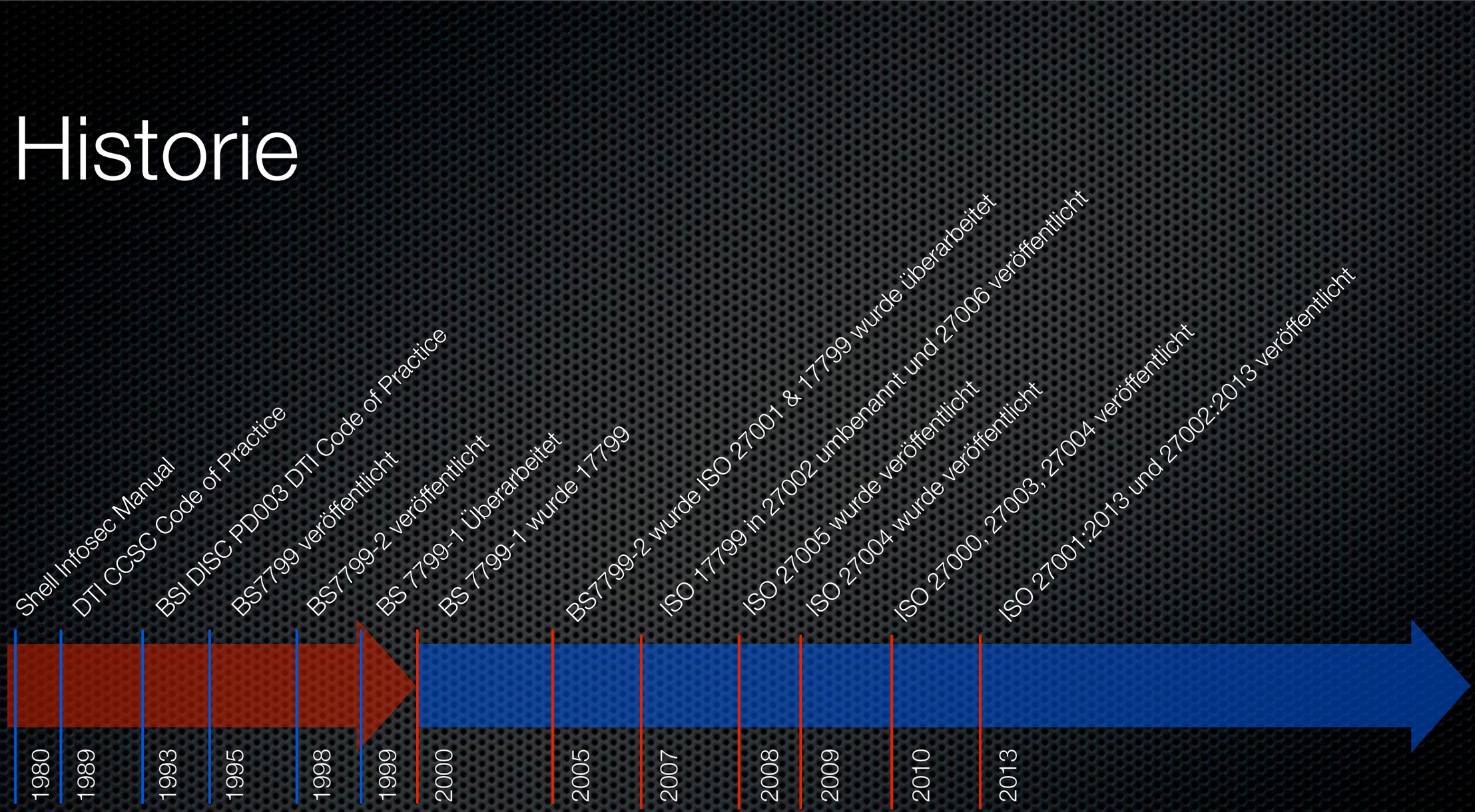
27001 & 27002:2013

Dr.-Ing. Oliver Weissmann

Inhalt

- Historie
- Status
- Standards
  - 27001
  - 27002
- Fazit

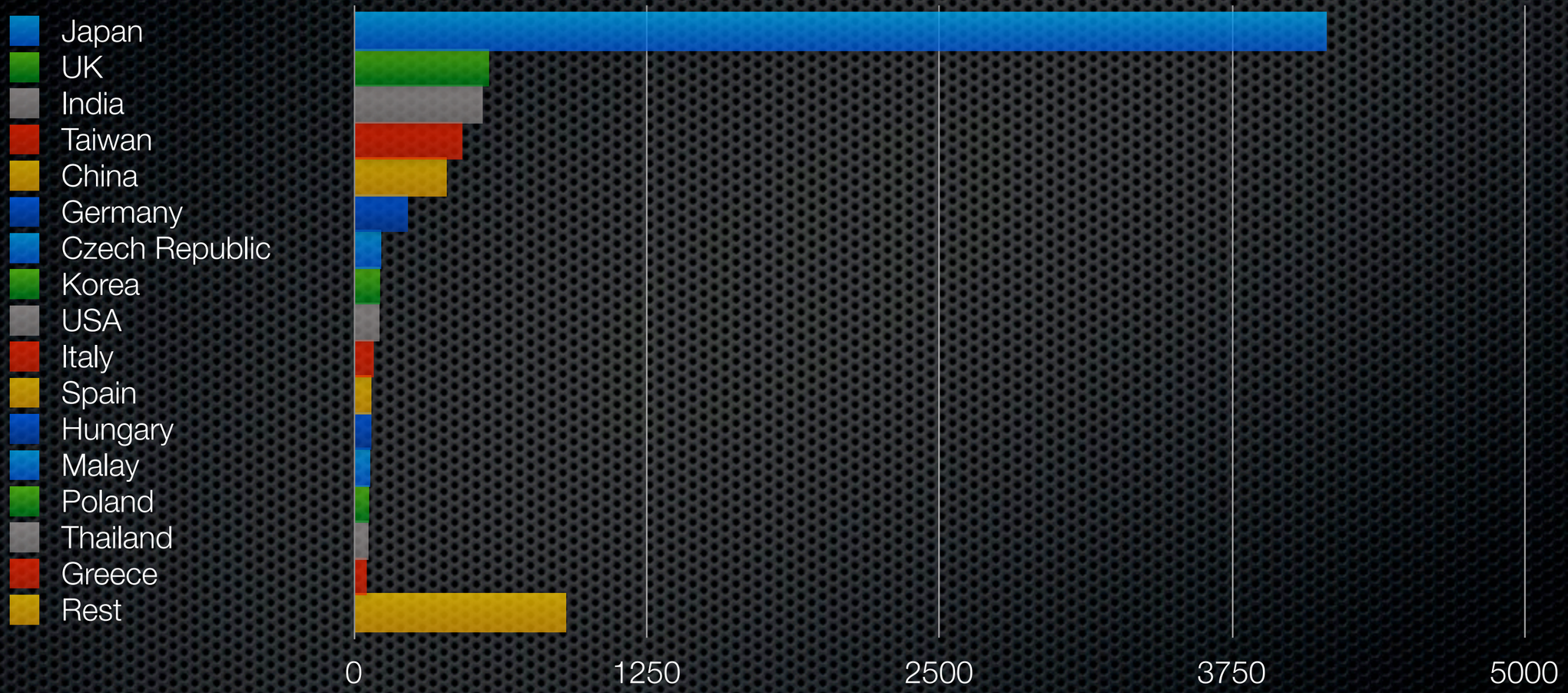
Historie



Status

- Weltweit ca. 8000 zertifizierte Unternehmen
  - Davon über 4000 in Japan
- Weitverbreitetster ganzheitlicher Sicherheitsstandard der Welt
- Starke Entwicklung sektorspezifischer Standards
  - Finance
  - Energy

Verteilung der Zertifizierungen



270XX Familie

- 27000 Terms and Definitions
- 27001 Requirements
- 27002 Code of Practice
- 27003 Impl. Guidance
- 27004 Measurements
- 27005 IS Risk Management
- 27006 Req. for Cert. Bodies
- 27007 Guidel. to Auditing
- 27008 GL. for Auditors on Controls
- 27010 Inter sector inter org. comm.

270XX Familie

- 27000 Terms and Definitions
- 27001 Requirements
- 27002 Code of Practice
- 27003 Impl. Guidance
- 27004 Measurements
- 27005 IS Risk Management
- 27006 Req. for Cert. Bodies
- 27007 Guidel. to Auditing
- 27008 GL. for Auditors on Controls
- 27010 Inter sector inter org. comm.
- 27011 Sector Telecommunication
- 27013 Integ. Impl. of 20000 & 27001
- 27014 Gov. of InfoSec
- 27015 Sector Financial Services
- 27016 Organisational Economics
- 27017 Cloud Computing
- 27018 Public Cloud Computing Serv.
- 27799 Healthcare

