# Mindestanforderungen der Rechnungshöfe des Bundes und der Länder zum Einsatz der Informationstechnik

**– Leitlinien und gemeinsame Maßstäbe für IT-Prüfungen –**

# (IT-Mindestanforderungen 2011)

**Fassung Berlin**

**Stand: November 2011**

## Inhaltsverzeichnis



**Anlage:**

**Fundstellen zu Normen, Standards und Empfehlungen**

# 1 Zweck der IT-Mindestanforderungen

Die IT-Mindestanforderungen bestimmen die beim Einsatz der Informationstechnik (IT) zu beachtenden Handlungsfelder. Insbesondere beschreiben sie die grundlegenden Voraussetzungen für einen wirtschaftlichen, ordnungsgemäßen und sicheren Einsatz der IT. Sie bilden eine wichtige gemeinsame Grundlage für Prüfungen der Rechnungshöfe des Bundes und der Länder. Mit ihnen sollen gemeinsame und transparente Prüfungsmaßstäbe geschaffen werden.

Für eine Vielzahl von Anforderungen existieren bereits Normen, Standards und Empfehlungen, die als Prüfungskriterien herangezogen werden können. Näheres zu den entsprechenden Stichworten, die im Text *kursiv* hervorgehoben sind, kann der Anlage entnommen werden.

# 2 Grundlegende Anforderungen

## 2.1 Wirtschaftlichkeit

Nach dem im Haushaltsrecht des Bundes und der Länder verankerten Grundsatz der Wirtschaftlichkeit und Sparsamkeit ist jede Maßnahme auf ihre Wirtschaftlichkeit hin zu überprüfen (§ 7 BHO/LHO). Die Wirtschaftlichkeit des IT-Einsatzes ist deshalb durch *Wirtschaftlichkeitsuntersuchungen* festzustellen. Die Kosten (i. d. R. personeller Zeitaufwand) für die Wirtschaftlichkeitsuntersuchung haben in einem angemessenen Verhältnis zum Umfang der zu betrachtenden Maßnahme zu stehen. Wirtschaftlichkeitsuntersuchungen sind zu den folgenden Zeitpunkten durchzuführen:

| Zeitpunkt | Zweck |
|---|---|
| Vor Maßnahmenbeginn (Ex-ante) | Nachweis der Wirtschaftlichkeit der Gesamtmaßnahme |
| Nach Entscheidung über Maßnahmenbeginn, aber vor Einzelmaßnahmen (Ex-ante) | Nachweis der Wirtschaftlichkeit jeder Einzelmaßnahme |
| Nach Durchführung von Einzelmaßnahmen (Ex-post) | Kontrolle der Wirtschaftlichkeit jeder Einzelmaßnahme (begleitend) |
| Nach Abschluss der Maßnahme (Ex-post) | Kontrolle der Wirtschaftlichkeit der Gesamtmaßnahme (begleitend und abschließend) |

Bei einer Wirtschaftlichkeitsuntersuchung ist insbesondere darauf zu achten, dass

- vorab die Ausgangslage und der Handlungsbedarf analysiert wurden,
- die mit der (Einzel-)Maßnahme verbundenen Risiken berücksichtigt werden,
- die Ziele der zu untersuchenden Varianten vorher eindeutig definiert sind,
- die geeignete Methode zum Tragen kommt (z. B. Kapitalwertmethode, Kostenvergleich),
- sämtliche Kosten im Betrachtungszeitraum angesetzt werden,
- die monetäre Betrachtung im Vordergrund zu stehen hat und ein positives Ergebnis auch haushaltswirksam zumindest mittelfristig erreicht wird,
- nur die Nutzenwirkungen einbezogen werden, die durch die zu betrachtende *IT-Maßnahme* ausgelöst werden und
- Personaleinsparungen nur in dem Ausmaß und ab dem Zeitpunkt angesetzt werden, in dem sie aufgrund der IT-Maßnahme eintreten.

Die zuständige Stelle hat nach der Durchführung einer *IT-Maßnahme* zu prüfen, inwieweit die der Planung und der Wirtschaftlichkeitsuntersuchung zugrunde liegenden Ziele erreicht worden sind (Zielerreichungs-, Wirkungs- und Wirtschaftlichkeitskontrolle).

## 2.2 Ordnungsmäßigkeit

Der ordnungsgemäße Einsatz der IT ist durch die Einhaltung der geltenden Normen zu gewährleisten (*Regelüberwachung* / IT-*Compliance*).

Die Abgrenzung und Zuweisung der Funktionen und Verantwortungsbereiche ist im Hinblick auf die Trennung von Fach- und Betriebsverantwortung im Einzelnen schriftlich festzulegen. Soweit eine Trennung von Funktionen und damit von Verantwortungsbereichen ausnahmsweise nicht zweckmäßig ist, sind geeignete Sicherungs- und Kontrollmaßnahmen vorzusehen. Auch in diesen Fällen muss die Zuordnung der Funktionen im Einzelnen geregelt sein. Es ist ein *internes Kontrollsystem* zu etablieren. Dabei sind Ausführungsfunktionen von Kontrollfunktionen zu trennen.

