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

– Leitlinien und gemeinsame Maßstäbe für IT-Prüfungen –

(IuK-Mindestanforderungen 2016)

Stand: Juni 2016

Inhaltsverzeichnis

Anlage:

Fundstellen zu Normen, Standards und Empfehlungen

1 Zweck der IuK-Mindestanforderungen

Die IuK-Mindestanforderungen beschreiben die wesentlichen beim Einsatz der Informationstechnik (IT)[1] zu beachtenden Handlungsfelder. Sie benennen die grundlegenden Voraussetzungen für einen wirtschaftlichen, ordnungsgemäßen und sicheren IT-Einsatz. Die IuK-Mindestanforderungen basieren auf den Prüfungserkenntnissen der Rechnungshöfe des Bundes und der Länder. Sie schaffen gemeinsame und transparente Prüfungsmaßstäbe. Vorschriften des Bundes oder der Länder, die weitergehende Anforderungen enthalten, bleiben unberührt.

Für eine Vielzahl von Anforderungen existieren 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 bei jeglichem Verwaltungshandeln die günstigste Relation zwischen dem verfolgten Zweck und den eingesetzten Ressourcen anzustreben. Für alle finanzwirksamen Maßnahmen sind daher angemessene *Wirtschaftlichkeitsuntersuchungen* durchzuführen (§/Artikel 7 BHO/LHO).

Wirtschaftlichkeitsuntersuchungen sind sowohl bei neuen als auch bei der Änderung bereits laufender Gesamt- oder Teilmaßnahmen wie folgt durchzuführen:

[1] Der im Dokument genutzte Begriff Informationstechnik (IT) schließt hier sämtliche Bereiche der Kommunikationstechnik mit ein.

Zeitpunkt	Zweck
während der Planung (vor Maßnahmenbeginn)	Entscheidungsgrundlage für die Realisierung der Maßnahme
während der Realisierung, ggf. mehrfach	begleitende *Erfolgskontrolle* bei zeitlich oder inhaltlich umfangreichen Maßnahmen
nach Abschluss	abschließende *Erfolgskontrolle*

Bei einer *Wirtschaftlichkeitsuntersuchung* ist insbesondere darauf zu achten, dass

- vorab die Ausgangslage und der Handlungsbedarf analysiert werden,
- Ziele, Prioritäten und mögliche Zielkonflikte vorher eindeutig definiert sind,
- die relevanten Lösungsmöglichkeiten betrachtet werden,
- sämtliche im Betrachtungszeitraum entstehende Kosten – auch nicht haushaltswirksame – einbezogen werden,
- nur der Nutzen zu berücksichtigen ist, der von der zu betrachtenden Maßnahme ausgeht,
- die mit der Maßnahme verbundenen Risiken berücksichtigt werden,
- eine geeignete Methode angewendet wird (z. B. Kostenvergleichsrechnung, Kapitalwertmethode, Nutzwertanalyse) und
- die monetäre Betrachtung im Vordergrund steht.

Im Rahmen von *Erfolgskontrollen* ist zu prüfen, inwieweit die mit der Maßnahme verfolgten Ziele erreicht worden sind (Zielerreichungs-, Wirkungs- und Wirtschaftlichkeitskontrolle).

2.2 Ordnungsmäßigkeit

Ordnungsmäßigkeit umfasst die Einhaltung der geltenden Normen (Compliance), insbesondere der Gesetze, Haushaltspläne, Verwaltungsvorschriften und -grundsätze.

Beim IT-Einsatz in der öffentlichen Verwaltung sind insbesondere die Regelungen zum *E-Government*, zur *Revisionsfähigkeit*, zur *Informationssicherheit* (siehe dazu

Abschnitt 2.3), *zum Datenschutz,* zum *Arbeitsschutz, zur Barrierefreiheit und zur Ergonomie* zu beachten.

Um einen ordnungsgemäßen IT-Einsatz sicherzustellen, ist ein *internes Kontrollsystem* zu etablieren. Insbesondere sind das Vier-Augen-Prinzip und das Prinzip der Funktionstrennung zu beachten.

