



26. DECUS Symposium

IT-Grundschutz-Zertifizierung

Angelika Jaschob
E-Mail: gssiegel@bsi.bund.de

Bundesamt für Sicherheit in der Informationstechnik
Referat I 1.4 - Systemsicherheit und Grundschutz

Dipl. Math. Angelika Jaschob 1 Bundesamt für Sicherheit in der Informationstechnik



Das BSI

Das Bundesamt für Sicherheit in der Informationstechnik wurde 1991 auf Gesetzesgrundlage errichtet. § 3 des BSI-Gesetzes vom 17.12.1990 (Bundesgesetzblatt I S. 2834) definiert die Aufgaben.

BSI heute:

- etwa 400 Mitarbeiter
- 3 Abteilungen



Dipl. Math. Angelika Jaschob 2 Bundesamt für Sicherheit in der Informationstechnik

Das BSI



Sitz: Bonn; ca. 400 Mitarbeiter

Hotlines

- Grundschatz: (01888) 9582 - 369
- Computer-Viren: - 444
- Zertifizierung: - 111
- CERT-Bund: - 222

Aufgaben des BSI:

- Förderung der IT-Sicherheit
- Aufklärung und Sensibilisierung der Bürger
- Sicherheitsbewertung von IT-Systemen oder -Komponenten
- Zertifizierung (ITSEC, Common Criteria, IT-Grundschatz)
- Entwicklung von Kryptosystemen
- Beratung der Hersteller, Verreiber und Anwender
- IT-Grundschatz

<http://www.bsi.bund.de>



Dipl. Math. Angelika Jaschob3Bundesamt für Sicherheit in der Informationstechnik

IT-Grundschatz 2002



IT-Grundschatz-handbuch 2002

- 55 Bausteine
- 600 Maßnahmen
- 2000 Seiten



Dipl. Math. Angelika Jaschob4Bundesamt für Sicherheit in der Informationstechnik

Registrierte Anwender (Auswahl)

> **3.500** registrierte Anwender,
davon

> **500** im Ausland

Auflage 2001:

> **20.000** Handbücher/CD-ROMs

- BASF
- DATEV eG
- Deutsche Bank AG
- Deutsche Telekom AG
- Hamburg-Mannheimer
- IBM Deutschland
- Merck KGaA
- Robert Bosch GmbH,
- Siemens AG
- Volkswagen AG
- u.v.m

Dipl. Math. Angelika Jaschob5Bundesamt für Sicherheit
in der Informationstechnik

Bezugsquellen IT-Grundschutzhandbuch



Print-Version- Loseblattsammlung
ca. 2200 Seiten, € 148
Bundesanzeigerverlag

BSI-CD-ROM (auch in Englisch)
kostenlos- gegen Rückumschlag
www.bsi.bund.de/produkte/cdrom

Internet
www.bsi.bund.de
10 internationale Mirrors

Dipl. Math. Angelika Jaschob6Bundesamt für Sicherheit
in der Informationstechnik

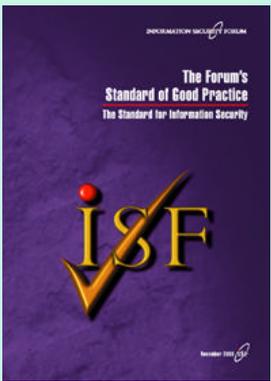
Informationsquellen

Sicherheitsstandards





Initiative D21
„IT-Sicherheitskriterien im Vergleich“
www.initiatived21.de/arbeitsgruppen/5sicherheit/leitfaden.pdf



Information Security Forum (ISF)
„The Forum's Standard of Good Practice“
www.isfsecuritystandard.com

Dipl. Math. Angelika Jaschob 7 Bundesamt für Sicherheit in der Informationstechnik

