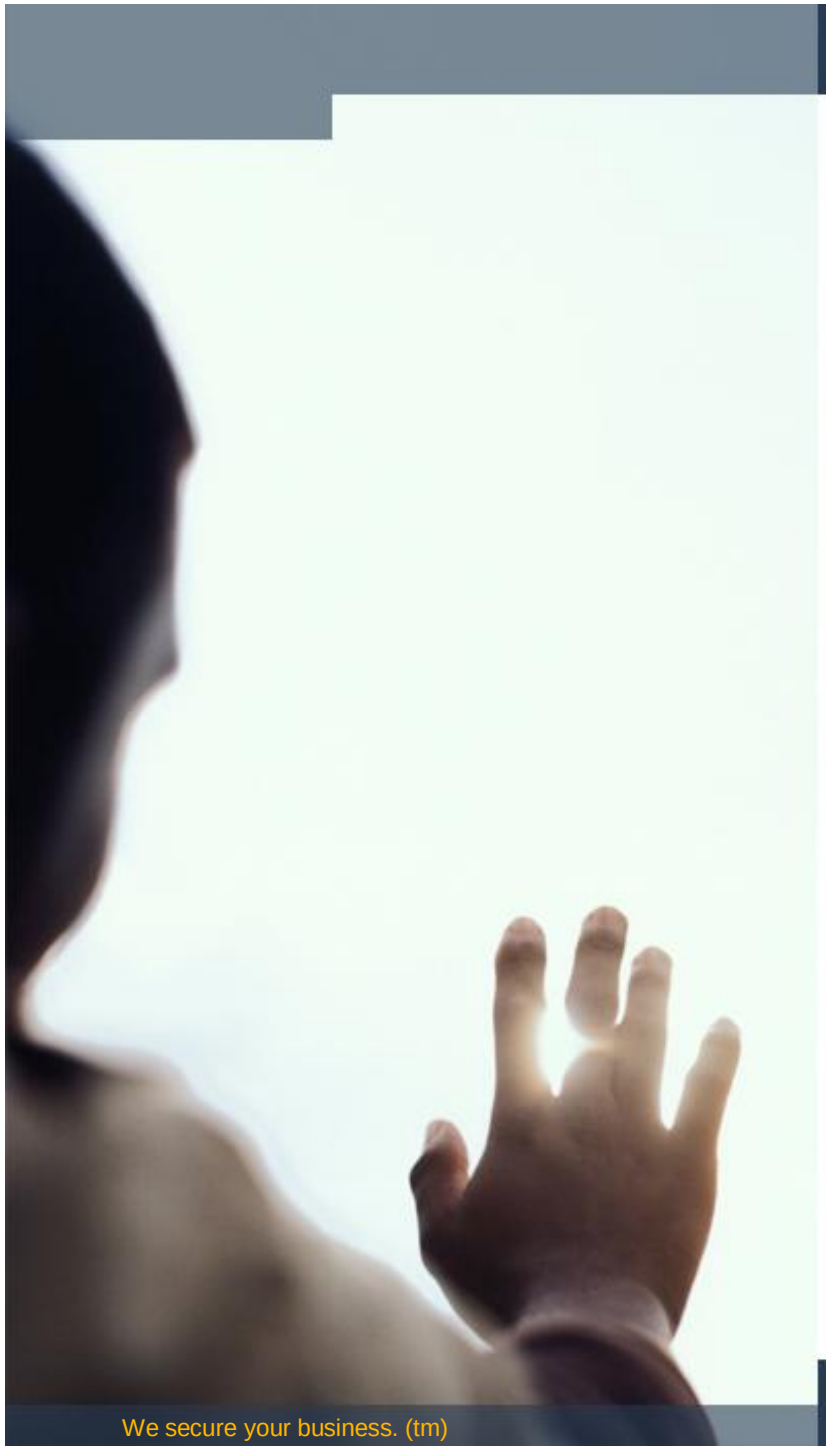


# ISO 27001 / Grundschutzhandbuch

Einführung in den Nachweis der IT-Sicherheit durch Zertifizierung oder Selbsterklärung.

Christoph Puppe
Sicherheitsberater, CISSP
HiSolutions AG, Berlin

# Agenda

- Überblick der Standards
- Inhalte des ISO 27001
- GSHB als deutsche Umsetzung
- Nutzen der Zertifizierung
- Kosten vs. Nutzen
- Projektablauf
- Referenzen HiSolutions

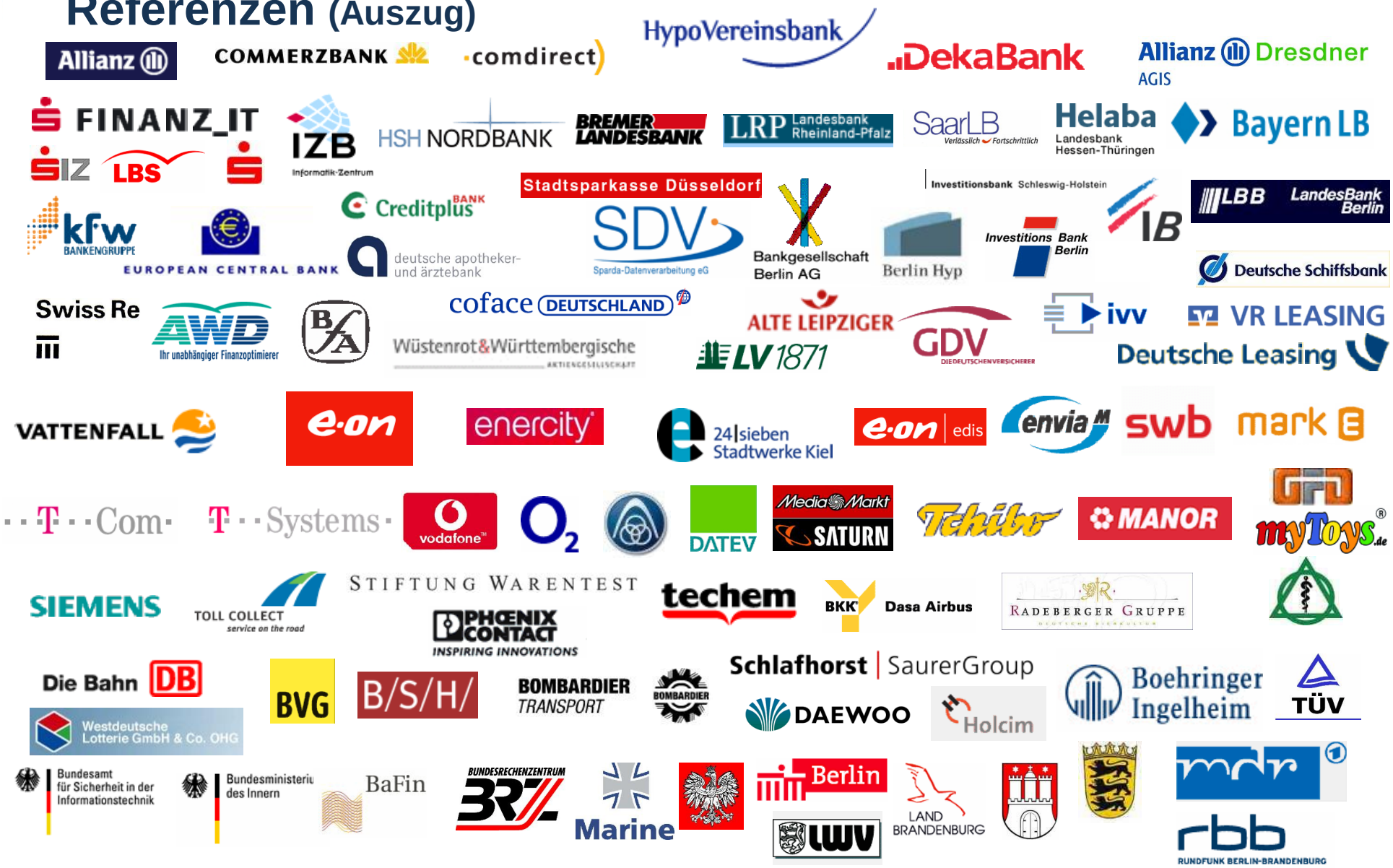
# Visitenkarte HiSolutions AG

| | |
|---|---|
| Gründung | 1994 |
| Vision | Der sichere und effiziente Umgang mit Informationen macht unsere Kunden erfolgreicher |
| Mission | Wir schützen und optimieren die Informationsverarbeitung unserer Kunden mit Organisations- und Technologiekompetenz |
| Felder | § IT-Service Management<br>§ Information Security |
| Mitarbeiter | 45 |
| Firmensitz | Berlin |
| Awards | Innovationspreis Berlin/Brandenburg<br>Fast50 Germany<br>Fast500 Europe |