Planung und Einsatz der IT sowie Maßnahmen der internen Kontrolle sind zu dokumentieren. Die *Dokumentation* muss vollständig, aktuell und verständlich sein sowie alle Änderungen und Entscheidungen nachweisen.

Soweit die Akten elektronisch geführt werden (*E-Akten*/*elektronische Dokumente*), sind dazu nur revisionssichere Systeme zu verwenden. Für externe Prüfer ist lesender Zugriff zu gewährleisten. Die Vollständigkeit, Authentizität, Integrität, Lesbarkeit und Verkehrsfähigkeit elektronisch gespeicherter Daten sind auch während der gesetzlichen Aufbewahrungsfristen (*Langzeitspeicherung*) und ggf. dauerhaft im Rahmen der *Archivierung* sicherzustellen.

2.3 Informationssicherheit

Den Risiken beim Einsatz der IT ist durch infrastrukturelle, organisatorische, personelle und technische Maßnahmen zur *Informationssicherheit* 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.

Für die *Informationssicherheit* ist die Leitung der jeweiligen Einrichtung verantwortlich. Sie hat die Maßnahmen und Prozesse des *Informationssicherheitsmanagements* (ISM) zu initiieren, zu steuern, zu überwachen und sicherzustellen, dass die hierfür erforderlichen finanziellen, personellen und zeitlichen Ressourcen zur Verfügung stehen.

Die *Informationssicherheit* ist in die organisationsweiten Prozesse zu integrieren. Insbesondere ist eine Verzahnung mit den Prozessen des *IT-Servicemanagements* anzustreben.

Zur Gewährleistung der *Informationssicherheit* ist ein angemessenes, der Gefahrenlage angepasstes *Informationssicherheitsmanagementsystem (ISMS)* auf Basis eines geeigneten Standards einzurichten. Die Wirksamkeit und die Umsetzung des *ISMS* sind kontinuierlich zu überwachen und zu verbessern.

Es ist ein/e IT-Sicherheitsbeauftragte*/*r zu benennen. Diese*/*r ist außerhalb des operativen IT-Managements anzusiedeln, um Interessen- und Rollenkonflikte zu vermeiden.

Das *ISM*-Personal ist für seine Tätigkeit ausreichend zu qualifizieren. Besonderes Augenmerk ist auch auf die Information und Sensibilisierung aller Beschäftigten zu legen.

Aus regelmäßigen Schutzbedarfs-/ *Risikoanalysen* und deren Bewertung sind die notwendigen Maßnahmen zur *Informationssicherheit* abzuleiten.

Bei den Maßnahmen zur *Informationssicherheit* ist der Grundsatz der *Wirtschaftlichkeit und Sparsamkeit* zu beachten. Investitionen in technische Sicherheitsinfrastrukturen sollen erst dann erfolgen, nachdem die organisatorischen und personellen Voraussetzungen geschaffen wurden.

Für die Bundes- und die einzelnen Landesverwaltungen ist jeweils ein zentrales *ISMS* einzurichten und eine ressortübergreifende Aufgabenerledigung anzustreben. Verantwortlichkeiten für das *ISM* sollten auf *IT-Services* und nicht primär auf Organisationsgrenzen bezogen festgelegt werden.

Für die operativen Aufgaben des *ISM* ist ein wirksames *Computer Emergency Response Team* (CERT) einzusetzen. Dabei sind ressort- und länderübergreifende Kooperationen anzustreben.

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

Weitere Anforderungen an die *Informationssicherheit* ergeben sich aus dem Grundsatzpapier der Rechnungshöfe des Bundes und der Länder zum *Informationssicherheitsmanagement*.

3 Strategische und organisatorische Anforderungen

Die IT ist kein Selbstzweck. Sie hat sich an den Zielen und Aufgaben der öffentlichen Verwaltung auszurichten (*IT-Governance*).

Die strategischen und organisatorischen Anforderungen für den Einsatz der IT leiten sich aus dem Gebot eines ordnungsgemäßen, sicheren und wirtschaftlichen Verwaltungshandelns ab.

Als Bindeglied zwischen politischer Führung und *IT-Organisation* sollten beim Bund, den Ländern und den Kommunen Beauftragte für IT (Chief Information Officer - CIO) bestellt werden.