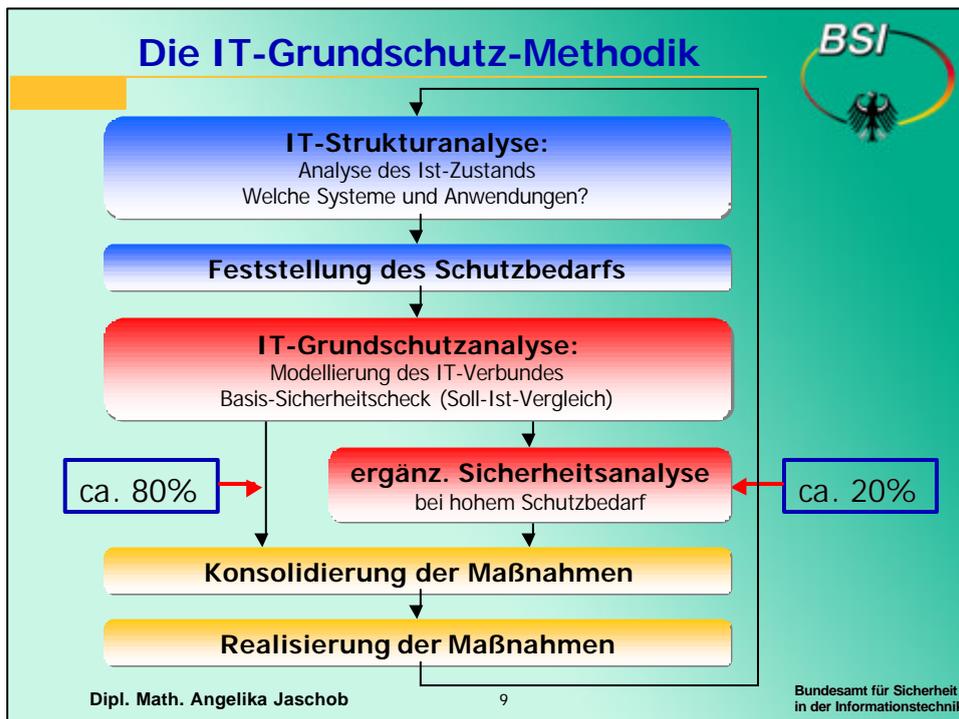
Grundwerte der IT-Sicherheit



IT-Sicherheit

- Schutz der Vertraulichkeit**
eine bestimmte Information dem berechtigten Anwender
- Schutz der Integrität**
Unversehrtheit und Korrektheit der Information
- Schutz der Verfügbarkeit**
zur rechten Zeit am rechten Ort

Dipl. Math. Angelika Jaschob 8 Bundesamt für Sicherheit in der Informationstechnik



IT-Grundschutz-Zertifizierung

BSI

Warum?

- Unternehmen und Behörden wollen Sicherheitsniveau dokumentieren
- Wie sicher sind meine Geschäftspartner?
 - » Maßstab für Umsetzung von Standard-Sicherheitsmaßnahmen

intern
nach außen

Dipl. Math. Angelika Jaschob 10 Bundesamt für Sicherheit in der Informationstechnik

IT-Grundschutz-Zertifizierung



Wer?

- Unternehmen oder Behörden, die mit anderen Institutionen zu kooperieren beabsichtigen
- E-Commerce-Anbieter für den Nachweis gegenüber Kunden
- Behörden im E-Government für den Nachweis gegenüber Bürgern
- Unternehmen, die aufgrund gesetzlicher oder anderer Vorschriften ihre IT-Sicherheit dokumentieren müssen (z.B. Banken)

Dipl. Math. Angelika Jaschob 11 Bundesamt für Sicherheit
in der Informationstechnik

IT-Grundschutz-Zertifizierung



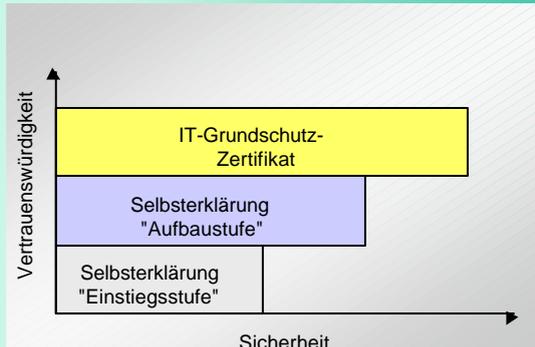
Was?

- ein oder mehrere Geschäftsprozesse
- eine oder mehrere Fachaufgaben
- eine oder mehrere Organisationseinheiten
- nicht notwendigerweise das gesamte Unternehmen
- IT-Verbund muss eine sinnvolle Mindestgröße haben!