Deloitte. 2004 Technology Fast 50 Deutschland

Deloitte. 2005 Technology Fast 50 Deutschland

# Referenzen (Auszug)





# Abgrenzung

**British Standards:**

**International Standards:**

| | | |
|---|---|---|
| BS7799-1 | **Leitfaden zum Management von Informationssicherheit: „man sollte“** | ISO17799 |
| BS7799-2 | **Spezifikation für ISMS zur Zertifizierung: „man muss“** | ISO27001 |
| BS7799-3 | **IT Risk Management** | |

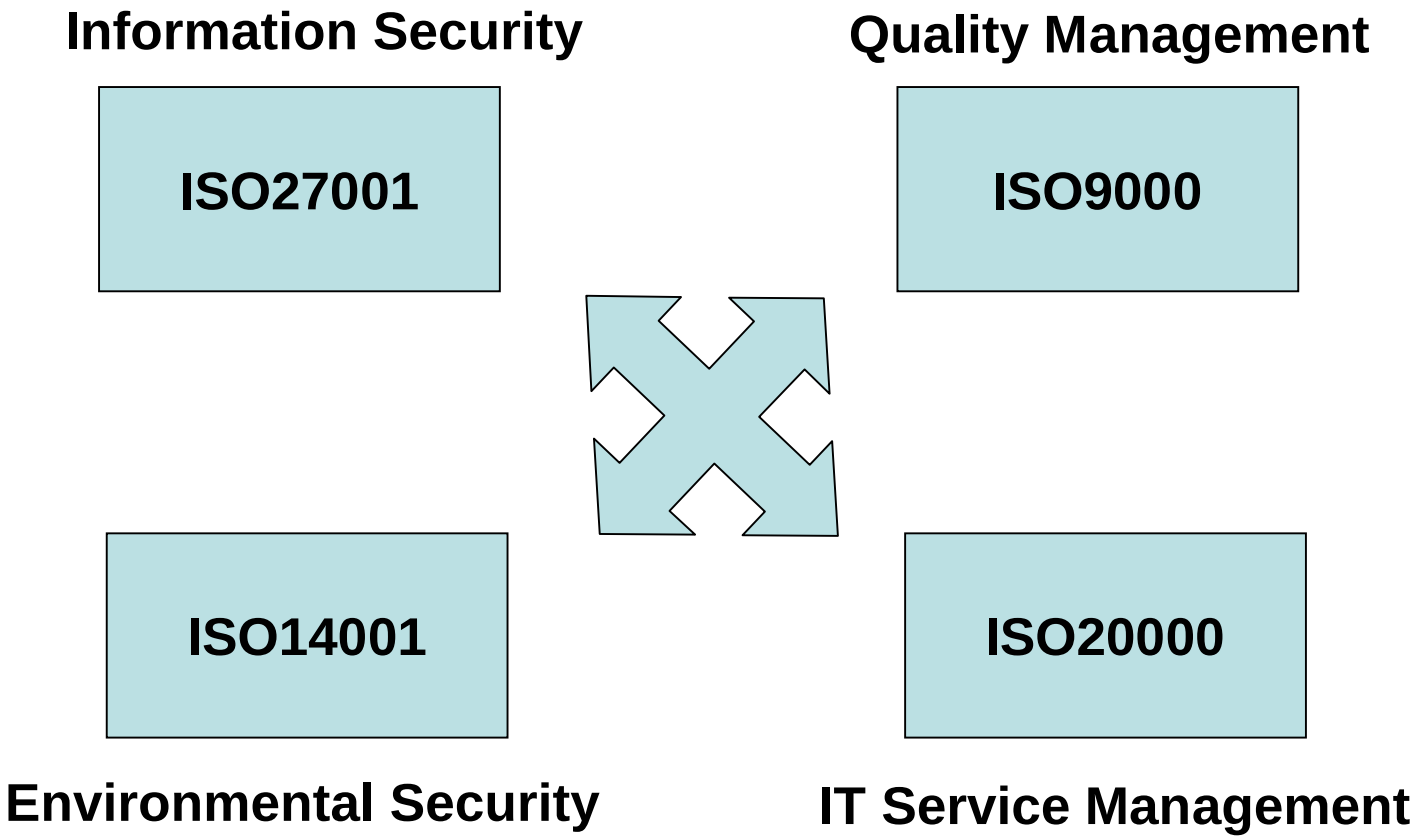


# Überblick ISO2700x-Familie

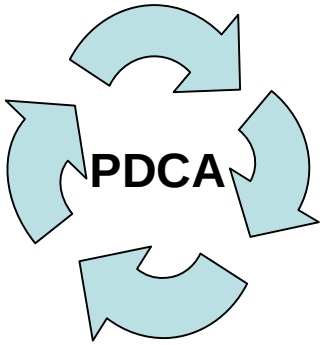
| Nummer | Titel | Status | Ursprung |
|---|---|---|---|
| ISO27000 | Principles and vocabulary | In Entwicklung | Auf Basis von ISO13335 – 1 |
| ISO27001 | ISMS Requirements | Veröffentlicht seit Oktober 2005 | BS-7799:2 (außer Appendix B) |
| ISO27002 | Code of Practice for ISMS | Ab 2007 | ISO17799:2005 |
| ISO27003 | ISMS Implementation Guidance | In Entwicklung | Auf Basis von BS-7799:2 Appendix B |
| ISO27004 | ISMS Metrics and measurement | In Entwicklung, Draft ist veröffentlicht | - |
| ISO27005 | ISMS Risk Management | In Entwicklung | Auf Basis von ISO13335 – 2 |

