

Werner Achtert

Managementsysteme für die Informationssicherheit



Vortragsübersicht

- Informationssicherheits-Management
- ISO 17799 und BS 7799-2
- IT-Grundschatz
- Gegenüberstellung ISO / Grundschatz
- Handlungsempfehlungen

IS-Management [1]

Eine umfassende, unternehmensweite Informationssicherheit, ausgerichtet auf

- nachhaltige Vermeidung geschäftsschädigender Vorfälle und
- dauerhafte Erfüllung der Forderungen

erfordert Managementinstrumente zur Planung, Realisierung, Betrieb, Überwachung und kontinuierlichen Verbesserung der IS-Prozesse.



IS-Management [2]

Informationssysteme sind nicht
grundsätzlich auf Sicherheit hin
ausgelegt; die technisch erzielbare
Sicherheit ist begrenzt!



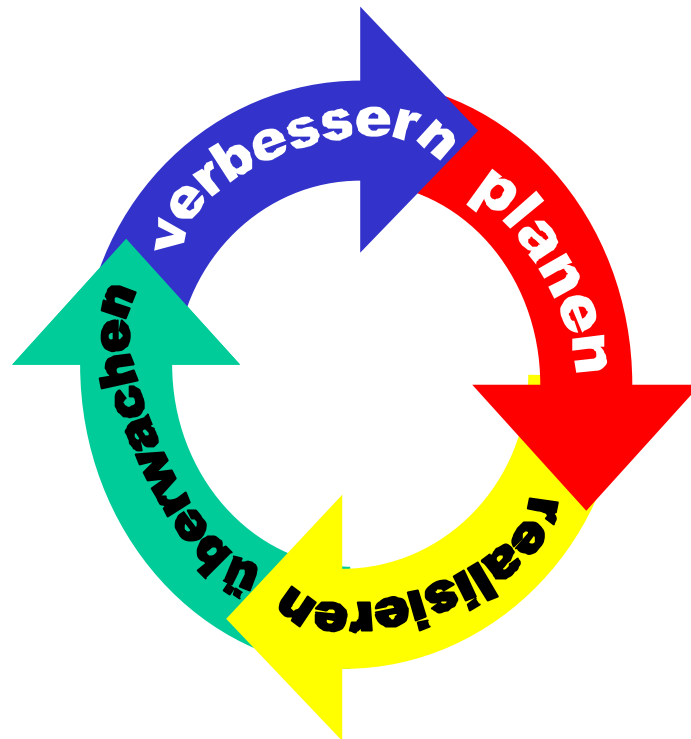
Notwendig:

- System von Verfahren, Prozeduren und Regeln zum Management der Informationssicherheit:
IS-Managementsystem (ISMS)



IS-Management [3]