Dipl. Math. Angelika Jaschob 12 Bundesamt für Sicherheit
in der Informationstechnik

Ausprägungen der Zertifizierung

- IT-Grundschutz-Zertifikat
- Selbsterklärung "IT-Grundschutz Aufbaustufe"
- Selbsterklärung "IT-Grundschutz Einstiegsstufe"



Dipl. Math. Angelika Jaschob 13 Bundesamt für Sicherheit
in der Informationstechnik

IT-Grundschutz-Zertifizierung Stufen

Zuordnung der Maßnahmen:

- "A"**: Umsetzung ist für alle drei Stufen erforderlich
- "B"**: Umsetzung ist für Aufbaustufe und für Zertifikat erforderlich
- "C"**: Umsetzung ist nur für das IT-Grundschutz-Zertifikat erforderlich



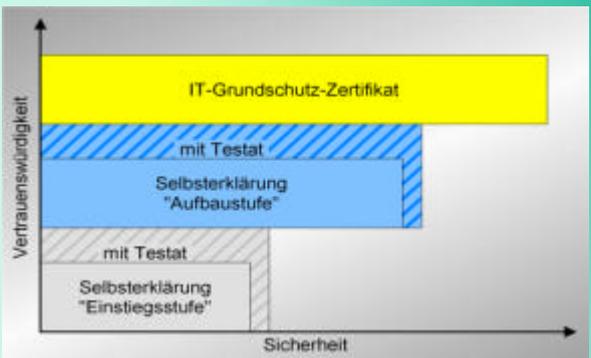
Dipl. Math. Angelika Jaschob 14 Bundesamt für Sicherheit
in der Informationstechnik

Arten der Qualifizierung



- Selbsterklärung "IT-Grundschutz Einstiegsstufe" mit Testat
- Selbsterklärung "IT-Grundschutz Aufbaustufe" mit Testat
- IT-Grundschutz-Zertifikat





Dipl. Math. Angelika Jaschob
15
Bundesamt für Sicherheit in der Informationstechnik

Selbsterklärung mit Testat

Inhalt

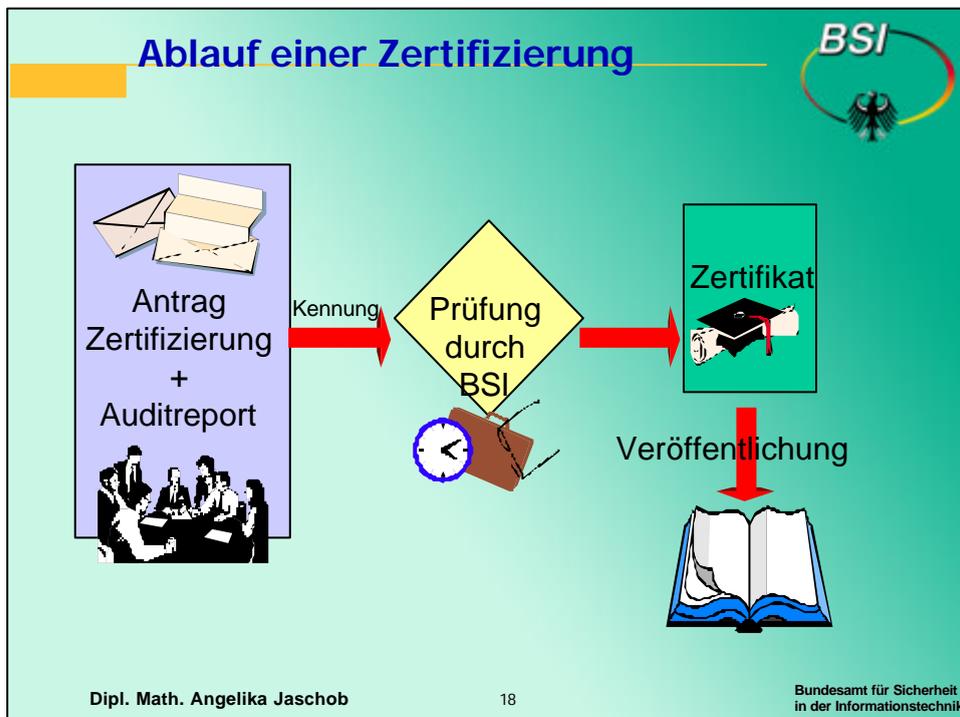
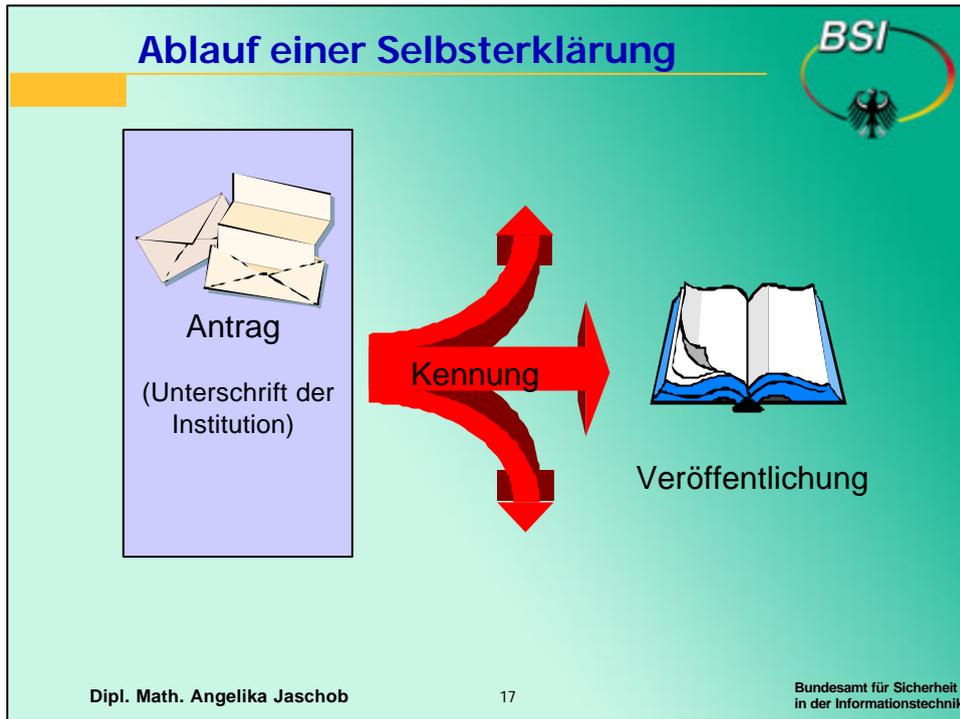