# Zusammenspiel von Standards

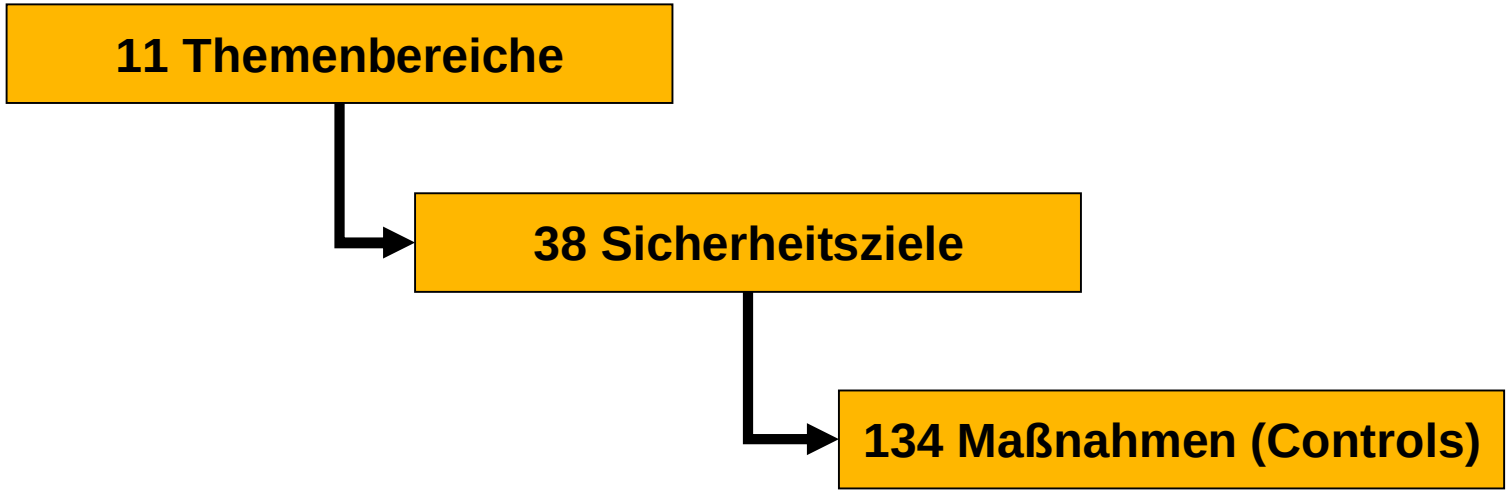


# ISO27001 – Grober Inhalt

- Managementrahmen (Kapitel 4-8)

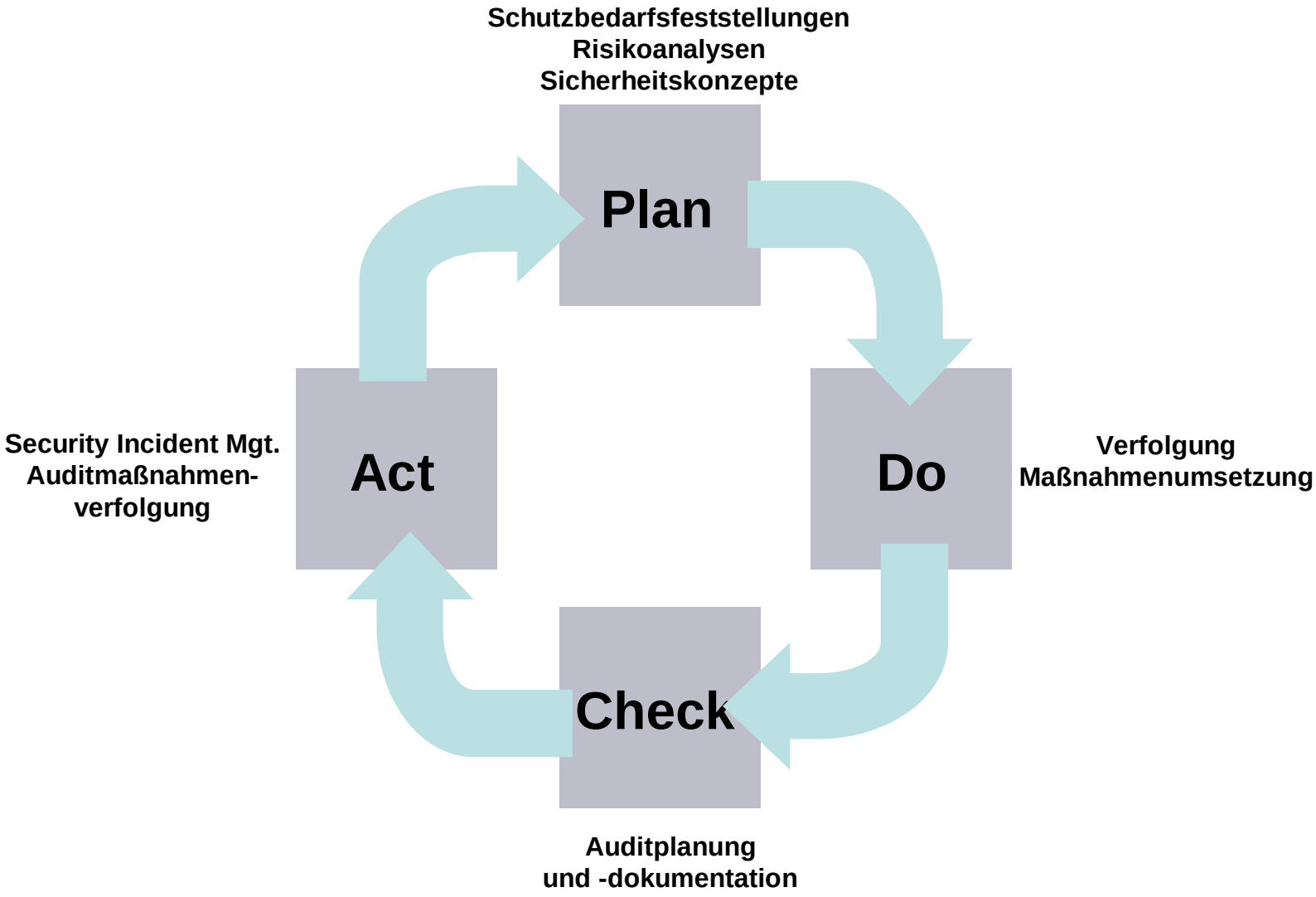



- Normative Anlage A (analog zu ISO17799)




- Zwei weitere Anlagen (hier nicht weiter betrachtet)

# Abbildung des Plan-Do-Check-Act-Modells





Bundesamt
für Sicherheit in der
Informationstechnik

# IT-Grundschutzhandbuch



# Motivation

- Das IT-Grundschutzhandbuch ist für die ökonomischer Erarbeitung wirksamer Sicherheitskonzepte als Standardwerk in Deutschland etabliert.

- Es stellt die Basis für die tägliche Arbeit des IT-Sicherheits-Managements und die kontinuierliche Umsetzung von Standard-Sicherheitsmaßnahmen.

# IT-Grundschutzgedanke

- **Idee**
  - **Gesamtsystem enthält typische Komponenten (z.B. Server und Clients, Betriebssysteme)**
  - **pauschalisierte Gefährdungen und Eintrittswahrscheinlichkeiten**
  - **Empfehlung geeigneter Bündel von Standard-Sicherheitsmaßnahmen**
  - **konkrete Umsetzungshinweise für Maßnahmen**

- **Vorteile**
  - **Arbeitsökonomische Anwendungsweise durch Soll-Ist-Vergleich**
  - **kompakte IT-Sicherheitskonzepte durch Verweis auf Referenzquelle**
  - **praxiserprobte Maßnahmen mit hoher Wirksamkeit**
  - **Erweiterbarkeit und Aktualisierbarkeit**

## Ziel des IT-Grundschutzes

„Durch organisatorische, personelle, infrastrukturelle und technische Standard-Sicherheitsmaßnahmen ein Standard-Sicherheitsniveau für IT-Systeme aufbauen, das auch für sensiblere Bereiche ausbaufähig ist.“