3.1 IT-Strategie

Der ebenenübergreifende Handlungsrahmen wird insbesondere durch die Nationale E-Government-Strategie (NEGS) des Planungsrats für die IT-Zusammenarbeit der öffentlichen Verwaltung zwischen Bund und Ländern (*IT-Planungsrat*) vorgegeben. Die Strategie bündelt die *gesellschaftlichen und politischen Ziele* des Bundes, der Länder und der Kommunen zur IT. Sie berücksichtigt insbesondere auch den gebietskörperschafts- oder verwaltungsebenenübergreifenden IT-Einsatz. Diese Ziele sind entsprechend der jeweiligen Bedürfnisse der Gebietskörperschaft und deren Aufgaben zu konkretisieren. Dafür sollten die CIO des Bundes und der Länder sowie vergleichbare Funktionsträger der Kommunen verantwortlich sein.[2]

Innerhalb der Gebietskörperschaften kann die *IT-Strategie* unter Berücksichtigung der fachspezifischen Aufgaben, z. B. in einem Ressort, einer Fachverwaltung oder einer kommunalen Behörde, präzisiert werden.

Eine *IT-Strategie* sollte insbesondere Aussagen zu folgenden Punkten enthalten:

- Prinzipien und Leitlinien des IT-Einsatzes,
- Beitrag der IT zur Erreichung der grundsätzlichen strategischen Ziele,
- Planung, Steuerung und Kontrolle der IT-Serviceprozesse,
- Organisation, Steuerung und Finanzierung des IT-Einsatzes,

[2] Im Folgenden wird nur noch von CIO gesprochen. Alle Aussagen gelten für vergleichbare kommunale Funktionsträger entsprechend.

- Konsolidierung und Zentralisierung,
- ebenenübergreifende IT (z. B. Kooperationen in IT-Verbünden),
- notwendige Umsetzungsressourcen,
- IT-Architektur (Technologien, Standards, *Schnittstellen* und Anwendungen) und
- IT-Infrastruktur.

Sie hat sich auch mit aktuellen gesellschaftlichen Fragestellungen zu befassen, wie z. B. dem demografischen Wandel. Dabei sind u. a. ein sich änderndes Nutzerverhalten in und außerhalb der öffentlichen Verwaltung sowie die Gewinnung von hinreichend qualifiziertem Personal zu berücksichtigen.

Die aus der *IT-Strategie* abgeleiteten IT-Maßnahmen sind zu benennen und zu priorisieren sowie mit operationalisierbaren *Kennzahlen* zu verbinden. Die *IT-Strategie*, IT-Maßnahmen und *Kennzahlen* sind zu kommunizieren und regelmäßig fortzuschreiben.

Durch ein Akzeptanzmanagement ist sicherzustellen, dass die Organisationseinheiten und die Anwender hinreichend eingebunden werden.

3.2 IT-Organisation

Die Organisation der IT soll gewährleisten, dass diese sowohl serviceorientiert als auch wirtschaftlich die Ziele der Verwaltung unterstützt. Die ressortübergreifende IT-Koordinierung, die Planung und Kontrolle strategischer Aufgaben, Querschnittsaufgaben und Infrastrukturen sollen zentral gebündelt werden.

Der *IT-Planungsrat* koordiniert die Zusammenarbeit von Bund und Ländern in Fragen der Informationstechnik, beschließt Standards, steuert zugewiesene Projekte und übernimmt Aufgaben für das Verbindungsnetz zwischen Bund und Ländern.