Beim Umgang mit personenbezogenen Daten ist auf den *Datenschutz*, bei der Bereitstellung von Webangeboten auf *Barrierefreiheit* zu achten. *Ergonomie*vorschriften sind zu berücksichtigen.

Die Planung und der Einsatz der IT sind zu dokumentieren. Die IT-Dokumentation muss vollständig, aktuell und verständlich sein sowie alle Änderungen und Entscheidungen nachweisen. Soweit *elektronische Dokumente* verwendet werden, ist deren *Revisionsfähigkeit* zu gewährleisten.

## 2.3 Sicherheit

Den Risiken beim Einsatz der IT ist durch infrastrukturelle, organisatorische, personelle und technische Maßnahmen zur *Sicherheit* der IT Rechnung zu tragen. Dies betrifft insbesondere Risiken, die zu

- unberechtigter Kenntnisnahme (Verlust der Vertraulichkeit),
- unberechtigter Veränderung oder Verfälschung (Verlust der Integrität) und
- Beeinträchtigung oder Verlust der Verfügbarkeit (Verlust der Funktionalität)

führen können.

Ein *Informationssicherheitsmanagement* ist einzurichten. Aus Schutzbedarfs-/ *Risikoanalysen* sind notwendige Maßnahmen zur Informationssicherheit abzuleiten. Dabei sind die *Standards* und die *Grundschutz-Kataloge* des *Bundesamts für Sicherheit in der Informationstechnik* (BSI) anzuwenden. Bei hohem bzw. sehr

hohem Schutzbedarf sollten zusätzlich oder ersatzweise höherwertige Maßnahmen ergriffen werden, die ebenfalls einschlägigen Normen zur IT-*Sicherheit* genügen.

Die Wirksamkeit von Sicherheitsmaßnahmen und -prozessen sollte durch angemessene *Audit*-Verfahren nachgewiesen werden.

## 3 Strategische und organisatorische Anforderungen

Die strategischen und organisatorischen Anforderungen für den Einsatz von IT leiten sich aus dem Gebot eines ordnungsgemäßen und wirtschaftlichen Verwaltungshandelns ab. Die *IT-Strategie* und deren Umsetzung soll zu einer Ausrichtung der IT an den Zielen der Organisation führen und auf diese Weise den Wertbeitrag des IT-Einsatzes bei der Erfüllung der Aufgaben gewährleisten. Dies sollte turnusmäßig überprüft und ggf. angepasst werden (*IT-Governance*). Ein strategischer Handlungsrahmen für die Integration der IT in die Aufbau- und Ablauforganisation der Verwaltung ergibt sich auch aus *gesellschaftlichen und politischen Zielsetzungen* sowie administrativen Aufgabenstellungen. Die Beschlüsse und Empfehlungen des *IT-Planungsrates* sind bei der Erarbeitung der IT-Strategie zu beachten.

Ressortübergreifend soll insbesondere geregelt und koordiniert werden:

- die Entwicklung und der Einsatz gemeinsamer IT-Verfahren,
- die Übernahme vorhandener IT-Verfahren anderer Länder oder des Bundes,
- landes- bzw. bundesweite IT-Initiativen sowie Programme und
- die Einrichtung von IT-Gremien.

Die ressortübergreifende IT-Koordinierung, die Planung und Kontrolle strategischer bzw. querschnittlicher Aufgaben und Infrastrukturen soll bei einer zentralen Stelle gebündelt werden. Ein Gremium der IT-Zuständigen soll beratend tätig werden.

Die zentrale Stelle soll insbesondere zu folgenden Themen ressortübergreifende Richtlinien erarbeiten:

- Führungs- und Steuerungsprinzipien,

- grundsätzliche Zuständigkeiten einer IT-Organisation,
- Mindestanforderungen an IT-*Qualität*,
- Sicherheitsstandards sowie Grundprinzipien des Informationssicherheitsmanagements,
- Standards für die übergreifende IT-Ressourcenplanung,
- *IT-Controlling* einschließlich *Risikomanagement*,
- Standards für IT-Systemarchitekturen, IT-Systemkomponenten, den Datenaustausch und Benutzerschnittstellen sowie
- Standards für das *IT-Projektmanagement* und den *IT-Betrieb*.

Die Bedarfsdeckung sollte organisationsübergreifend gebündelt werden, ohne den Wettbewerb nachhaltig einzuschränken. IT-Rahmenverträge sind bekannt zu geben. Für die auf IT-Dienstleistungszentren übertragenen Aufgaben sind verbindliche Vereinbarungen zu treffen.

Innerhalb der Ressorts ist die Gesamtstrategie unter Berücksichtigung der fachspezifischen Aufgabenstellungen und des Bedarfs im Rahmen einer Gesamtplanung zu konkretisieren. Diese soll bestimmte, messbare, erreichbare, realistische und terminierte Qualitäts- und Prozessziele für den IT-Einsatz enthalten. Ziele und Strategie müssen den betroffenen Organisationseinheiten auf geeignete Weise kommuniziert werden.

Vorgaben zur Festlegung geeigneter *Kennzahlen* sowie zur Identifizierung der Kosten der IT sind zu treffen, um den IT-Einsatz zu optimieren und die Effizienz und Effektivität des Verwaltungshandelns sicherzustellen.