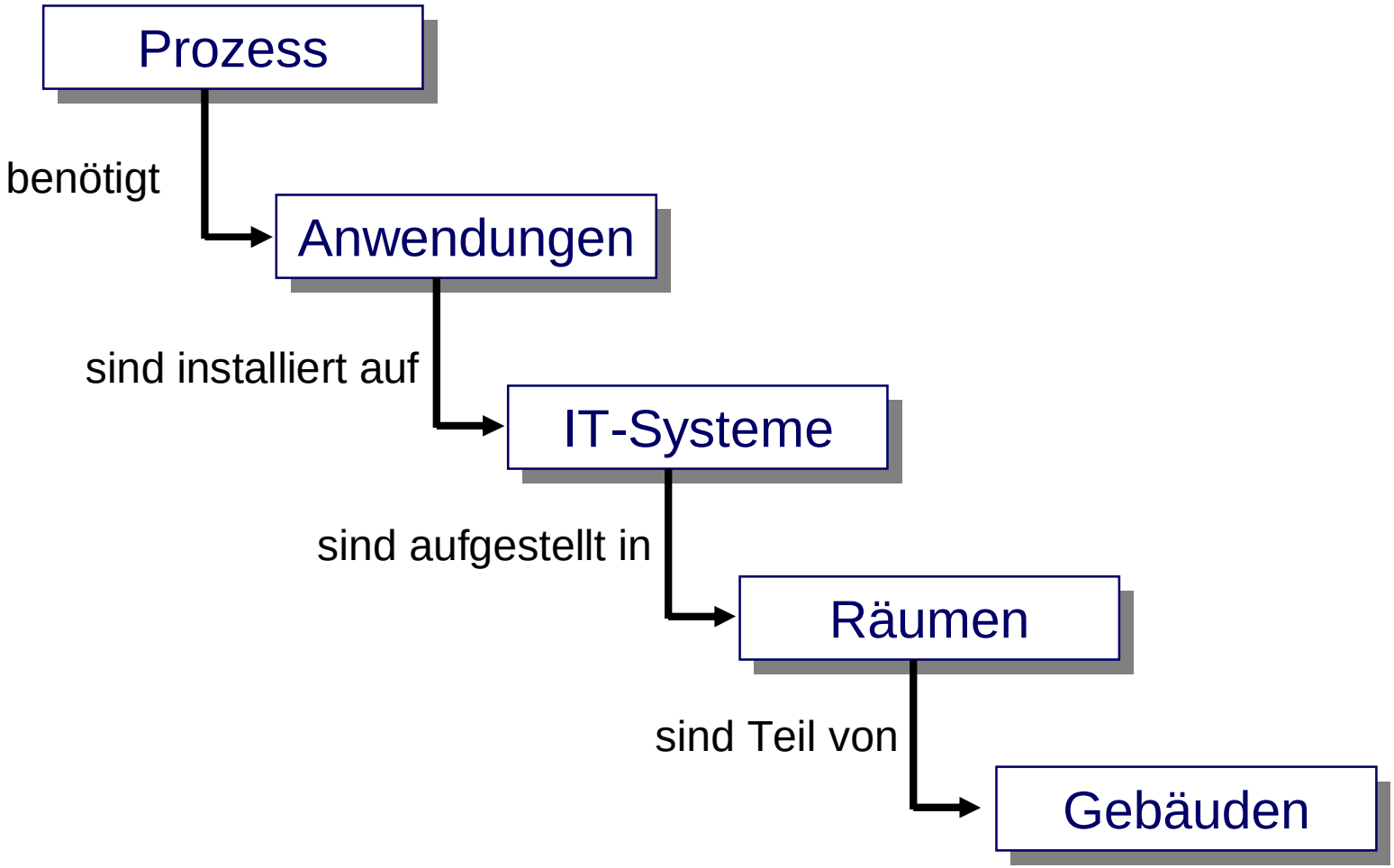
# Generelle Vorgehensweise

- Die Anwendungsweise des IT-Grundschutzhand-buchs ist modulorientiert.
- Anhand der Bestandteile der eigenen Umgebung wählt der Anwender geeignete Bausteine aus und erstellt dadurch ein "Modell" der IT-Landschaft.
- Innerhalb des Modells werden die IT-Sicherheits-aspekte nach den folgenden Themen gruppiert:

| | |
|---|---|
| Schicht 1: | übergreifende Aspekte |
| Schicht 2: | Infrastruktur |
| Schicht 3: | IT-Systeme |
| Schicht 4: | Netze |
| Schicht 5: | IT-Anwendungen |

# Grundsätzlicher Analyseansatz





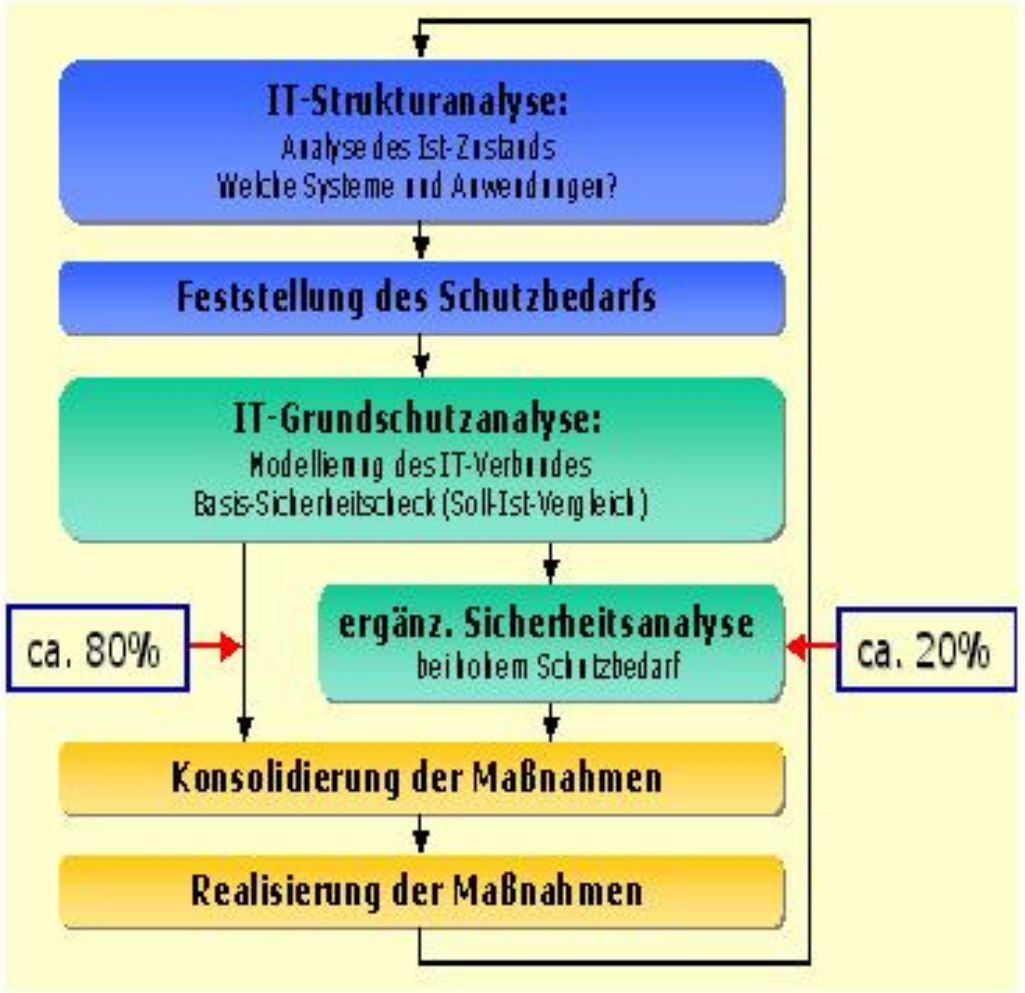
 

# BSI-Standard 100-2

## IT-Grundschutz Vorgehensweise

- bisheriges GSHB Kapitel 2
- Methodik wie man die Normanforderungen umsetzen kann
- Stärkere Fokussierung auf Managementaspekte