Die Selbsterklärung mit Testat muss mindestens folgende Informationen umfassen:

- Antragsverfahren (Selbsterklärung mit Testat)
- Die Auditierung wird von einem externen, vom BSI **lizenzieren Auditor** durchgeführt.
- Das Testat ist ein zusätzlichen Absatz des Antrages in dem der Auditors die ordnungsgemäße Durchführung eines IT-Grundschutz-Audits bestätigt.



Dipl. Math. Angelika Jaschob
16
Bundesamt für Sicherheit in der Informationstechnik



**Ablauf eines
Zertifizierungsverfahrens**



Inhalt eines Zertifikat

Dipl. Math. Angelika Jaschob 19 Bundesamt für Sicherheit in der Informationstechnik

**Ablauf eines
Zertifizierungsverfahrens**



Inhalt eines Anhangs zum Zertifikat

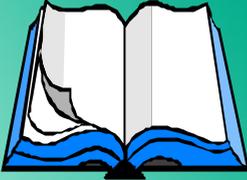
- Angaben zu den Grundlagen des Zertifizierungsverfahrens und zum Verlauf der Auditierung
- Name und Adresse des Auditors
- ggf. Name und Adresse des Unternehmens, für den der Auditor tätig ist
- Beschreibung des Untersuchungsgegenstandes

Dipl. Math. Angelika Jaschob 20 Bundesamt für Sicherheit in der Informationstechnik

IT-Grundschutz-Zertifizierung

Veröffentlichung

- Internet unter www.bsi.bund.de
- KES
- diverse Publikationen
- usw.



Dipl. Math. Angelika Jaschob 21 Bundesamt für Sicherheit in der Informationstechnik

Gültigkeitsdauer und Kosten einer Selbsterklärung

- Die Gültigkeit von einer Selbsterklärung ist auf **2 Jahre** beschränkt.
- Eine Verlängerung der Gültigkeit einer Selbsterklärung ist **nicht** möglich. Es kann jedoch ein neuer Antrag für denselben IT-Verbund für eine höhere Sicherheitsstufe gestellt werden.
- Für jegliche Selbsterklärung wird vom BSI eine Pauschalgebühr von **20 Euro** erhoben.



Dipl. Math. Angelika Jaschob 22 Bundesamt für Sicherheit in der Informationstechnik

Gültigkeitsdauer und Kosten eines Zertifikats



- Die Gültigkeit eines IT-Grundschutz-Zertifikats ist auf **2 Jahre** beschränkt.
- Nach Ablauf der Gültigkeit eines IT-Grundschutz-Zertifikats muss ein Re-Zertifizierungsantrag gestellt werden.
- Für eine Zertifizierungsverfahren wird vom BSI eine Pauschalgebühr von **2500 Euro** erhoben.