# 4 Anforderungen an IT-Prozesse

## 4.1 Operative Planung und IT-Organisation

Auf Grundlage der strategischen *IT-Planung* muss die operative *IT-Planung* der Ressorts und der weiteren Verwaltung erstellt werden. Dabei sind die einzelnen Aufgaben auf die Struktureinheiten zu verteilen (*IT-Organisation*).

Die operative *IT-Planung* sollte ziel- und zukunftsorientiert, angemessen detailliert, aktuell und lückenlos sein. Die in der *IT-Planung* festgeschriebenen Ziele und Aussagen zur IT-Ausrichtung sind den Beteiligten gegenüber zu kommunizieren.

Die *IT-Planung* ist kontinuierlich zu überprüfen sowie fortzuschreiben und soll je nach Planungs- und Entwicklungsstand Folgendes ausweisen:

- Zielsetzung des behördlichen IT-Einsatzes,
- Aussagen zur IT-Organisation,
- Bedarfsanalyse, generelles Anforderungsmanagement,
- Festlegungen zur *IT-Architektur* der Verwaltung mit Aussagen zu IT-Verfahren, IT-Diensten inkl. *Verfügbarkeit*sanforderungen,
- Einführungsstrategien,
- Konzeption für Schulung und Anwenderbetreuung,
- IT-Sicherheitsdokumentation als Teil eines Managementsystems für Informationssicherheit,
- Aussagen zum Bedarf an Ressourcen: Haushaltsmittel (konsumtiv und investiv), Personal, Technik/Systeme, Infrastruktur,
- Regelungen zur Bestandsführung von Hardware, Software, Infrastrukturen (Konfigurationsmanagement),
- Festlegungen zum Risikomanagement in Projekten und Betrieb,
- Aussagen zur Organisation von Qualitätssicherung und -management und
- Festlegungen zur Organisation des IT-Controllings.

Die Organisation der IT soll gewährleisten, dass die *IT-Prozesse* sowohl serviceorientiert als auch wirtschaftlich die Ziele der Verwaltung unterstützen. Hierzu sind bzgl. der Kernprozesse und eingesetzter IT-Technologien ausreichende Kompetenzen beim IT-Personal aufzubauen und zu pflegen. Auch beim Einsatz Externer muss durch qualifiziertes eigenes IT-Personal die Verlässlichkeit und Flexibilität der IT sichergestellt werden.

## 4.2 IT-Maßnahmen

### 4.2.1 Planung und Durchführung von IT-Maßnahmen

Zur Planung gehören die Festlegung der Ziele der *IT-Maßnahme*[1], die Entscheidung über eine Projektorganisation, eine Anforderungsanalyse, ein Pflichtenheft, eine an Meilensteinen orientierte Zeitplanung und eine *Wirtschaftlichkeitsuntersuchung*. Die erwarteten Kosten und die Maßnahmendauer sind zu dokumentieren. Die Planungsdokumente sind regelmäßig mit dem aktuellen Projektstand abzugleichen und ggf. zu aktualisieren (rollierende Planung).

Vor der Einführung neuer Verfahren sind eine Analyse und ggf. Optimierungen der Geschäftsprozesse durchzuführen. Daher sind die für Organisationsfragen zuständigen Stellen rechtzeitig einzubinden. Bei behördenübergreifenden Maßnahmen sind Beteiligung und Verantwortung im Einzelnen zu regeln.

Bei der Planung des Einsatzes von IT-Verfahren sind durch eine *Wirtschaftlichkeitsuntersuchung* folgende Alternativen zu prüfen:

- der Einsatz von Standard-Software – ggf. nach einer Anpassung,
- die Übernahme vorhandener Software,
- die Neuentwicklung durch eigene Mitarbeiter und
- die Neuentwicklung durch Externe.

Bei IT-Projekten ist ein *Projektmanagement*-System zu nutzen, das alle relevanten Teildisziplinen, insbesondere das Termin-, Kosten- und *Risikomanagement*, angemessen berücksichtigt.

### 4.2.2 Beschaffung, Beauftragung Externer

Die IT-*Beschaffung* sollte die bedarfs- und nutzergerechte Versorgung der Dienststellen mit den von ihnen zur Erfüllung ihrer Aufgaben benötigten IT-Komponenten und IT-Dienstleistungen gewährleisten. Bei der *Beschaffung* ist

[1] IT-Maßnahmen (IT-Vorhaben, IT-Projekte usw.) umfassen die Konzeption, die Entwicklung, die Beschaffung, die Einführung oder wesentliche Änderungen im IT-Betrieb, von IT-Verfahren, IT-Infrastruktur und IT-Diensten.

unter dem Gesichtspunkt der Wirtschaftlichkeit die günstigste Konfiguration und Beschaffungsart (Kauf, Miete, Leasing) auszuwählen. Die technische bzw. wirtschaftliche Abhängigkeit von einzelnen Herstellern ist zu vermeiden.