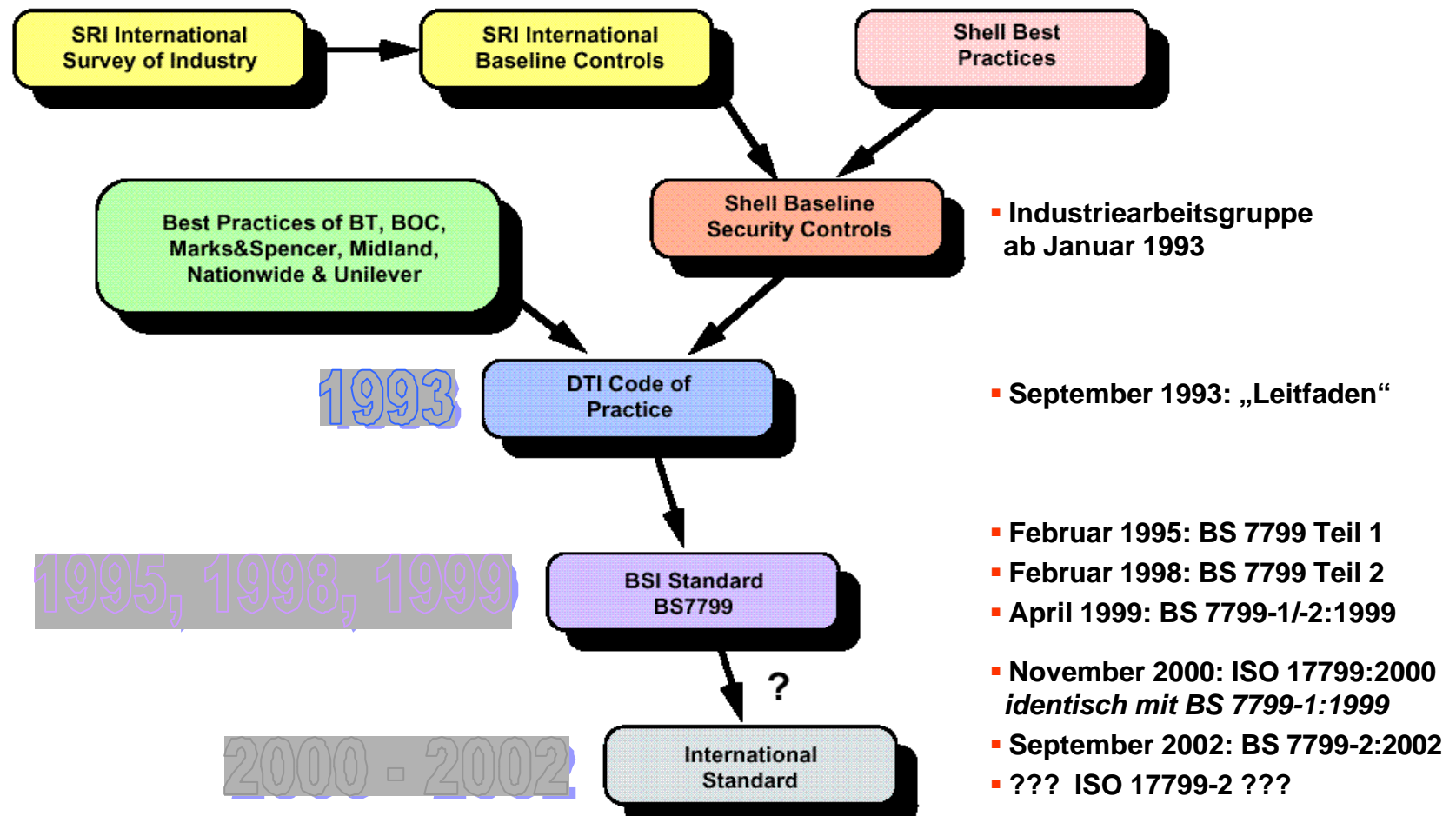
Informationssicherheit ist ein Prozess, der gesteuert (gemanagt) werden muss!



Teilprozesse:

- Planen
- Realisieren und Betreiben
- Überwachen
- Verbessern

Historische Entwicklung ISO 17799

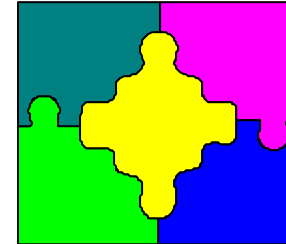


ISO/IEC 17799 auf einen Blick



- **Internationaler Standard (ISO)**
- **Leitfaden für eine umfassende, Informationssicherheit im Unternehmen**
- **gegliedert in 10 Themenbereiche der Informationssicherheit**
- **Basis zur Entwicklung eigener Sicherheitsmaßnahmen und -verfahren im Unternehmen**
- **kein Zertifizierungsschema!**

Themengebiete der ISO/IEC 17799



1. Sicherheitspolitik
2. Organisation der Sicherheit
3. Einstufung und Kontrolle der Werte (Schutzobjekte)
4. Personelle Sicherheit
5. Physische und umgebungsbezogene Sicherheit
6. Management der Kommunikation und des IT-Betriebs
7. Zugangskontrolle
8. Systementwicklung und –wartung
9. Management des kontinuierlichen Geschäftsbetriebs
10. Einhaltung der Verpflichtungen

BS 7799-2 auf einen Blick

- **Britischer Standard mit hoher internationaler Akzeptanz**
- **Spezifiziert Anforderungen an Informationssicherheits-Managementssysteme (ISMS) bzgl.**
 - **Vorgehensmodell** für Planung, Realisierung, Betrieb, Überwachung und kontinuierliche Verbesserung der Informationssicherheit in einem Unternehmen
- **Verweist auf die 10 Themenbereiche der ISO/IEC 17799**
- **Auditierung und Zertifizierung möglich!**

BS 7799-2:2002 im Detail:

Allgemeine Aspekte

- **Modell für Einführung und Betrieb eines effektiven ISMS**
- **ISMS als strategische Entscheidung**
- **ISMS-Ausprägung abhängig von**
 - Geschäftsprofil, -zielen und abgebildeten Prozessen
 - daraus resultierenden Sicherheitsanforderungen
 - Größe und Struktur der Organisation
- **Norm dient zur Feststellung der Fähigkeit einer Organisation:**
 - eigene Forderungen und Kundenforderungen zu erfüllen
 - sonstigen Regelungen und Verpflichtungen gerecht zu werden