270XX Familie

- 27000 Terms and Definitions
- 27001 Requirements
- 27002 Code of Practice
- 27003 Impl. Guidance
- 27004 Measurements
- 27005 IS Risk Management
- 27006 Req. for Cert. Bodies
- 27007 Guidel. to Auditing
- 27008 GL. for Auditors on Controls
- 27010 Inter sector inter org. comm.
- 27011 Sector Telecommunication
- 27013 Integ. Impl. of 20000 & 27001
- 27014 Gov. of InfoSec
- 27015 Sector Financial Services
- 27016 Organisational Economics
- 27017 Cloud Computing
- 27018 Public Cloud Computing Serv.
- 27799 Healthcare
- 27031 ICT Readiness BC
- 27032 Cyber Security
- 27033 Network Security
- 27034 Application Security
- 27035 Information Security Inc. Mgmt.
- 27036 Suppl Relationships
- 27037 Digital Evidence
- 27039 IDPS
- 27040 Storage Security
- 27041-43 Investigation
- 27044 Sec. Inform. and Event Mgmt.

270XX Familie

27000 Terms and Definitions

27001 Requirements

27002 Code of Practice

27003 Impl. Guidance

27004 Measurements

27005 IS Risk Management

27006 Req. for Cert. Bodies

27007 Guidel. to Auditing

27008 GL. for Auditors on Controls

27010 Inter sector inter org. comm.

27011 Sector Telecommunication

27013 Integ. Impl. of 20000 & 27001

27014 Gov. of InfoSec

27015 Sector Financial Services

27016 Organisational Economics

27017 Cloud Computing

27018 Public Cloud Computing Serv.

27799 Healthcare

27031 ICT Readiness BC

27032 Cyber Security

27033 Network Security

27034 Application Security

27035 Information Security Inc. Mgmt.

27036 Suppl Relationships

27037 Digital Evidence

27039 IDPS

27040 Storage Security

27041-43 Investigation

27044 Sec. Inform. and Event Mgmt.

27001:2013

ISO Struktur

ISO Directives

ISO Directives Annex SL

ISO Guide 72

TQM ISO 90XX

ISO 140XX

ISO 270XX

ISO 500xx

ISO Struktur

ISO Directives

ISO Directives Annex SL

ISO Guide 72

TQM ISO 90XX

ISO 140XX

ISO 270XX

ISO 500xx

ISO Struktur

ISO Directives

ISO Directives Annex SL

Depreciated

ISO Guide 72

TQM ISO 90XX

ISO 140XX

ISO 270XX

ISO 500xx

27001:Fokus

- Compliance mit ISO Directives Annex SL für Managementsysteme
  - Ziel: Vereinfachung integrierter Managementsysteme

27001:Fokus

- Compliance mit ISO Directives Annex SL für Managementsysteme
  - Ziel: Vereinfachung integrierter Managementsysteme

This International Standard applies the high-level structure, identical sub-clause titles, identical text, common terms, and core definitions defined in Annex SL of ISO/IEC Directives, Part 1, and therefore maintains compatibility with other management system standards that have adopted the Annex SL.

This common approach defined in the Annex SL will be useful for those organizations that choose to operate a single management system that meets the requirements of two or more management system standards.

27001:Struktur

- 5 - Leadership
- 6 - Planning
- 7 - Support
- 8 - Operation
- 9 - Performance evaluation
- 10 - Improvement

27001:Struktur

- 5 - Leadership
- 6 - Planning
- 7 - Support
- 8 - Operation
- 9 - Performance evaluation
- 10 - Improvement

5.1 Leadership and commitment
5.2 Policy
5.3 Organisational roles, responsibilities and authorities

27001:Struktur

- 5 - Leadership
- 6 - Planning
- 7 - Support
- 8 - Operation
- 9 - Performance evaluation
- 10 - Improvement

27001:Struktur

- 5 - Leadership
- 6 - Planning
- 7 - Support
- 8 - Operation
- 9 - Performance evaluation
- 10 - Improvement

6.1 Actions to adress risk and opportunities

6.2 Information security objectives and plans to achieve them

27001:Struktur

- 5 - Leadership
- 6 - Planning
- 7 - Support
- 8 - Operation
- 9 - Performance evaluation
- 10 - Improvement

27001:Struktur

- 5 - Leadership
- 6 - Planning
- 7 - Support
- 8 - Operation
- 9 - Performance evaluation
- 10 - Improvement

7.1 Resources
7.2 Competences
7.3 Awareness
7.4 Communication
7.5 Documented Information

27001:Struktur

- 5 - Leadership
- 6 - Planning
- 7 - Support
- 8 - Operation
- 9 - Performance evaluation
- 10 - Improvement

27001:Struktur

- 5 - Leadership
- 6 - Planning
- 7 - Support
- 8 - Operation
- 9 - Performance evaluation
- 10 - Improvement