Durch die zentrale *Ausschreibung* von Rahmenverträgen für Hard- und Software sowie für Standard-IT-Dienstleistungen sollen Einsparpotenziale realisiert werden. Ebenso soll die IT-Standardisierung sichergestellt und vorangetrieben werden. IT-Rahmenverträge sind zu nutzen.

Bei der *Beauftragung und dem Einsatz Externer* hat die Verwaltung insbesondere folgende Aufgaben wahrzunehmen:

- Problembeschreibung und Festlegung von Zielen, die mit dem Einsatz Externer erreicht werden sollen,
- Prüfung der Zulässigkeit und der Erforderlichkeit der Beauftragung Externer,
- Wirtschaftlichkeitsuntersuchungen zur Bewertung aller Lösungsalternativen,
- Erstellung einer eindeutigen und umfassenden Leistungsbeschreibung,
- Ausschreibung und Vergabe,
- Vertragsgestaltung,
- Risikomanagement lieferantenbezogener Risiken,
- Kontrolle und Steuerung der Leistungserbringung durch Überwachung und Messung,
- Abnahme der Ergebnisse einschließlich Forderungsmanagement bei vertragswidrigem Verhalten oder Schlechtleistung,
- Gewährleistung des Know-how-Transfers,
- Vermeidung der Abhängigkeit von Externen.

Die Verwaltung soll durch ein wirksames Management sicherstellen, dass die von Externen erbrachten Leistungen den Anforderungen des Auftraggebers entsprechen und dabei Kosten, Nutzen und Risiken transparent bleiben. Auch Sicherheitsbelange, z. B. die Zuverlässigkeit des Externen, müssen angemessen berücksichtigt werden.

### 4.2.3 Entwicklung und Pflege von IT-Verfahren

Die *Softwareentwicklung* ist – auch zur Sicherung der Pflege und Weiterentwicklung – nach geeigneten Methoden des Software-Engineerings durchzuführen. Festgelegte Vorgehensweisen, Qualitätsvorgaben und Arbeitstechniken sind einzuhalten, regelmäßig zu überprüfen und anzupassen.

Die Dokumentation muss die Pflege bzw. Wartung und einen ordnungsgemäßen Betrieb unterstützen sowie eine effektive und effiziente Verfahrensnutzung durch die Anwender ermöglichen.

Werden Externe mit der Entwicklung von Software beauftragt, soll der Zugriff auf den Quellcode – ggf. durch Hinterlegung – sichergestellt werden.

### 4.2.4 Test und Freigabe

IT-Verfahren, bei komplexen Verfahren auch fertig gestellte Teile, sind vor ihrer Freigabe für den Betrieb in allen Funktionen zu testen. Einzelheiten des *Test- und Freigabeverfahren*s sind zu regeln. Die *Schnittstellen* zu anderen Verfahren und die spätere organisatorische Einbindung in den Betrieb sind besonders zu beachten.

Tests müssen aufgrund von Testfällen mit im Voraus festgelegten Eingaben und erwarteten Ausgaben durchgeführt werden. Die fachlich zuständigen Stellen haben hierfür Testfälle zu erstellen. Die Ergebnisse des abschließenden Tests sind unter gebotener Beteiligung des IT-Bereichs von den am Vorhaben beteiligten Fachbereichen zu kontrollieren, zu bewerten und abzunehmen. Der Abschlusstest ist revisionsfähig zu dokumentieren.

Es soll eine Stelle bestimmt sein, die auf der Grundlage der Abnahmeerklärung zum Abschlusstest das Verfahren freigibt, eine Freigabebescheinigung erstellt und damit die Gesamtverantwortung für die Ordnungsmäßigkeit und die *Sicherheit* des Verfahrens übernimmt.

Ein Verfahren darf grundsätzlich nur freigegeben werden, wenn dessen Dokumentationsunterlagen vollständig vorliegen. Auch nicht selbst entwickelte Verfahren sind vor ihrem Einsatz entsprechend zu testen und förmlich freizugeben.

Soweit ein Verfahren von mehreren öffentlichen Stellen eingesetzt werden soll, können eigene Tests mit Testergebnissen anderer öffentlicher Stellen kombiniert oder ergänzt werden. Die kombinierten oder ergänzten Tests sind zu dokumentieren. Die Notwendigkeit der Freigabe bleibt hiervon unberührt.

Lässt sich ein vorläufiger Verfahrenseinsatz nach einem ausreichenden und revisionsfähig dokumentierten Test aus unabweisbaren Gründen nicht umgehen, ist die Freigabe unverzüglich nachzuholen.

### 4.2.5 Einführung, Anwenderschulung

Bei der Einführung eines IT-Verfahrens ist insbesondere rechtzeitig zu gewährleisten, dass

- die erforderliche Hard- und Softwareumgebung eingerichtet ist,
- die Datenbestände eines abzulösenden Verfahrens übernommen,
- die Benutzer bedarfsgerecht und zeitnah geschult wurden und
- alle notwendigen rechtlichen Voraussetzungen vorliegen.

Für eine fortlaufende Beratung und *Schulung* der Benutzer – auch nach der Verfahrenseinführung – muss Vorsorge getroffen werden. Eine im Umfang angemessene Anwenderdokumentation des Verfahrens ist bereitzustellen.