BS 7799-2:2002 im Detail:

Verhältnis zu anderen Normen

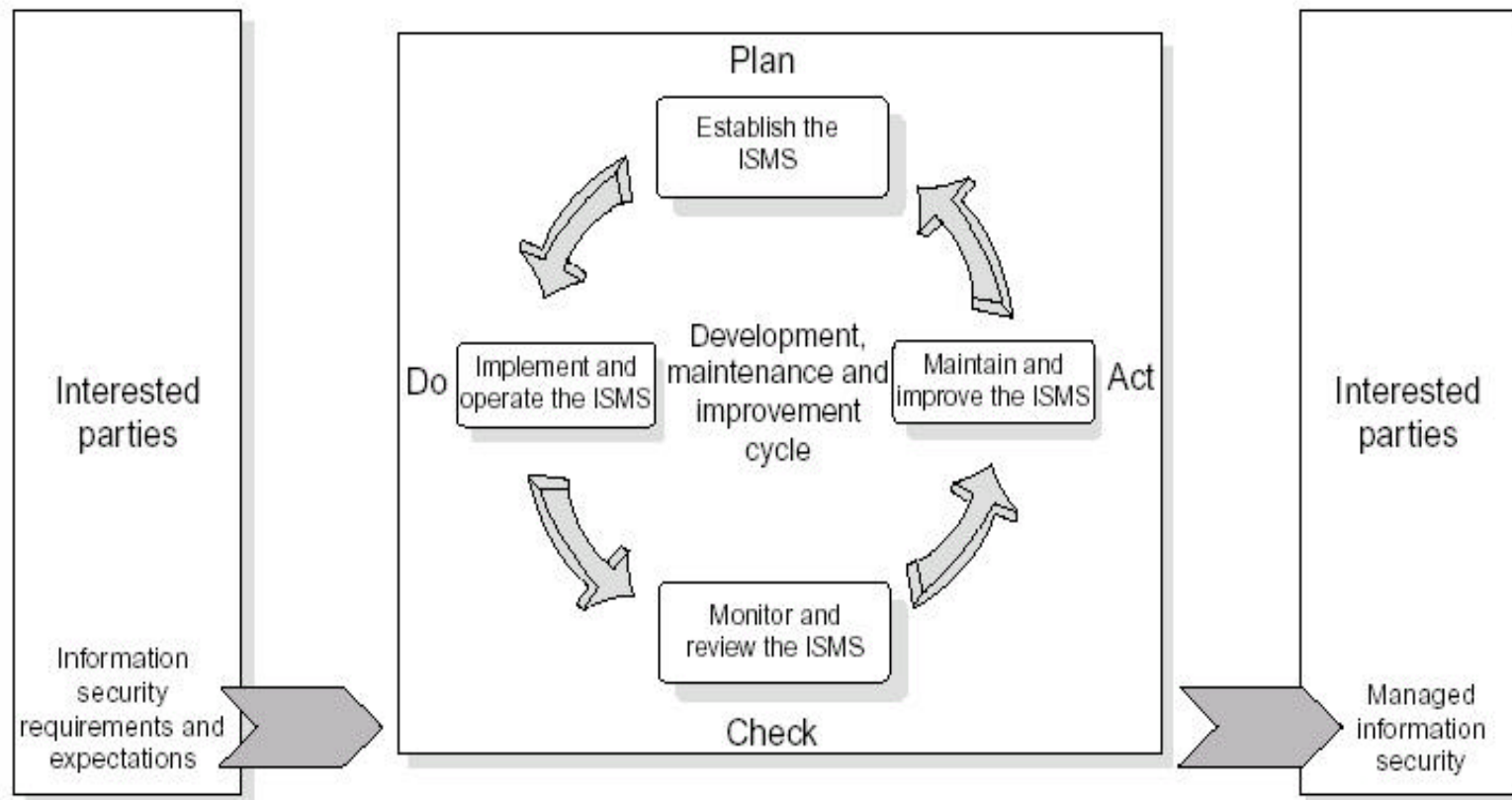
- **Kompatibilität mit ISO 9001:2000 und ISO 14001:1996 erleichtert den Ansatz der integrativen Managementsysteme**
- **Mitgeltende Normen, für die Anwendung der BS 7799-2:2002 unabdingbar:**
 - ISO 9001:2000, Quality management systems — Requirements
 - ISO/IEC 17799:2000, Information technology — Code of practice for information security management
 - ISO Guide 73:2002, Risk management — Vocabulary — Guidelines for use in standards

BS 7799-2:2002 im Detail:

Detailtiefe, Ausschlüsse

- **Anforderungen sind so generisch formuliert, dass sie auf jede Organisation, unabhängig von Art, Größe und Geschäftsprofil anwendbar sind**
- **Ausschlüsse sind nur dann akzeptabel, wenn diese die Fähigkeit und/oder Verantwortung einer Organisation nicht beeinträchtigen, eine Informationssicherheit gem. ihren spezifischen Anforderungen nachhaltig zu betreiben**
- **Etwaige Ausschlüsse sind nur bzgl. der empfohlenen Maßnahmen (gem. Anlage A sowie im Detail gem. ISO/IEC 17799:2000) akzeptabel, nicht jedoch im Hinblick auf die Forderungen der Kapitel 4, 5, 6 und 7.**

BS 7799-2:2002 im Detail: Prozessorientierung



BS 7799-2 - Auditierung und Zertifizierung: Vorteile

- **intensive und kontinuierliche Beschäftigung mit dem Thema Informationssicherheit**
- **Sensibilisierung der Mitarbeiter:**
 - gegen Unachtsamkeit, Nachlässigkeit, Leichtsinn
 - für Schaffung und Einhaltung der Informationssicherheit
- **Auditierung gibt Defizite zu erkennen:**
 - viele kurzfristige Problemlösungen möglich
 - mittelfristige Problemlösungen werden geplant und systematisch angegangen
- **wahrnehmbare Verbesserung der Informationssicherheit**

IT-Grundschutzhandbuch



- **IT-Grundschutzhandbuch – „Sicherheitsmaßnahmen für den mittleren Schutzbedarf“**
 - **Leitfaden** zur Planung, Realisierung, Betrieb und Überwachung einer umfassenden Informationssicherheit (BSI: IT-Sicherheit)
 - **Maßnahmenkatalog**, der über 600 Standard-IT-Sicherheitsmaßnahmen enthält
 - **Spezifikation** der Anforderungen für eine formale

IT-Grundschutz-Qualifizierung: Phasenmodell [1]

- **Initiierungsphase**

(interne Durchführung, ggf. externe Unterstützung):

- Erstellung einer IT-Sicherheitsleitlinie (IT-Sicherheitspolitik)
- Einrichtung eines IT-Sicherheitsmanagements

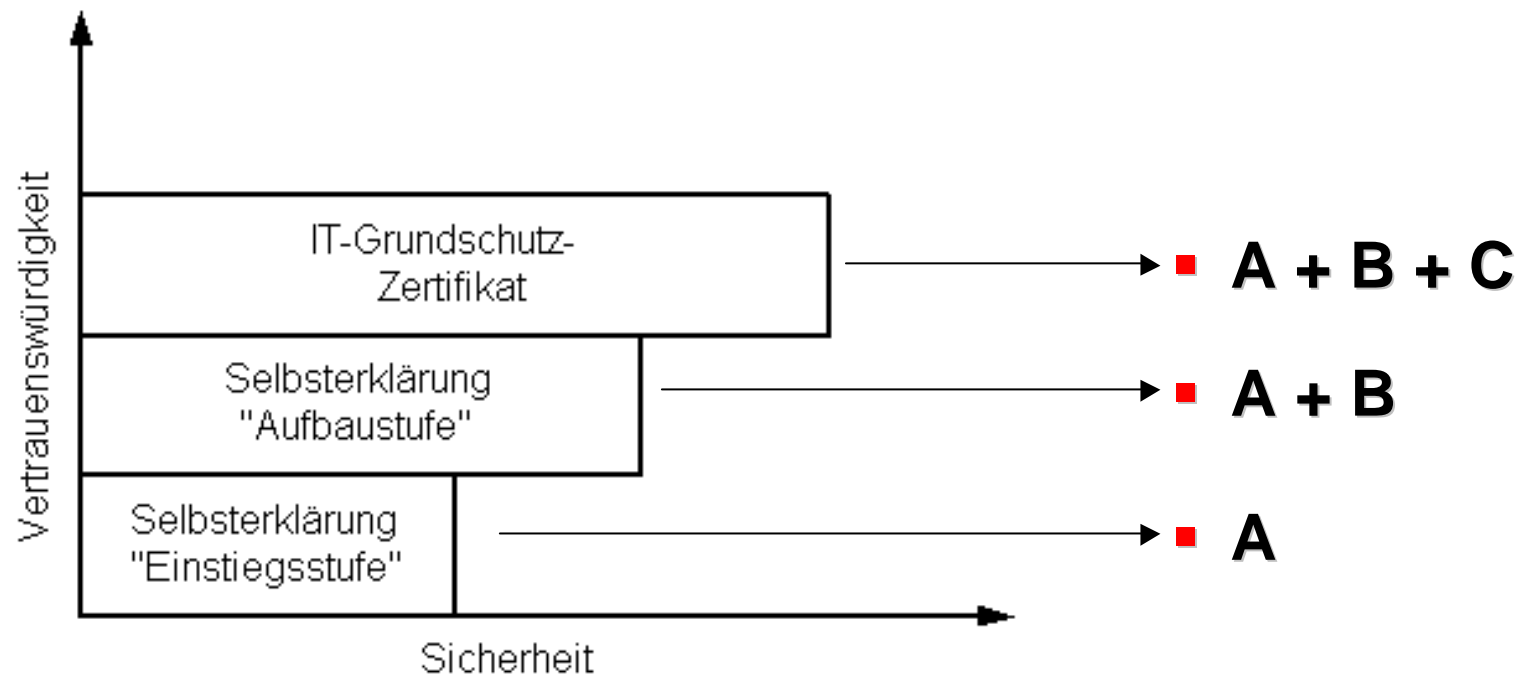
IT-Grundschutz-Qualifizierung: Phasenmodell [2]