8.1 Operational planning and control
8.2 Information security risk assessment
8.3 Information security risk treatment

27001:Struktur

- 5 - Leadership
- 6 - Planning
- 7 - Support
- 8 - Operation
- 9 - Performance evaluation
- 10 - Improvement

27001:Struktur

- 5 - Leadership
- 6 - Planning
- 7 - Support
- 8 - Operation
- 9 - Performance evaluation
- 10 - Improvement

9.1 Monitoring, measurement, analysis and evaluation
9.2 Internal Audit
9.3 Management Review

27001:Struktur

- 5 - Leadership
- 6 - Planning
- 7 - Support
- 8 - Operation
- 9 - Performance evaluation
- 10 - Improvement

27001:Struktur

- 5 - Leadership
- 6 - Planning
- 7 - Support
- 8 - Operation
- 9 - Performance evaluation
- 10 - Improvement

10.1 Nonconformity and corrective action

10.2 Continual improvement

27002:2013

27002:Fokus

- Stand-alone anwendbar
- Klarere Formulierungen
- Einfachere Implementation
- Reduktion von Redundanz
- Aktualisierung und Verschlankung auf dem technischen Bereichen
  - ca. 3000 technische Änderungen verarbeitet

27002:Struktur

- 5 - Security Policies
- 6 - Organisation of Information Security
- 7 - Human Ressource Security
- 8 - Asset Management
- 9 - Access Control
- 10 - Cryptography
- 11 - Physical and Environmental Security
- 12 - Operations Security
- 13 - Communications Security
- 14 - Sys. Acc. Dev. and Maintenance
- 15 - Supplier Relationships
- 16 - Info. Sec. Incident Management
- 17 - Info. Sec. Aspects of BCM
- 18 - Compliance

27002:Incident Management

- 13 - Communications Security
- 14 - Sys. Acc. Dev. and Maintenance
- 15 - Supplier Relationships
- 16 - Info. Sec. Incident Management
- 17 - Info. Sec. Aspects of BCM
- 18 - Compliance

16.1 Management of information Security Incident and Improvements
16.1.1 Responsibilities and procedures
16.1.2 Reporting information security events
16.1.3 Reporting information security weaknesses
16.1.4 Assesment and decision of information security events
16.1.5 Response to information security incidents
16.1.6 Learning from information security incidents
16.1.7 Collection of evidence

27002:Mobile Devices and Teleworking

Objective: To ensure the security of teleworking and use of mobile devices.

6.2.1 Mobile Device Policy

A policy and supporting security measures should be adopted to protect against the risks introduced by using mobile devices.

Implementation Guidance (... excerpt ...)

Care should be taken when using mobile devices in public places, meeting rooms and other unprotected areas. Protection should be in place to avoid the unauthorized access to or disclosure of the information stored and processed by these devices, e.g. using cryptographic techniques (see chapter 10) and enforcing use of secret authentication information (see control 9.2.3)...

27002:Secure Development Policy

14.2.1 Secure development policy

Rules for the development of software and systems should be established and applied to developments within the organization.

Implementation Guidance (... excerpt ...)

... Secure programming techniques should be used both for new developments and in code re-use scenarios where the standards applied to development may not be known or were not consistent with current best practices. Secure coding standards should be considered and where relevant mandated for use. Developers should be trained in their use and testing and code review should verify their use...

Other Information

Development may also take place inside applications, such as office applications, scripting, browsers and databases.

27002:Secure Development Policy

14.2.1 Secure development policy

Rules for the development of software and systems should be established and applied to developments within the organization.

Implementation Guidance (... excerpt ...)

... Secure programming techniques should be used both for new developments and in code re-use scenarios where the standards applied to development may not be known or were not consistent with current best practices. Secure coding standards should be considered and where relevant mandated for use. Developers should be trained in their use and testing and code review should verify their use...

Other Information

Development may also take place inside applications, such as office applications, scripting, browsers and databases.

Fazit

- Der Standard hat erheblich an Redundanz verloren
- Adressiert die Ziel und Verantwortlichkeiten stärker über Policies
- Viele der Controls sind besser messbar geworden
- Die Anzahl der Länder die den Standard nutzen ist erheblich gestiegen
- Das gesamte Framework ergänzt sich gegenseitig

Personals

xiv – consult
eXcellence in Information Values

Dr.-Ing. Oliver Weissmann
Editor ISO/IEC 27002:2013

xiv-consult GmbH
Königswinterer Str. 409
53639 Königswinter
Mail: ow@xiv-consult.de
Tel.: +49 2223 9192540