Bei der Einführung neuer Verfahren sind die Aspekte des *organisationalen Wandels* und des *Akzeptanzmanagements* zu beachten.

## 4.3 IT-Betrieb

Unter Beachtung der grundsätzlichen Anforderungen zur Wirtschaftlichkeit, Ordnungsmäßigkeit und *Sicherheit* ist der *IT-Betrieb* ergebnis- und auftraggeberorientiert auszurichten. Standardisierte Lösungen sind anzustreben.

Die Anforderungen an den *IT-Betrieb* und dessen Leistungen sind zu fixieren. Dazu gehören insbesondere Regelungen zur Nutzung von behördenübergreifenden Standards und zu eventuellen Leistungsverrechnungen.

Der *IT-Betrieb* ist ständig mit geeigneten und angemessenen Methoden zu überwachen und zu dokumentieren. Dies sollte mit einem *IT-Service-Management* (ITSM) gewährleistet werden, welches hinsichtlich des *IT-Betriebs* insbesondere folgende Teildisziplinen angemessen berücksichtigt:

- Änderungsmanagement,
- Datenmanagement,
- Kapazitätsmanagement,
- Konfigurationsmanagement,
- Kontinuitätsmanagement,
- Sicherheitsmanagement,
- Störungsmanagement und
- Verfügbarkeitsmanagement.

## 4.4 Kontrolle und Steuerung

Zur Kontrolle und Steuerung der Zielerreichung ist ein angemessenes *IT-Controlling* einzusetzen. Dazu sind insbesondere folgende Funktionen und Aufgaben des Controllings rechtzeitig zu planen und festzulegen:

- Zieldefinitionen: Messbarkeit durch Leistungsindikatoren und *Kennzahlen*, Software-*Metriken* zur Qualitätssicherung, Identifikation von Kosten und Nutzen.
- Organisation: Zuordnung zur strategischen und operativen Ebene, zentrale und/oder dezentrale Controlling-Einheiten, Kompetenzen und Zuständigkeiten.
- Instrumente: Aufbau eines Zielvereinbarungssystems, Einsatz Controlling-Software, ggf. IT-Balanced-Scorecard.
- Information: Installierung eines zielorientierten Berichtswesens, Kommunikation der *Kennzahlen*ergebnisse.
- Steuerung: Bewertung *kritischer Erfolgsfaktoren*, Zuordnung von *Früh- und Spätindikatoren*, Maßnahmen aufgrund von Abweichungsanalysen.

Die Ergebnisse interner und externer *Audits* können ergänzend herangezogen werden.

Für eine Vielzahl von Anforderungen existieren bereits Normen, Standards und Empfehlungen. Sie sind für den jeweiligen Adressaten von unterschiedlicher Verbindlichkeit.

*Anlage: Fundstellen zu Normen, Standards und Empfehlungen*

# IT-Mindestanforderungen

## Anlage:
## Fundstellen zu Normen, Standards und Empfehlungen

## Stand: November 2011

Für eine Vielzahl von Anforderungen existieren bereits Normen, Standards und Empfehlungen. Sie sind für den jeweiligen Adressaten von unterschiedlicher Verbindlichkeit.

| **Stichwort** | **zu Tn.** | **Norm, Standard, Empfehlung** | **Quelle/Bemerkung** |
|---|---|---|---|
| Akzeptanzmanagement | 4.2 | | Sicherung der Nutzerakzeptanz im Rahmen von IT-Vorhaben, siehe auch Change Management http://www.olev.de/ak.htm#Akzeptanzmanagement |
| Audits zu Prozessen | 4.4 | ISO 9000:2005 | http://www.iso.org |
| | | Common Assessment Framework (CAF) | http://www.caf-netzwerk.de |
| Audits zur IT-Sicherheit | 2.3 | Zertifizierung nach ISO 27001 auf Basis von IT-Grundschutz des BSI | http://www.iso.org<br>http://www.bsi.bund.de |
| Ausschreibung | 4.2 | siehe Beschaffung | |
| Barrierefreiheit | 2.2 | Gesetz zur Gleichstellung behinderter Menschen (BGG) i. V. m. Verordnung zur Schaffung barrierefreier Informationstechnik nach dem Behindertengleichstellungsgesetz (Barrierefreie Informationstechnik-Verordnung - BITV) bzw. entsprechende Landesregelungen | BGG vom 27. April 2002 (BGBl. I S. 1467)<br>BITV vom 17. Juli 2002 (BGBl. I S. 2654) |
| Beauftragung und Einsatz Externer | 4.2 | Einsatz externer Berater durch die Bundesverwaltung, BWV-Schriftenreihe, Band 14, Novem- | http://www.bundesrechnungshof.de |