- **Erhebungsphase [Konzeption]**
(interne Durchführung, ggf. externe Unterstützung):
 - Definition des IT-Verbundes (Geltungsbereich)
 - IT-Strukturanalyse (Inventarisierung)
 - Feststellung des Schutzbedarfs
 - Modellierung nach IT-Grundschutz
(Identifizierung der erforderlichen Maßnahmen)
 - Basis-Sicherheitscheck (Soll-Ist-Analyse)

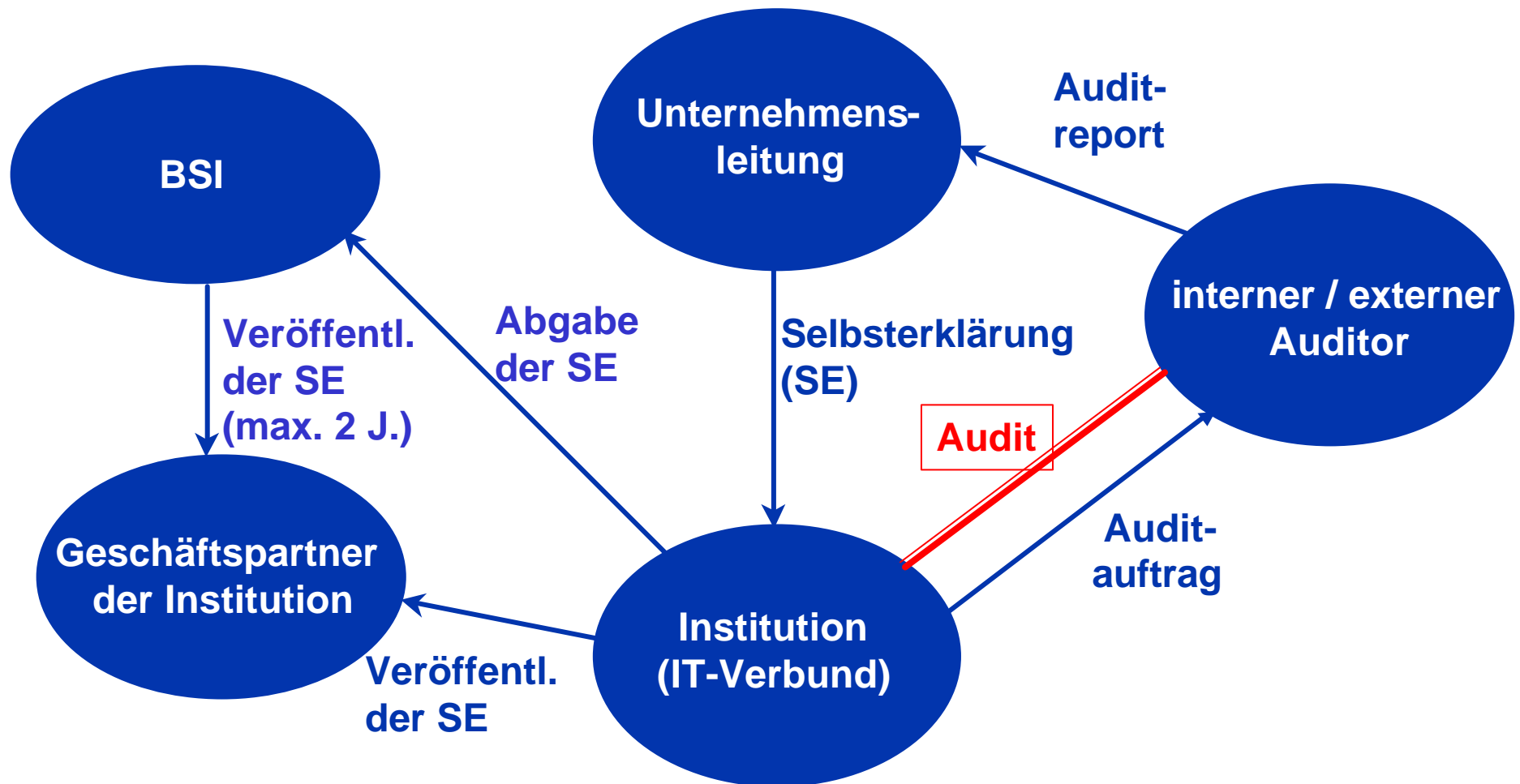
IT-Grundschutz-Qualifizierung: Phasenmodell [3]