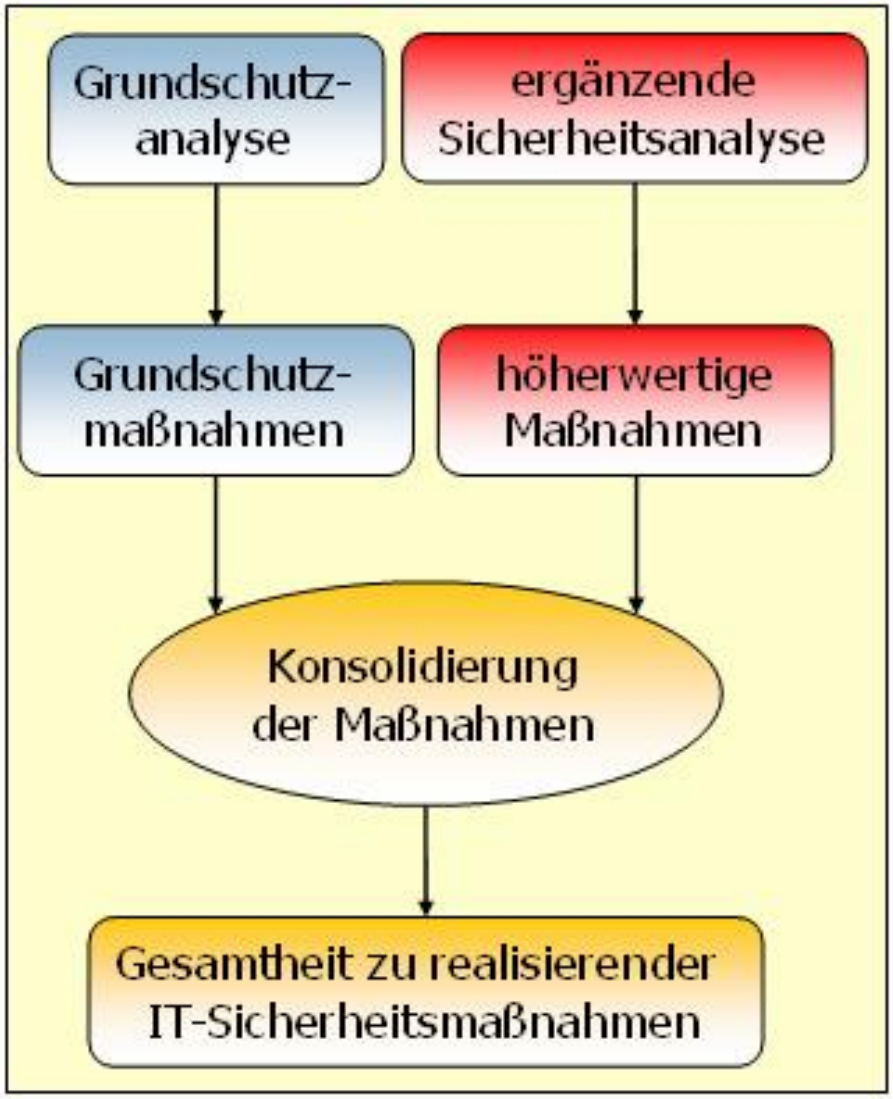
Integration einer Methode zur Risikobetrachtung für hohen und sehr hohen Schutzbedarf



# BSI-Standard 100-3
# Risikoanalyse auf der Basis von IT-GS

## Eine ergänzende Sicherheits-analyse ist durchzuführen, wenn

- hoher oder sehr hoher Schutzbedarf vorliegt,
- zusätzlicher Analysebedarf besteht oder
- für bestimmte Aspekte kein geeigneter Baustein im IT-Grundschutzhandbuch existiert.



# Bausteinstruktur

## 1 Übergeordnete Aspekte

In der Schicht Übergeordnete Aspekte sind folgende Bausteine enthalten:

- B 1.0 IT-Sicherheitsmanagement
- B 1.1 Organisation
- B 1.2 Personal
- B 1.3 Notfallvorsorge-Konzept
- B 1.4 Datensicherungskonzept
- B 1.5 Datenschutz
- B 1.6 Computer-Viren-Schutzkonzept
- B 1.7 Kryptokonzept
- B 1.8 Behandlung von Sicherheitsvorfällen
- B 1.9 Hard- und Software-Management
- B 1.10 Standardsoftware
- B 1.11 Outsourcing
- B 1.12 Archivierung
- B 1.13 IT-Sicherheitssensibilisierung und -schulung

# Bausteinstruktur

## 2 Infrastruktur

In der Schicht Infrastruktur sind folgende Bausteine enthalten:

- B 2.1 Gebäude
- B 2.2 Verkabelung
- B 2.3 Büroraum
- B 2.4 Serverraum
- B 2.5 Datenträgerarchiv
- B 2.6 Raum für technische Infrastruktur
- B 2.7 Schutzschränke
- B 2.8 Häuslicher Arbeitsplatz
- B 2.9 Rechenzentrum
- B 2.10 Mobiler Arbeitsplatz
- B 2.11 Besprechungs-, Veranstaltungs- und Schulungsräume

# Bausteinstruktur

## 3 IT-Systeme

In der Schicht IT-Systeme sind folgende Bausteine enthalten:

- B 3.101 Allgemeiner Server
- B 3.102 Server unter Unix
- B 3.103 Server unter Windows NT
- B 3.104 Server unter Novell Netware 3.x
- B 3.105 Server unter Novell Netware Version 4.x
- B 3.106 Server unter Windows 2000
- B 3.107 S/390- und zSeries-Mainframe
- B 3.201 Allgemeiner Client
- B 3.202 Allgemeines nicht vernetztes IT-System
- B 3.203 Laptop
- B 3.204 Client unter Unix
- B 3.205 Client unter Windows NT
- B 3.206 Client unter Windows 95
- B 3.207 Client unter Windows 2000
- B 3.208 Internet-PC
- B 3.209 Client unter Windows XP
- B 3.301 Sicherheitsgateway (Firewall)
- B 3.302 Router und Switches
- B 3.401 TK-Anlage
- B 3.402 Faxgerät
- B 3.403 Anrufbeantworter
- B 3.404 Mobiltelefon
- B 3.405 PDA

# Bausteinstruktur

## 4 Netze

In der Schicht Netze sind folgende Bausteine enthalten:

- B 4.1 Heterogene Netze
- B 4.2 Netz- und Systemmanagement
- B 4.3 Modem
- B 4.4 Remote Access
- B 4.5 LAN-Anbindung eines IT-Systems über ISDN

# Bausteinstruktur

## 5 IT-Anwendungen

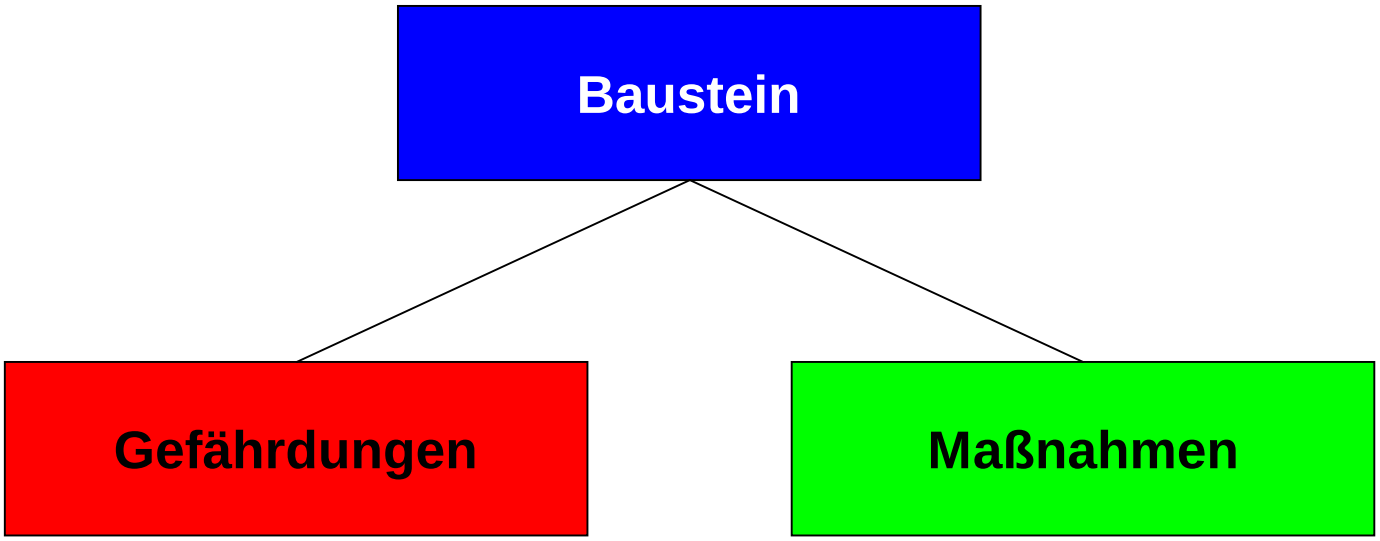
In der Schicht IT-Anwendungen sind folgende Bausteine enthalten:

- B 5.1 Peer-to-Peer-Dienste
- B 5.2 Datenträgeraustausch
- B 5.3 E-Mail
- B 5.4 Webserver
- B 5.5 Lotus Notes
- B 5.6 Faxserver
- B 5.7 Datenbanken
- B 5.8 Telearbeit
- B 5.9 Novell eDirectory
- B 5.10 Internet Information Server
- B 5.11 Apache Webserver
- B 5.12 Exchange 2000 / Outlook 2000

# Bausteinaufbau

Jeder Baustein besteht aus Gefährdungen und Maßnahmen, die den jeweiligen Lebenszyklus-Phasen zugeordnet sind.





# Gefährdungen für Clients unter XP

## Höhere Gewalt

- G 1.1 Personalausfall
- G 1.2 Ausfall des IT-Systems
- G 1.4 Feuer
- G 1.5 Wasser
- G 1.8 Staub, Verschmutzung

## Organisatorische Mängel

- G 2.7 Unerlaubte Ausübung von Rechten
- G 2.9 Mangelhafte Anpassung an Veränderungen beim IT-Einsatz

## Menschliche Fehlhandlungen

- G 3.2 Fahrlässige Zerstörung von Gerät oder Daten
- G 3.3 Nichtbeachtung von IT-Sicherheitsmaßnahmen
- G 3.6 Gefährdung durch Reinigungs- oder Fremdpersonal
- G 3.8 Fehlerhafte Nutzung des IT-Systems
- G 3.9 Fehlerhafte Administration des IT-Systems
- G 3.22 Fehlerhafte Änderung der Registrierung
- G 3.48 Fehlkonfiguration von Windows 2000/XP Rechnern

# Gefährdungen für Clients unter XP

## Technisches Versagen

- G 4.1 Ausfall der Stromversorgung
- G 4.7 Defekte Datenträger
- G 4.8 Bekanntwerden von Softwareschwachstellen
- G 4.23 Automatische CD-ROM-Erkennung

## Vorsätzliche Handlungen

- G 5.2 Manipulation an Daten oder Software
- G 5.4 Diebstahl
- G 5.7 Abhören von Leitungen
- G 5.9 Unberechtigte IT-Nutzung
- G 5.18 Systematisches Ausprobieren von Passwörtern
- G 5.21 Trojanische Pferde
- G 5.23 Computer-Viren
- G 5.43 Makro-Viren
- G 5.52 Missbrauch von Administratorrechten im Windows NT/2000/XP System
- G 5.71 Vertraulichkeitsverlust schützenswerter Informationen
- G 5.79 Unberechtigtes Erlangen von Administratorrechten unter Windows NT/2000/XP Systemen
- G 5.83 Kompromittierung kryptographischer Schlüssel
- G 5.85 Integritätsverlust schützenswerter Informationen

# Maßnahmen für Clients unter Windows XP

## Planung und Konzeption

- M 2.324 (A)Einführung von Windows XP planen
- M 2.325 (A)Planung der Windows XP Sicherheitsrichtlinie
- M 2.326 (A)Planung der Windows XP Gruppenrichtlinien
- M 2.327 (B)Sicherheit beim Fernzugriff unter Windows XP
- M 2.328 (B)Einsatz von Windows XP auf mobilen Rechnern
- M 3.28 (A)Schulung zu Windows 2000/XP Sicherheitsmechanismen für Benutzer
- M 4.48 (A)Passwortschutz unter Windows NT/2000/XP
- M 4.57 (A)Deaktivieren der automatischen CD-ROM-Erkennung
- M 4.75 (A)Schutz der Registrierung unter Windows NT/2000/XP
- M 4.147 (Z)Sichere Nutzung von EFS unter Windows 2000/XP
- M 4.149 (A)Datei- und Freigabeberechtigungen unter Windows 2000/XP
- M 4.243 (Z)Windows XP Verwaltungswerkzeuge
- M 4.244 (A)Sichere Windows XP Systemkonfiguration
- M 4.245 (A)Basiseinstellungen für Windows XP GPOs
- M 4.246 (A)Konfiguration der Systemdienste unter Windows XP
- M 4.247 (A)Restriktive Berechtigungsvergabe unter Windows XP
- M 5.37 (B)Einschränken der Peer-to-Peer-Funktionalitäten in einem servergestützten Netz
- M 5.89 (A)Konfiguration des sicheren Kanals unter Windows 2000/XP
- M 5.90 (Z)Einsatz von IPSec unter Windows 2000/XP
- M 5.123 (B)Absicherung der Netzwerkkommunikation unter Windows XP
- M 4.56 (C)Sicheres Löschen unter Windows-Betriebssystemen

# Maßnahmen für Clients unter Windows XP

## Umsetzung

- M 2.32 (Z)Einrichtung einer eingeschränkten Benutzerumgebung
- M 4.248 (A)Sichere Installation von Windows XP

## Betrieb

- M 2.329 (A)Einführung von Windows XP SP2
- M 2.330 (B)Regelmäßige Prüfung der Windows XP Sicherheitsrichtlinien und ihrer Umsetzung
- M 4.49 (A)Absicherung des Boot-Vorgangs für ein Windows NT/2000/XP System
- M 4.52 (A)Geräteschutz unter Windows NT/2000/XP
- M 4.146 (A)Sicherer Betrieb von Windows 2000/XP
- M 4.148 (B)Überwachung eines Windows 2000/XP Systems
- M 4.249 (A)Windows XP Systeme aktuell halten

## Aussonderung/Stilllegung

- M 4.56 (C)Sicheres Löschen unter Windows-Betriebssystemen

## Notfallvorsorge

- M 6.76 (C)Erstellen eines Notfallplans für den Ausfall eines Windows 2000/XP Netzes
- M 6.78 (A)Datensicherung unter Windows 2000/XP

# Nutzen einer Zertifizierung

## Wem nutzt eine Zertifizierung?

- Unternehmen die auf Grund gesetzlicher oder anderer **Vorschriften** ihre IT-Sicherheit dokumentieren müssen
  - § Nachweis der Erfüllung regulatorischer Anforderungen:
    - Anlage zu § 9 BDSG
    - § 87 TKG (Technische Schutzmaßnahmen)

- IT-Betreiber können das **Niveau** ihrer IT-Sicherheit nach innen und außen dokumentieren.

- Wie sicher sind meine **Geschäftspartner**?

- **Maßstab** für Umsetzung von Standard-Sicherheitsmaßnahmen!