| **Stichwort** | **zu Tn.** | **Norm, Standard, Empfehlung** | **Quelle/Bemerkung** |
|---|---|---|---|
| | | ber 2006 | |
| | | Empfehlungen zur Inanspruch-nahme von externen Unterstüt-zungsleistungen durch Bundes-behörden im IT-Bereich, KBSt-Empfehlung vom 16. Januar 2001 | http://www.cio.bund.de |
| Beschaffungen | 4.2 | Unterlage für die Ausschreibung und Bewertung von IT-Leistungen – UfAB V | BMI http://www.cio.bund.de |
| | | Ergänzende Vertragsbedingun-gen für die Beschaffung von In-formationstechnik (EVB-IT), Besondere Vertragsbedingungen für die Beschaffung von DV-Anlagen und Geräten (BVB) | BMI http://www.cio.bund.de |
| | | Leitfäden und Empfehlungen zur IT-Beschaffung | http://www.itk-beschaffung.de |
| | | Umfassende Liste zu Normen und Rechtsgrundlagen beim Beschaf-fungsamt des BMI | http://www.bescha.bund.de (→ Rechtsgrundlagen → Normen u.Rechtsvorschr.) |
| Bundesamt für Sicherheit in der Informations-technik (BSI) | 2.3 | siehe Sicherheit | http://www.bsi.bund.de |

| **Stichwort** | **zu Tn.** | **Norm, Standard, Empfehlung** | **Quelle/Bemerkung** |
|---|---|---|---|
| COBIT | | Control Objectives for Information and<br>Related Technology | COBIT (Control Objectives for Information and Related Technology) - international anerkanntes Framework zur IT-Governance, gliedert die Aufgaben der IT in Prozesse und Control Objectives (Steuerungsvorgaben).<br>http://www.isaca.org , http://www.isaca.de |
| Compliance | 2.2 | siehe Regelüberwachung | |
| Datenschutz | 2.2 | Bundesdatenschutzgesetz (BDSG)<br>bzw. entsprechende Ländergesetze<br>IT-Grundschutz Datenschutz (Baustein 1.5 der IT-Grundschutz-Kataloge) | http://www.bfdi.bund.de<br><br>https://www.bsi.bund.de/ |
| Elektronische Dokumente | 2.2 | DOMEA - Dokumentenmanagement und elektronische Archivierung im IT-gestützten Geschäftsgang, Vers. 2.1 | Schriftenreihe der KBSt, Band 61<br>http://www.cio.bund.de |
| Ergonomie | 2.2 | Bildschirmarbeitsverordnung (BildscharbV) | BildscharbV vom 4. Dezember 1996 (BGBl. I S. 1841) |
| | | DIN EN ISO 9241 “Ergonomische Anforderungen für Bürotätigkeiten mit Bildschirmgeräten” | http://www.iso.org<br>http://www.din.de |

| **Stichwort** | **zu Tn.** | **Norm, Standard, Empfehlung** | **Quelle/Bemerkung** |
|---|---|---|---|
| Früh- u. Spätindikatoren | 4.4 | siehe Kennzahlen und Metriken | |
| Gesellschaftliche Ziele | 3 | E-Government-Aktionsplan im Rahmen der i2010-Initiative: Beschleunigte Einführung elektronischer Behördendienste in Europa zum Nutzen aller | Kommission der Europäischen Gemeinschaften, Brüssel, 25.04.2006 |
| Grundschutzkataloge | 2.3 | siehe Sicherheit | |
| Grundschutz-Standards | 2.3 | siehe Sicherheit | |
| Informationssicherheitsmanagement | 2.3 | siehe Sicherheit | |
| Internes Kontrollsystem | 2.2 | COBIT | http://www.isaca.org<br>http://www.isaca.de |
| | | IDW PS 330<br>IDW RS FAIT1 und IDW RS FAIT3 | http://www.idw.de |
| | | BMF Schreiben zu GoBS vom 7.11.1995 | http://www.bmf.bund.de |
| | | Empfehlungen für Interne Revisionen in der Bundesverwaltung | BMI, 10.04.2008<br>http://www.bmi.bund.de |
| IT-Governance | 3 | COBIT | http://www.isaca.org<br>http://www.isaca.de |

| **Stichwort** | **zu Tn.** | **Norm, Standard, Empfehlung** | **Quelle/Bemerkung** |
|---|---|---|---|
| | | Dokumente des ITGI zu IT-Governance, hier insb. ITGI Val IT- Framework | http://www.itgi.org |
| | | ISO 38500 | http://www.iso.org |
| IT-Planungsrat | 3 | Beschlüsse und Empfehlungen | http://www.it-planungsrat.de |
| IT-Architektur | 4.1 | Standards und Architekturen für E-Government-Anwendungen (SAGA) ; ggf. landesspezifische Regelungen und Vorgaben | http://www.cio.bund.de |
| IT-Betrieb/ITSM | 3<br>4.3 | ISO/IEC 20000:2005 bzw.<br>IT Infrastructure Library (ITIL) | IT-Service-Management (ITSM) bezeichnet die Gesamtheit von Maßnahmen und Methoden, die nötig sind, um die bestmögliche Unterstützung von Geschäftsprozessen durch die IT-Organisation zu erreichen. Die Mindestanforderungen an die Prozesse wurden in der ISO/IEC 20000:2005 spezifiziert.<br>http://www.iso.org/<br>IT Infrastructure Library (ITIL) des OGC ist eine Sammlung von Empfehlungen, die eine mögliche Umsetzung eines IT-Service-Managements (ITSM) beschreiben und inzwischen international als De-facto-Standard hierfür gelten.<br>http://www.ogc.gov.uk/guidance_itil.asp<br>http://www.itsmf.de<br>http://www.cio.bund.de |