- **Qualifizierungsphase [Auditierung und Zertifizierung]**
(interne und/oder externe Durchführung):
 - Auditierung
 - Plausibilitätsprüfung
 - Realisierungsprüfung
 - Abgabe der Selbsterklärung oder Ausstellung des IT-Grundschutz-Zertifikates
 - Re-Qualifizierung

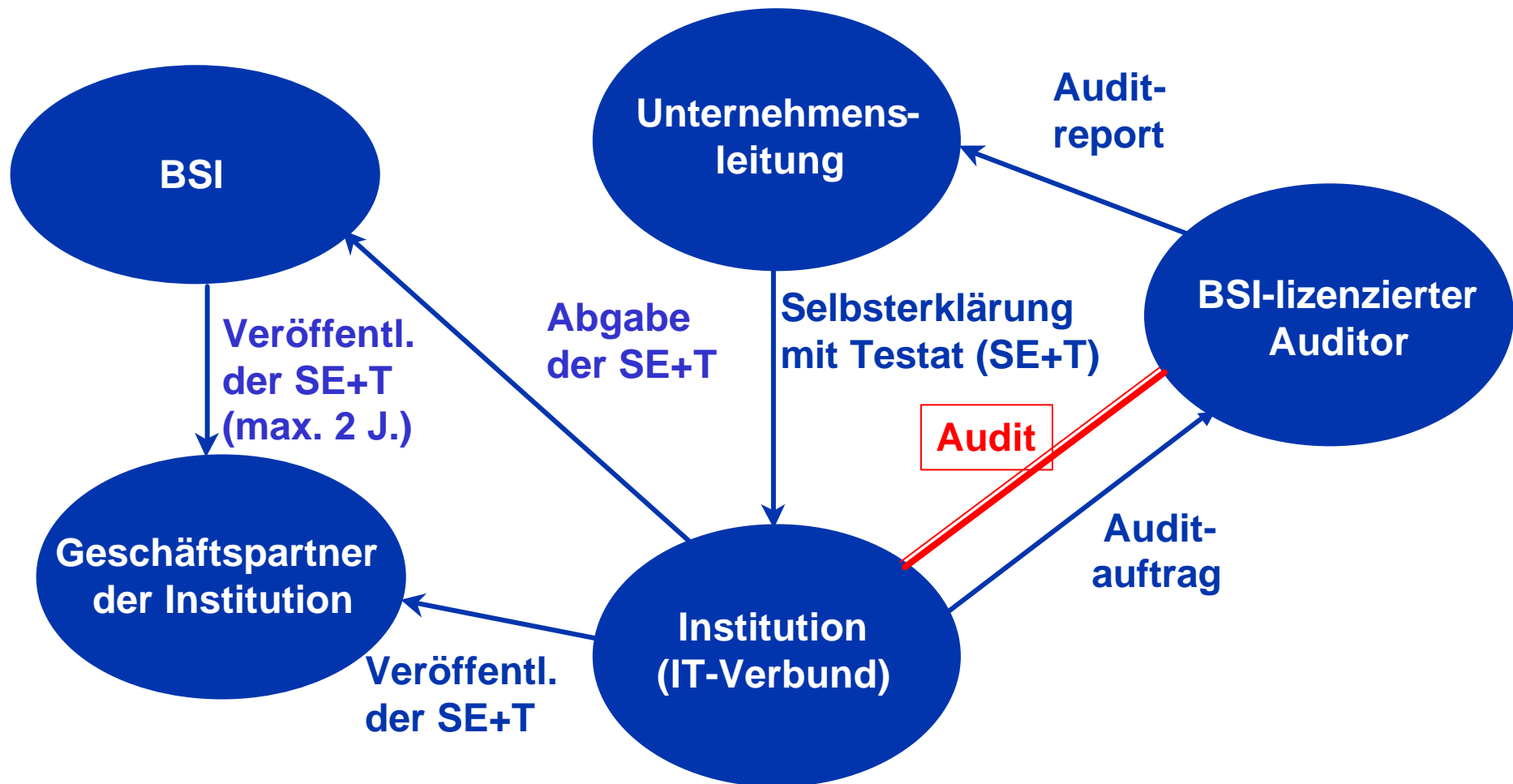
IT-Grundschutz-Qualifizierung: Qualifizierungsstufen