Die CIO sind mit Kompetenzen und Personalkapazitäten so auszustatten, dass sie die IT organisationsübergreifend planen, entwickeln und koordinieren können. Ein Gremium der IT-Zuständigen sollte sie dabei beratend unterstützen. Insbesondere sollte durch die CIO geregelt werden:

- Führungs- und Steuerungsprinzipien,
- grundsätzliche Zuständigkeiten einer *IT-Organisation*,
- Aufgabenzuweisungen an IT-Dienstleister,

- Anforderungen an ein *IT-Servicemanagement* (ITSM) und die IT-*Qualität,* ggf. die Auswahl eines geeigneten Werkzeugs,
- Grundprinzipien für das *Informationssicherheitsmanagement* (ISM) auf Basis der vom *IT-Planungsrat* verabschiedeten Leitlinie für *Informationssicherheit*,
- Standards für die übergreifende IT-Ressourcenplanung unter besonderer Berücksichtigung der Personalgewinnung und -entwicklung sowie der Aus- und Fortbildung und laufenden Qualifizierung,
- die Einbindung, Steuerung und Kontrolle Externer derart, dass die Verlässlichkeit und Flexibilität der IT durch eigenes Personal sichergestellt ist,
- *IT-Controlling* einschließlich *Risikomanagement*,
- Organisation von *Qualitäts*sicherung und -management,
- Standards für *IT-Systemarchitekturen*, *IT-Systemkomponenten*, den *Datenaustausch* und Benutzerschnittstellen (Architekturmanagement) sowie
- Standards für das *Projektmanagement*, den *IT-Betrieb* und *IT-Beschaffungen*.

Die Dienststellen und Organisationseinheiten haben die zugewiesenen IT-Aufgaben entsprechend der strategischen und organisatorischen Rahmenbedingungen wahrzunehmen. Bei der Wahrnehmung der IT-Aufgaben sind

- die fachliche Anforderung und Freigabe,
- deren IT-fachliche Entwicklung/Umsetzung und
- die Betriebsverantwortung für die Informationssysteme

organisatorisch und personell zu trennen.

Die *IT-Organisation* ist regelmäßig durch die CIO wie auch durch die IT-Verantwortlichen zu überprüfen und anzupassen.

3.3 IT-Management

Die CIO und die Führungskräfte sind für das IT-Management verantwortlich. Das IT-Management soll sicherstellen, dass sich die IT an der *IT-Strategie* und den Zielen der jeweiligen Institution ausrichtet (strategisches IT-Management) und dass die IT-Ressourcen optimal eingesetzt werden (operatives IT-Management).

Aufgaben des IT-Managements sind u. a.:

- Richtlinien zu entwickeln und *Rahmenwerke* bedarfsgerecht anzupassen,
- Organisationsstrukturen festzulegen,

- die erforderlichen Beschäftigten mit den benötigten Fähigkeiten und Kompetenzen bereitzustellen,
- Prozesse und Sicherheitsanforderungen zu definieren,
- Fach-, Entwicklungs- und Betriebsverantwortung abzugrenzen,
- die notwendigen Informationen, z. B. geeignete *Kennzahlen* bereitzustellen,
- Dienste, Infrastruktur und Verfahren einschließlich deren Lebens- und Beschaffungszyklen zu definieren,
- Vorgaben zu entwickeln, welche IT-Leistungen eigenes Personal oder Externe erbringen sollen,
- in Institutionen, die eine direkte Leistungsbeziehung mit IT-Dienstleistern haben, die entsprechenden Fähigkeiten zur Anforderungsdefinition, Steuerung und Überwachung der Leistungen vorzuhalten (Auftraggeberfähigkeit),
- *verbindliche Vereinbarungen* für die auf IT-Dienstleister übertragenen Aufgaben zu treffen,
- Vorgaben zur Identifizierung der Kosten und des Nutzens der IT festzulegen, um den IT-Einsatz optimieren und die Effizienz und Effektivität des Verwaltungshandelns sicherstellen zu können (*IT-Controlling*).

Die Aufgaben des IT-Managements sind regelmäßig – auch im Sinne eines Innovationsmanagements – zu überprüfen und anzupassen.