| **Stichwort** | **zu Tn.** | **Norm, Standard, Empfehlung** | **Quelle/Bemerkung** |
|---|---|---|---|
| | | | http://www.itil-officialsite.com<br>http://www.iso.org |
| | | IT-Methode IT Infrastructure Library (ITIL)<br>Studien zu ITIL | http://www.cio.bund.de/<br>ITIL und Standards für IT-Prozesse – Prozessstandards für die Entwicklung der IT-Service-Organisation gemäß ITIL Best Practices |
| | | BS 25999 Part one and two: Business Continuity Management | Norm des British Standards Institute (Vergleichbar mit dem BSI-Standard 100-4)<br>http://www.thebci.org/standards.htm<br>http://www.bsigroup.com |
| | | DIN EN ISO 9000 ff. | http://www.iso.org<br>http://www.din.de |
| IT-Controlling | 3<br>4.4 | COBIT | http://www.isaca.org<br>http://www.isaca.de |
| | | ITGI Val IT | http://www.itgi.org |
| IT-Maßnahmen | 4.2 | Standards und Architekturen für E-Government (SAGA) und landesspezifische Pendants | http://www.cio.bund.de |
| IT-Organisation | 4.1 | Handbuch für Organisationsuntersuchungen und Personalbedarfsermittlung, Stand 31. Juli 2007 | http://www.orghandbuch.de<br>http://www.bmi.bund.de |

| **Stichwort** | **zu Tn.** | **Norm, Standard, Empfehlung** | **Quelle/Bemerkung** |
|---|---|---|---|
| IT-Planung | 4.1 | COBIT<br>ITGI Val IT<br>ITIL | http://www.isaca.org<br>German Chapter: http://www.isaca.de<br>http://www.itgi.org/<br>http://www.ogc.gov.uk/guidance_itil.asp<br>http://www.itsmf.de<br>http://www.cio.bund.de |
| IT-Prozesse | 4 | Beschlüsse und Empfehlungen des IT-Planungsrates | http://www.it-planungsrat.de/DE/Home/home_node.html |
| | | Dokumente zu IT-Methoden und IT-Steuerung | http://www.cio.bund.de |
| | | COBIT | http://www.isaca.org |
| | | ITIL | http://www.ogc.gov.uk/guidance_itil.asp |
| | | Booklet „Informatikprozesse der Bundesverwaltung“ „Prozesslandkarte der Informatikprozesse in der Bundesverwaltung“ des Eidgen. Finanzdepartements | http://www.nove-it.admin.ch/dokumente/prozesse/isb-pbook_web.pdf<br>http://www.isb.admin.ch |
| IT-Strategie | 3 | Organizational Project Management Maturity Model (OPM3) | Systematisches Management von Projekten, Programmen und Portfolios, um strategische Ziele einer Organisation zu erreichen, Herausgeber: PMI<br>http://www.pmi.org<br>http://opm3online.pmi.org |

| **Stichwort** | **zu Tn.** | **Norm, Standard, Empfehlung** | **Quelle/Bemerkung** |
|---|---|---|---|
| | | Umsetzungsplan IT-Steuerung Bund,<br>verabschiedet vom Bundeskabinett am 5. Dezember 2007 | http://www.cio.bund.de |
| Kennzahlen und Metriken | 4.4 | COBIT | http://www.isaca.org |
| | | ITIL | http://www.ogc.gov.uk/guidance_itil.asp |
| | | IT-Balanced Scorecard, kritische Erfolgsfaktoren, Früh- und Spätindikatoren | „Balanced Scorecard in der IT"<br>http://www.kundenkennzahlen.ch/pdf/paper_it_bsc_darius_zumstein.pdf |
| | | Software-Metriken | „Metriken im Qualitätsmanagement" http://www.wi.uni-muenster.de/pi/lehre/ss04/SeminarTesten/Metriken.pdf |

| **Stichwort** | **zu Tn.** | **Norm, Standard, Empfehlung** | **Quelle/Bemerkung** |
|---|---|---|---|
| kritische Erfolgsfaktoren | 4.4 | siehe Kennzahlen und Metriken | |
| Metriken | 4.4 | siehe Kennzahlen und Metriken | |
| Organisationaler Wandel | 4.2 | | Literaturliste unter:<br>http://www.olev.de/c.htm#cm |
| Projektmanagement | 3<br>4.2 | V-Modell XT | http://www.cio.bund.de |
| | | Projects in Controlled Environments – PRINCE 2 | http://www.ogc.gov.uk/prince2/ |
| | | IEEE Std. 1490-2003,<br>ANSI/PMI 99-001-2004 (PMBoK-Guide 2010) | http://www.pmi.org<br>http://www.ansi.org<br>http://www.ieee.org |
| | | ISO 10006 :2003 (QMS für Projekte) | http://www.iso.org |
| | | DIN 69901 | http://www.din.de |
| | | HERMES | http://www.hermes.admin.ch |
| Qualität/ Qualitätsmanagement | 3<br>4.1<br>4.4 | DIN EN ISO 900x<br>DIN 69900-1<br>DIN 69900-2<br>DIN 69901-69905 | http://www.iso.org<br>http://www.din.de |
| | | ISO 10006 (QMS für Projekte) | http://www.iso.org |