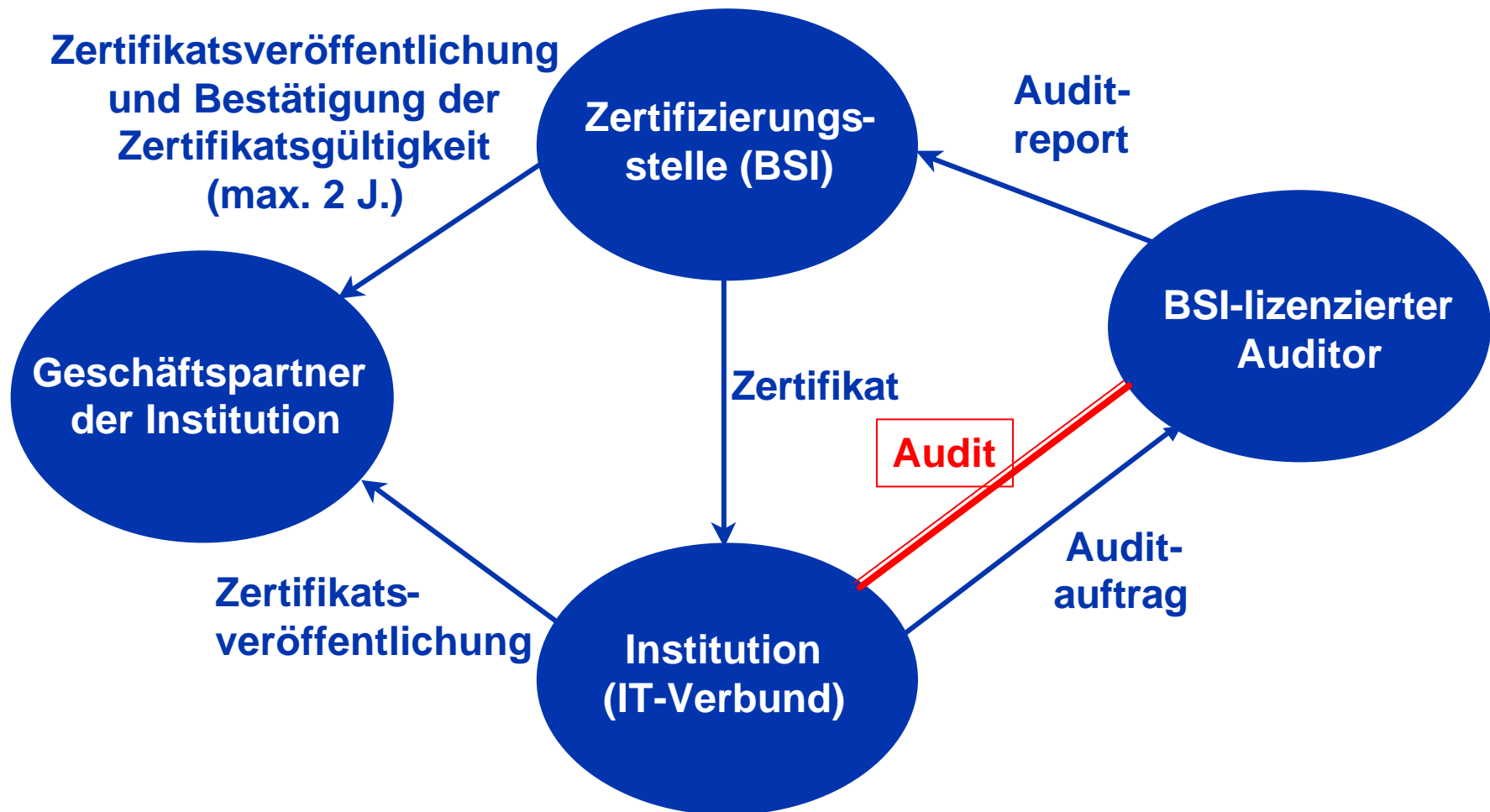
IT-Grundschutz-Qualifizierung: Selbsterklärung