4 Operative IT-Planung, IT-Steuerung und IT-Betrieb

4.1 IT-Planung

Auf Grundlage der strategischen und organisatorischen IT-Anforderungen muss die operative *IT-Planung* der Ressorts und der weiteren Verwaltung erstellt werden. Die operative *IT-Planung* sollte ziel- und zukunftsorientiert, angemessen detailliert, aktuell und lückenlos sein. Die *IT-Planung* umfasst insbesondere:

- den behördlichen IT-Einsatz,
- Bedarfsanalyse und generelles Anforderungsmanagement,
- Einführungsstrategien,

- Konzeption für Schulung und Anwenderbetreuung,
- *Informationssicherheit*,
- Aussagen zum Bedarf an Ressourcen: Haushaltsmittel (konsumtiv und investiv), Personal, Technik/Systeme, Infrastruktur,
- Regelungen zur Bestandsführung von Hardware, Software, Infrastrukturen,
- Festlegungen zum (Multi-)*Projektmanagement*-System, das alle relevanten Teildisziplinen, insbesondere das Termin-, Kosten- und *Risikomanagement*, angemessen berücksichtigt,
- Berücksichtigung der speziellen Erfordernisse bei *IT-Großprojekten*.

Die *IT-Planung* ist kontinuierlich zu überprüfen, fortzuschreiben und zu kommunizieren.

Das *IT-Servicemanagement* (ITSM) muss insbesondere folgende Teildisziplinen angemessen berücksichtigen:

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

Die Personalressourcen für die IT sind auf Grundlage von Personalbedarfsberechnungen zu ermitteln. Grundlage sollten Daten zu durchgeführten Maßnahmen, Projekten und zum *IT-Betrieb* sein. Sie sollten den jeweils zu Beginn geschätzten Aufwand, den tatsächlichen Personaleinsatz und hinreichende Aussagen über die Fertigkeiten der eingesetzten Personen und die Gründe für die Abweichungen enthalten. Der erforderliche Umfang des eingesetzten Personals ist in regelmäßigen Abständen zu überprüfen.

Das IT-Personal ist durch Fortbildungen entsprechend der fachlichen Anforderungen und des technischen Fortschritts zu qualifizieren, um für die Kernprozesse und eingesetzten Technologien ausreichende Kompetenzen aufzubauen und zu pflegen.

4.2 IT-Steuerung

Zur Steuerung und Kontrolle 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, Metriken* zur *Qualität*ssicherung, 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.
- 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.

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 definieren und dokumentieren. 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. Im *Risikomanagement* sind die Maßnahmen zur systematischen Erkennung, Analyse, Überwachung und Kontrolle von Risiken im *IT-Betrieb* festzulegen.

5 IT-Maßnahmen

5.1 Planung

Zur Planung einer IT-Maßnahme[3] gehören

- die Festlegung der Ziele,
- die Entscheidung über eine Projektorganisation,
- Festlegung eines geeigneten *Projektmanagement*systems,
- eine Anforderungsanalyse,
- ein Pflichtenheft,
- eine an Meilensteinen orientierte Zeitplanung und
- eine *Wirtschaftlichkeitsuntersuchung*.

Die Planung ist zu dokumentieren. Die Planungsdokumente sind regelmäßig mit dem aktuellen Projektstand abzugleichen und zu aktualisieren (rollierende Planung).

Vor der Planung und Einführung neuer Verfahren und Dienste sind die Geschäftsprozesse zu analysieren und zu optimieren. Dabei sind die für Organisationsfragen zuständigen Stellen in Zusammenarbeit mit den Fachbereichen und den IT-Bereichen zu beteiligen. Bei behördenübergreifenden Maßnahmen sind Beteiligung und Verantwortung im Einzelnen zu regeln.

Bei der Planung sind durch eine *Wirtschaftlichkeitsuntersuchung* insbesondere folgende Alternativen zu prüfen:

- der Einsatz von Standard-Produkten,
- die Übernahme vorhandener Produkte,
- die Neuentwicklung durch eigene Mitarbeiter und
- die Neuentwicklung durch Externe.

[3] IT-Maßnahmen (in einigen Ländern auch bezeichnet als IT-Vorhaben, IT-Projekte) umfassen die Konzeption, die Entwicklung, die Beschaffung, die Einführung oder wesentliche Änderungen im *IT-Betrieb*, von IT-Verfahren, der IT-Infrastruktur und bei IT-Diensten.