| **Stichwort** | **zu Tn.** | **Norm, Standard, Empfehlung** | **Quelle/Bemerkung** |
|---|---|---|---|
| Regelüberwachung | 2.2 | Richtlinie 2006/43/EG des Europäischen Parlaments und des Rates vom 17. Mai 2006 | Amtsblatt Nr. L 157 vom 09/06/2006<br>S. 0087 – 0107 |
| Revisionsfähigkeit | 2.2<br>3<br>4.1 | IDW RS FAIT1 und IDW RS FAIT3<br>IDW PS 880 | http://www.idw.de |
| | | BMF Schreiben zu GoBS vom 7.11.1995 | http://www.bmf.bund.de |
| | | DOMEA-Konzept | http://www.cio.bund.de |
| Risikoanalysen/ Risikomanagement | 2.2<br>3<br>4.1<br>4.4 | IT-Grundschutz-Kataloge des Bundesamtes für Sicherheit in der Informationstechnik (BSI);<br>BSI-Standard 100-3, Risikoanalyse auf der Basis von IT-Grundschutz | http://www.bsi.bund.de |
| | | IDW PS 330<br>IDW RS FAIT1 und IDW RS FAIT3 | http://www.idw.de |

| **Stichwort** | **zu Tn.** | **Norm, Standard, Empfehlung** | **Quelle/Bemerkung** |
|---|---|---|---|
| | | ISO 27005, Informationssicher-heit-Risikomanagement<br>ISO Guide 73:2002, Risiko-Management – Wörterbuch – Leitfaden für die Berücksichtigung von Termini zum Risiko-Management in Normen | http://www.iso.org |
| Schnittstelle | 4.2.4 | XÖV-Standards<br>OSCI-Transport | http://www.xoev.de/<br>http://www.osci.de |
| (Anwender-)Schulung | 4.2.5 | IT-Aus- und Fortbildungsrichtli-nien der KBSt: Rahmenrichtlinien für die Aus- und Fortbildung im Bereich Informationstechnik in der öffentlichen Verwaltung | BMI – Schriftenreihe der KBSt, Bd. 38, 1997<br>http://www.cio.bund.de |
| | | Grundkonzept der IT-Fortbildung | BMI – Schriftenreihe der KBSt, Band 47, Juli 2000<br>http://www.cio.bund.de |

| **Stichwort** | **zu Tn.** | **Norm, Standard, Empfehlung** | **Quelle/Bemerkung** |
|---|---|---|---|
| Sicherheit | 2.3 | BSI-Standard 100-1: Managementsystem für Informationssicherheit (ISMS )<br>BSI-Standard 100-2: IT-Grundschutz-Vorgehensweise<br>BSI-Standard 100-3: Risikoanalyse auf der Basis von IT-Grundschutz<br>BSI-Standard 100-4: Notfallmanagement<br>IT-Grundschutz-Kataloge<br>IT-Grundschutz GSTOOL<br>BSI-Standard zur Internetsicherheit (ISi-Reihe)<br>Technische Richtlinien (BSI-TR)<br>Leitfaden Informationssicherheit – IT Grundschutz kompakt | http://www.bsi.bund.de bzw. als Print-Version über Bundesanzeiger-Verlag |
| | | ISO/IEC 27000 ff. | http://www.iso.org |
| | | Informationssicherheitsrevision: Ein Leitfaden für die IS-Revision auf Basis von IT-Grundschutz, BSI 2010 | http://www.bsi.bund.de |

| **Stichwort** | **zu Tn.** | **Norm, Standard, Empfehlung** | **Quelle/Bemerkung** |
|---|---|---|---|
| Softwareentwicklung | 4.2 | Technologien: Standards und Architekturen für E-Government-Anwendungen (SAGA) | http://www.cio.bund.de |
| | | Modellierung: Unified Modeling Language (UML) (ISO/IEC 19501) | http://www.uml.org<br>http://www.omg.org |
| | | Prozessmodellierung: Business Process Modeling Notation (BPMN) | http://www.omg.org |
| | | V-Modell XT | http://www.cio.bund.de |
| Test- und Freigabeverfahren | 4.2 | IDW PS 880<br>V-Modell XT | http://www.idw.de<br>http://www.cio.bund.de<br>http://www.datenschutzzentrum.de |
| Verfügbarkeit | 4.1 | BSI-Standard 100-4: Notfallmanagement | http://www.bsi.bund.de |
| | | Hochverfügbarkeits-Kompendium des BSI, V. 1.2 | |
| | | Klassifikationen des Uptime-Institutes, Santa Fe | http://www.uptimeinstitute.org |

| **Stichwort** | **zu Tn.** | **Norm, Standard, Empfehlung** | **Quelle/Bemerkung** |
|---|---|---|---|
| Wirtschaftlichkeitsuntersuchung | 2.1 | WiBe (V. 4.1);<br>ggf. landesspezifische Regelungen | Schriftenreihe der KBSt, Band 92<br>http://www.cio.bund.de |