IT-Grundschutz-Qualifizierung: Selbsterklärung mit Testat



IT-Grundschutz-Qualifizierung: Zertifizierung



Vergleich ISO 17799 / IT-GSHB nach Standard-Sicherheitsmaßnahmen

IT-Grundschutzhandbuch **ISO 17799 / BS 7799-2**

- über 600 Maßnahmen
 - konkret, tlw. mit Umsetzungshilfen
 - direkte Eignung für Si.-Konzepte (Soll-Ist-Vergleich möglich und leicht realisierbar)
 - geeignet für Realisierungskonzepte
 - angemessen und ausreichend für einen „Standard“-Schutzbedarf
 - Basis für den über den „Standard“ hinaus gehenden Schutzbedarf
- 127 Maßnahmen
 - eher generisch
 - indirekte Eignung für Si.-Konzepte (Konkretisierung/Interpretation erforderlich)
 - geeignet als Zielrichtung für die Implementierung
 - nach Konkretisierung angemessen für jeden Schutzbedarf

Vergleich ISO 17799 / IT-GSHB nach Wirtschaftlichkeit

IT-Grundschutzhandbuch ISO 17799 / BS 7799-2

- Einsparungen durch Minimierung der „klassischen“ Risikoanalyse
- Aufwand steigt proportional mit Anzahl der einzelnen Schutzobjekte
- Einsparungen durch tlw. konkrete Maßn. und Umsetzungshilfen
- Fachwissen von Vorteil, Expertenwissen i.d.R. nicht erforderlich
- Aufwändig: umfangreiche Risikoanalysen
- Aufwand steigt nur wenig proportional mit Anzahl der einzelnen Schutzobjekte
- Aufwändig: Definition von konkreten Maßnahmen
- Fach- und tlw. Expertenwissen notwendig

Vergleich ISO 17799 / IT-GSHB nach Anwendbarkeit

IT-Grundschutzhandbuch ISO 17799 / BS 7799-2

- für kleine Organisationen i.d.R. zu aufwändig
 - für Organisationen mittlerer Größe gut geeignet
 - für größere Organisationen wird die Anwendung zunehmend schwieriger zu beherrschen
 - einige Einschränkungen bzgl. Systeme und Anwendungen
 - für Anwendung im Ausland: einige sprachliche Einschränkungen (de,en)
- auch für kleine Organisationen geeignet, da Ausschlüsse möglich
 - für Organisationen mittlerer Größe geeignet
 - für größere Organisationen bestens geeignet
 - keine Einschränkungen bzgl. Systeme und Anwendungen
 - wenig sprachliche Einschr., da ISO-Dok. in vielen Sprachen verfügbar

Vergleich ISO 17799 / IT-GSHB nach Ausbaufähigkeit

IT-Grundschutzhandbuch ISO 17799 / BS 7799-2

- stufenweise Einführung möglich (z. B. durch Beachtung der Maßnahmenkategorien A,B,C)
- Sicherheitsmaßnahmen für einen höheren Schutzbedarf sind jederzeit als „Add-on“ realisierbar
- stufenweise Einführung möglich (z. B. durch höhere Priorisierung der „brennenden“ Punkte)
- Betrachtung der sogenannten Risikobereiche kann jederzeit auf sonstige Bereiche erweitert werden

Vergleich ISO 17799 / IT-GSHB nach Nachweisbarkeit

IT-Grundschutzhandbuch ISO 17799 / BS 7799-2

- messbare, revisionsfähige und für Dritte nachvollziehbare Informationssicherheit durch:
 - Qualifizierung nach IT-Grundschutz:
 - Einstiegsstufe
 - Aufbaustufe
 - IT-Grundschutz-Zertifizierung
 - Prüf- und Zertifizierungsschema fertig gestellt
- für Dritte nachvollziehbares Informationssicherheits-Management durch:
 - Zertifizierung nach BS 7799-2, unter Benutzung der ISO 17799 als Leitfaden für die Sicherheitsmaßnahmen
 - Prüf- und Zertifizierungsschema etabliert u. international anerkannt



TÜV Informationstechnik GmbH

- ein Unternehmen der RWTÜV-Gruppe -

Geschäftsstelle Süd
Hübnerstraße 3
D-86150 Augsburg

Werner Achtert

Telefon: +49 (0) 821/45 09 54 – 42 60

Telefax: +49 (0) 821/45 09 54 – 42 69

E-Mail: w.achtert@tuvit.de

URL: <http://www.tuvit.de>