# Kosten / Nutzen

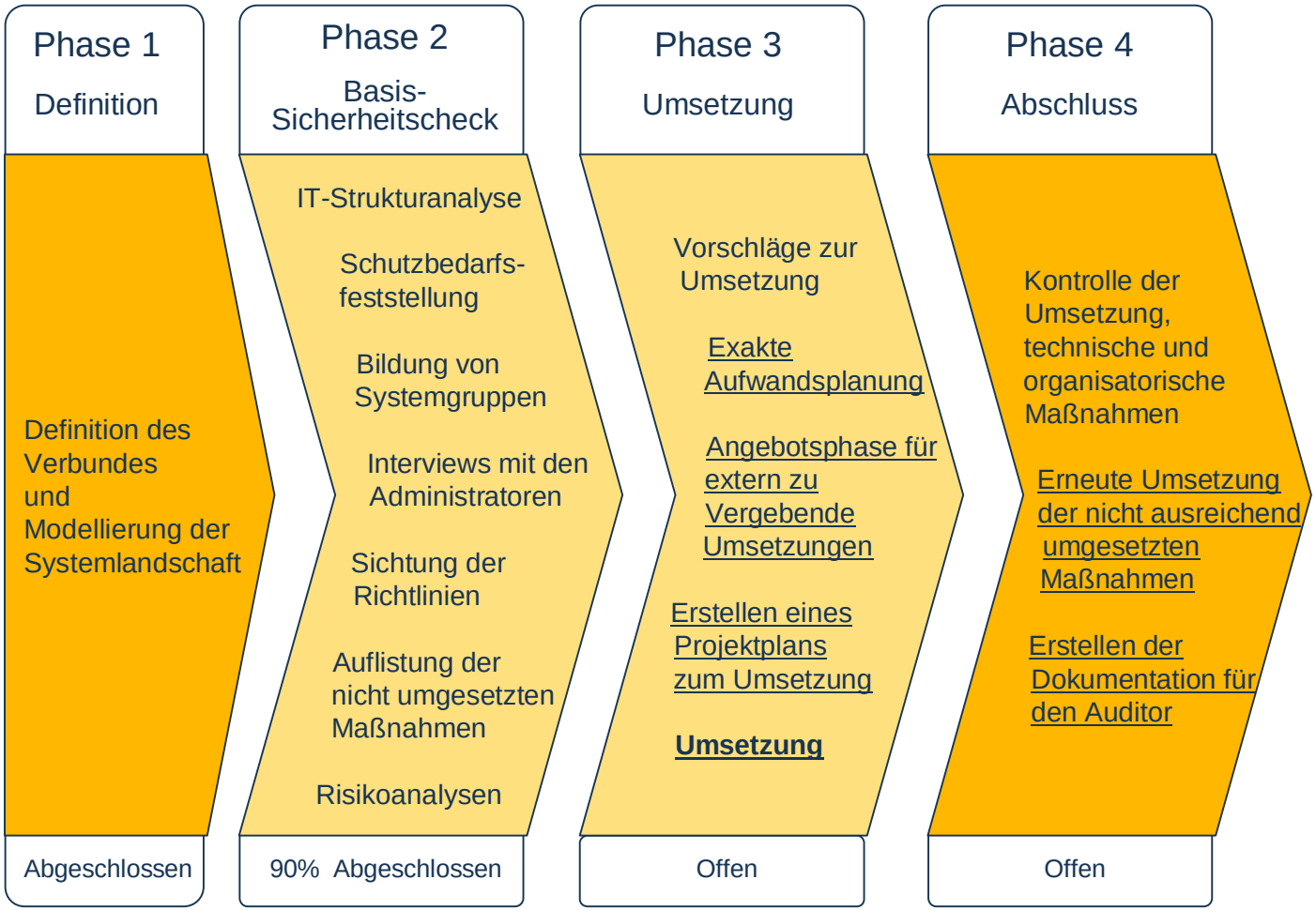
## Kann eine Zertifizierung die ROSI erhöhen, Kosten sparen oder anders einen wirtschaftlichen Beitrag leisten?

- Diverse Zielgruppen verlangen den Nachweis einer sicheren Nutzung der IT
  - Jeder einzelne Nachweis verursacht Kosten
  - Das Zertifikat ist Nachweis für – fast – alle
- Strafgelder und Zivilklagen
  - Wenn der ordnungsgemäße Umgang mit Daten angezweifelt wird, kann das Zertifikat den gegenteiligen Nachweis bringen
- Verhindern von übertriebenen Sicherheitsmaßnahmen
  - Kosten für Sicherheitsmaßnahmen, die über den Branchendurchschnitt liegen können gespart werden
- Gleichmäßige Sicherheit erhöht die Sicherheit
  - Schwachstellen werden vermieden
  - Ausreißer nach Oben werden identifiziert

# Ablauf des Projektes

## Um die Zertifizierung vorzubereiten sind die folgenden Schritte geplant und teilweise umgesetzt.




Unterstrichen sind die Aufgaben, die nicht an die HiSolutions AG vergeben wurden

# Referenzen HiSolutions

- Große Public-Private-Partnerschaft
  - Aufbau ITSM
  - Projektleitung und Umsetzung der Zertifizierungsvorbereitung
  - Zertifizierung
  - Anstehend: Erneuerung des Zertifikats
- Dachverband einer Industrie
  - Projektleitung und Umsetzung der Zertifizierungsvorbereitung
- Verbands RZ einer Genossenschaftsbankgruppe
  - Vorbereitung und Umsetzung der Zertifizierungsvorbereitung
  - Anstehend: Zertifizierung
- Ministerium für Ländliche Entwicklung, Umwelt und Verbraucherschutz
  - Vorbereitung und Umsetzung der Zertifizierungsvorbereitung
  - Zertifizierung
- diverse weitere Projekte nach Grundschutz
  - Versicherung aus dem Süddeutschen: Arbeitsgruppe Projektdefinition
  - BSI: Überarbeitung Baustein „Unix“
  - BSI: Studie „IT-Servicemanagement IT-Grundschutz“
  - Allgemeiner Wirtschaftsdienst (AWD): Sicherheitsanalyse auf Basis GSHB
  - BerlinHyp: Arbeitsgruppe Grundschutzkonzept
  - .etc
- 6 Zertifizierte Grundschutzauditoren, mehr als jede andere Firma

# Kontakt


Anschrift

**HiSolutions AG**
Bouchéstraße 12
D-12435 Berlin

Fon: +49 30 533289-0
Fax: +49 30 533289-99
www.hisolutions.com

Information Security

**Timo Kob**
Mitglied des Vorstands
Leiter Information Security
kob@hisolutions.com

**Alexander Geschonneck**
Leitender Sicherheitsberater
geschonneck@hisolutions.com

# Security Management

## Sicherheit organisatorisch gewährleisten

### Ihr Ziel

- Balance zwischen Sicherheitsbedürfnis und Wirtschaftlichkeit herstellen
- Wirksamkeit technischer Maßnahmen organisatorisch gewährleisten
- Anforderungen KontraG, Basel II und Sarbanes-Oxley-Act nachweisbar erfüllen

### Unsere Leistung

Mit 11 Jahren Erfahrung im Aufbau von ISMS haben wir die Kompetenz, die für Sie optimale Kombination aus Standards und individuellen Anpassungen zu finden. Durch unsere parallele langjährige Nutzung der ITIL-Practices (und als Autor der BSI-Studie „ITIL und IT-Sicherheit“) sind wir seit Jahren einer der Vorreiter der nun allgemein anerkannten Synergien zwischen IT-Sicherheit und ITIL und mussten hier nicht auf einen „fahrenden Zug“ aufspringen. Eine ähnliche Vorreiter-Rolle spielen wir bei der Reifegradsmessung mit SSE-CMM.

- **Umsetzung von Standards** entsprechend BS7799 (ISO 27001), IT Grundschutz, u.a.
- **IT-Security Policies** Entwicklung und Einführung
- **Prozessintegration** mit dem IT-Betrieb gemäß ITIL Best Practices
- **Awareness:** Unterstützung bei der Sensibilisierung der Entscheidungsträger
- **Management technischer Risiken** in der IT
- **Messung des Reifegrades** auf Basis von SSE-CMM/ISO21827

# Business Continuity Management

## Notfälle vermeiden, Schäden minimieren

### Ihr Ziel

- Notfallvermeidung, Aufrechterhaltung der Geschäftsprozesse
- Transparenz der Schwachstellen und Ausfallrisiken
- Begrenzung des Wiederherstellungs-aufwandes in Notfallsituationen
- Vermeidung von Vertrauensverlust und Verbesserung des Ratings

### Unsere Leistung

Wir helfen mit eigener Methodik unseren Kunden bei pragmatischen und effektiven Lösungen von der Business Impact Analyse bis zur Umsetzung risiko-reduzierender Maßnahmen und der Krisenfall-Übung. Wir betrachten die gesamte Breite notfall-relevanter Aspekte und konzentrieren uns nicht allein auf IT-Aspekte - ohne diese zu vernachlässigen.