Dipl. Math. Angelika Jaschob 23 Bundesamt für Sicherheit in der Informationstechnik

IT-Grundschutz-Zertifizierung Status Quo



Selbsterklärungen

- 6 Selbsterklärungen Einstiegsstufe
- 1 Selbsterklärung Aufbaustufe

Zertifikate

- zwei Zertifikate vergeben
- mehrere Ankündigungen



Dipl. Math. Angelika Jaschob 24 Bundesamt für Sicherheit in der Informationstechnik

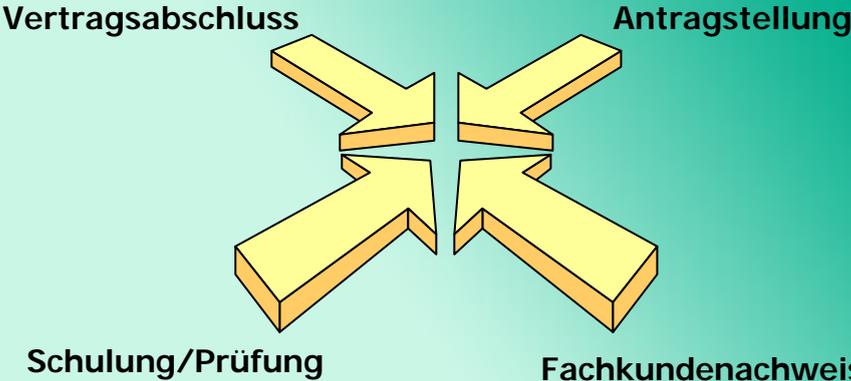


Das Lizenzierungsschema für IT-Grundschutz-Auditoren

Dipl. Math. Angelika Jaschob 25 Bundesamt für Sicherheit
in der Informationstechnik



Lizenzierungsschema



Vertragsabschluss Antragstellung

Schulung/Prüfung Fachkundenachweis

Dipl. Math. Angelika Jaschob 26 Bundesamt für Sicherheit
in der Informationstechnik

Lizenzierungsschema

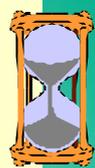
Die Lizenz wird erteilt, wenn der Antragsteller folgende Bedingungen erfüllt:

- Der Fachkundenachweis:
 - Nachweis von 2 Jahren IT-Sicherheitserfahrung
 - Nachweis von 3 IT-Grundschutzprojekten
- Die 1,5 tägige Schulungsveranstaltung wurde absolviert.
- Die Prüfung wurde bestanden.
- Der Lizenzierungsvertrag zwischen BSI und Auditor ist unterzeichnet. (Personenlizenz)
- Die Kosten für die Lizenzierung sind entrichtet.

Dipl. Math. Angelika Jaschob 27 Bundesamt für Sicherheit in der Informationstechnik

Lizenzierungsschema

Kosten und Gültigkeitsdauer eine Auditoren-Lizenz:

- Für das Lizenzierungsverfahren wird vom BSI eine Pauschalgebühr von **1800 Euro** erhoben.
- Eine Lizenz als IT-Grundschutz-Auditor ist **5 Jahre** gültig. 
- Eine Verlängerung der Gültigkeit ist durch eine neue Antragstellung möglich.

Dipl. Math. Angelika Jaschob 28 Bundesamt für Sicherheit in der Informationstechnik

Lizenzierungsschema



Unabhängigkeit des Auditors:

- Auditor darf nicht der zu prüfenden Institution angehören oder in den letzten 2 Jahren dort tätig gewesen sein.
- Die Verantwortung für den Audit-Prozess verbleibt auf jeden Fall beim lizenzierten Auditor.

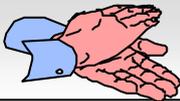
Dipl. Math. Angelika Jaschob 29 Bundesamt für Sicherheit in der Informationstechnik

Lizenzierungsschema



Aufrechterhaltung der Lizenz

Erfahrungsaustausch

Lizenzverlängerung

Lizenzentzug

Dipl. Math. Angelika Jaschob 30 Bundesamt für Sicherheit in der Informationstechnik

IT-Grundschutz-Lizenzierung Status Quo



- Lizenzierung von **73 IT-Grundschutz-Auditoren**
- Veröffentlichung aller Auditoren im Internet
- 16 Antragsteller erbringen den Fachkompetenznachweis (nächste Schulung am 2+3.4.03)
- weitere Anträge liegen vor
- nächste Schulung ist bereits in der Vorbereitung

Dipl. Math. Angelika Jaschob 31 Bundesamt für Sicherheit
in der Informationstechnik



Haben Sie noch Fragen?



Dipl. Math. Angelika Jaschob 32 Bundesamt für Sicherheit
in der Informationstechnik