- **Ermittlung kritischer Prozesse und Ressourcen**
- **Risikobewertung**
- **Risikominimierung:** Technische und organisatorische Maßnahmen
- **Einführung des Notfallmanagements**
- **Entwicklung der Notfallpläne**

# Auditierung und Zertifizierung

## Probleme identifizieren, Sicherheit dokumentieren

### Ihr Ziel

- Angemessene Bewertung der Sicherheitslücken und -maßnahmen
- Nutzung von Informationen aus Benchmarks
- Nachweis der Wirksamkeit eigener Maßnahmen u.a. gegenüber Kunden, Partnern und Aufsichtsbehörden

### Unsere Leistung

HiSolutions ist Mitautor des Grundschutzhandbuchs des BSI und verfügt über mehrere Grundschutz- und BS7799-Auditoren. Mit der Grundschutz-Zertifizierung von Toll Collect und T-Systems wurden die zwei derzeit größten und wohl komplexesten Zertifizierungen durch Auditoren der HiSolutions AG vorbereitet und durchgeführt.

- **Auditierung** gemäß IT-Grundschutz, BS7799 oder OSSTMM
- **Technische Überprüfungen** (bauliche und IT-Infrastruktur, Penetrationstests, Sourcecode-Analysen, etc.)
- **Krisen- und Bedrohungssimulation** durch konkrete Szenarien
- **Prüfung und Bewertung** organisatorischer Abläufe
- **Konkrete Lösungsvorschläge und Priorisierungen**
- **Schulungen** zum Aufbau eigener Prüfkompetenz

# IT-Risikomanagement

## Risiken identifizieren, bewerten und gegensteuern

### Ihr Ziel

- Vergleichbarkeit von IT-Risiken mit anderen Risikotypen
- Valide Aussagen zum Return On Security Investment (ROSI)
- Beitrag zur Erfüllung von Anforderungen Basel II, KontraG oder Sarbanes-Oxley
- Synergien zwischen Risiko-, Security- und Business Continuity Management

### Unsere Leistung

Oft genug laufen in Unternehmen Security-, Risk- und BCM nebeneinander und erzeugen statt Synergieffekten eher Reibungsverluste und Doppelarbeiten (auch bei den anderen Fachbereichen). Wir haben die Methodik und Erfahrung, diese Themen zusammenzuführen. Darüber hinaus unterstützen wir bei der Risikoidentifizierung, -bewertung und -behandlung oder dem Aufbau von Kontrollmechanismen z.B. für Sarbanes-Oxley-Anforderungen.

- **Integration** von Security-, Business Continuity- und Risk Management-Prozessen
- Entwicklung Etablierung von **Risikoanalyse-Methodiken**
- Unterstützung beim Aufbau Sarbanes-Oxley-konformer **Prüf- und Kontrollprozesse**
- **Return On Security Investment-Bewertungen**
- Durchführung von **Risiko-Identifikations- und -Bewertungsprojekten**

# Technische IT-Security

## Wirksame Sicherheitslösungen konzipieren und umsetzen

### Ihr Ziel

- Gefahren der IT-Nutzung reduzieren
- Neue Geschäftsideen mit sicheren Lösungen umsetzen
- Anwendungskomplexität minimieren und Nutzerkomfort auf sicherem Wege verbessern

### Unsere Leistung

Wir helfen Ihnen, die Sicherheit Ihrer IT-Infrastruktur mit innovativen Lösungen zu gewährleisten. Herstellerneutral, kompetent und mit langjähriger Erfahrung beraten wir Sie bei der Lösungsfindung und unterstützen bei der Implementierung neuer oder bei der Härtung/Optimierung bestehender Lösungen. Können Standardprodukte Ihre Anforderungen nicht vollständig erfüllen, so entwickeln wir auch individuelle Lösungen.

- **Innovative Security-Lösungen für verschiedenste IT-Security-Anwendungen**
- **Schutzbedarf bestehender Lösungen ermitteln**
- **Härtung von IT-Systemen**
- **Integration von Standardprodukten und Schließung von Tool-Lücken durch individuelle Lösungen**

# SAP-Sicherheit

## Ihre zentrale Anwendung schützen – auf allen Ebenen

### Ihr Ziel

- Wichtige Daten in den ERP-Systemen schützen
- Korrekte Finanzdaten gewährleisten
- Rechtliche Auflagen erfüllen
- Manipulationen verhindern

### Unsere Leistung

Wir helfen Ihnen, die sichere Konfiguration und sicheren Betrieb der SAP-Systeme zu gewährleisten – auf allen Ebenen: vom Betriebssystem und der Datenbank über die SAP-Konfigurationsmöglichkeiten und Rechtekonzepten bis hin zu starken Authentifizierungsmöglichkeiten.

- **Erstellung von SAP Security Policies und Richtlinien**
- **Überprüfung der Sicherheit von SAP-Systemen**
- **Review von SAP-Sicherheitskonzepten**
- **Beratung bei der Einführung von Authentisierungsmechanismen im R/3-Classic und mySAP-Umfeld**

# Computer Forensik

## Sicherheitsvorfälle erkennen, ermitteln und aufklären

### Ihr Ziel

- Minimierung der Geschäfts- oder Produktionsunterbrechung
- Ermöglichung der straf- bzw. zivilrechtlichen Verfolgung der Täter
- Ermittlung des entstanden Schadens nach einem Systemeinbruch,
- Problemvermeidung für die Zukunft

### Unsere Leistung

Dank langjähriger intensiver Erfahrung durch Zusammenarbeit mit Ermittlungsbehörden, als auch als Autor des deutschen Standardwerks zu diesem Thema bieten wir Ihnen kompetente Unterstützung bei der Erkennung, Ermittlung und letztendlich Vermeidung von Sicherheitsvorfällen.

- **Verdeckte Beweismittelsicherung**
- **Aktive Ermittlung**
- **Auswertung sichergestellter Beweismittel**
- **Erstellung von Ermittlungsberichten**
- **Formulierung von Handlungsempfehlungen für die Vermeidung weiterer Schäden**

# Unsere Stärken

## Auf unseren Feldern zählen wir zu den führenden Beratungs- und Lösungsspezialisten in Deutschland

- Integration von Prozess-, Technologie- und betriebswirtschaftlicher Kompetenz
- Praxis- und umsetzungsorientierte Arbeitsweise, integrierende Tätigkeit auf Prozess- und Lösungsebene, nachhaltiger Wissenstransfer zum Kunden
- Flexibilität, Vertrauenswürdigkeit und Partnerschaftlichkeit, Top-Referenzen und langjährige Kundenbeziehungen
- Profunde Erfahrungen in der Umsetzung etablierter Standards wie ITIL, BS7799, IT-Grundschutz, etc. und Einsatz eigener Modelle und Methoden
- Umfassende Erfahrungen in IT-Organisationen aller Größenordnungen und verschiedenster Branchen sowie in Optimierungs-, Outsourcing-, Merger-, Spin-off- und Benchmarking-Situationen
- Starkes Berater-, Entwickler- und Hackerteam, zertifizierte Berater
- Verständnis als strategischer Servicemanagement- und Sicherheitspartner des Kunden
- Innovative Lösungen in über 50 Ländern auf allen Kontinenten im Einsatz
- und kontinuierliches Wachstum