5.2 Beschaffung

Die *IT-Beschaffung* sollte die bedarfs- und nutzergerechte Versorgung der Dienststellen mit den zur Aufgabenerfüllung benötigten IT-Komponenten und IT-Dienstleistungen gewährleisten. Bei Beschaffungen ist der Grundsatz der *Wirtschaftlichkeit und Sparsamkeit* zu beachten. Dabei ist die wirtschaftlichste Beschaffungsart (Kauf, Miete, Leasing) auszuwählen.

Technische und wirtschaftliche Abhängigkeiten von einzelnen Externen sind möglichst 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. Rahmenvereinbarungen sind zu nutzen.

5.3 Beauftragung und Einsatz Externer

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,
- Management 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. Beratungsergebnisse dürfen nicht unreflektiert übernommen werden.

5.4 Entwicklung und Pflege

Bei der Entwicklung und Pflege sind Vorgehensweisen, *Qualität*svorgaben und Arbeitstechniken festzulegen, regelmäßig zu überprüfen und anzupassen.

Die *Softwareentwicklung* ist – auch zur Sicherung der Pflege und Weiterentwicklung – nach geeigneten Methoden des Software-Engineerings durchzuführen. Werden Externe mit der Entwicklung von Software beauftragt, soll der Zugriff auf den Quellcode – ggf. durch Hinterlegung – sichergestellt werden.

Eine revisionssichere *Dokumentation* muss die Pflege, die Wartung und einen ordnungsgemäßen *IT-Betrieb* unterstützen sowie eine effektive und effiziente Nutzung durch die Anwender ermöglichen.

5.5 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 im Voraus festgelegten Testszenarien durchgeführt werden. Die fachlich zuständigen Stellen haben hierfür geeignete 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. Tests sind nicht im produktiven System durchzuführen. 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.

Soweit bei IT-Maßnahmen, die nicht Verfahren betreffen, Tests und Freigaben erforderlich werden, gelten die oben dargestellten Anforderungen entsprechend.

5.6 Einführung

Bei der Einführung von IT-Maßnahmen ist insbesondere rechtzeitig zu gewährleisten, dass

- die erforderliche Hard- und Softwareumgebung eingerichtet ist,
- die vorhandenen Datenbestände übernommen werden,
- die Benutzer bedarfsgerecht und zeitnah geschult werden und
- alle notwendigen rechtlichen Voraussetzungen vorliegen.

Für eine fortlaufende Beratung und Schulung der Benutzer muss Vorsorge getroffen werden. Eine im Umfang angemessene aktuelle Anwenderdokumentation ist bereitzustellen.

Bei der Einführung von IT-Maßnahmen sind die Aspekte des organisationalen Wandels und des Akzeptanzmanagements zu beachten.

IuK-Mindestanforderungen

Anlage:
Fundstellen zu Normen, Standards und Empfehlungen

Stand: Juni 2016

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

Die nachfolgend aufgeführten Links und Versionsangaben geben den Stand zum Zeitpunkt der Erstellung des Dokuments wieder. Sollten danach neue Versionen der entsprechenden Unterlagen und Regelwerke veröffentlicht werden, so werden auch diese hinsichtlich fortgeführter Inhalte von den Rechnungshöfen des Bundes und der Länder berücksichtigt.

Bei Rechtsgrundlagen ist auf die jeweils geltende Fassung zu achten.

Die nachfolgende Aufzählung erhebt keinen Anspruch auf Vollständigkeit.

Bei vergleichbaren Normen, Standards und Empfehlungen, die sowohl vom Bund wie auch von den Ländern herausgegeben wurden, wird aus Platzgründen auf eine Quelle der Bundesebene verwiesen.

Stichwort	Zu Nr.	Norm, Standard, Empfehlung	Quelle, Bemerkung
Arbeitsschutz	2.2	Arbeitsschutzgesetz (ArbSchG)	www.gesetze-im-internet.de | ArbSchG
		Bildschirmarbeitsverordnung (BildscharbV)	www.gesetze-im-internet.de | BildscharbV
Archivierung	2.2		Zeitraum nach Abschluss der Langzeitspeicherung
		Grundsätze zur ordnungsgemäßen Führung und Aufbewahrung von Büchern, Aufzeichnungen und Unterlagen in elektronischer Form sowie zum Datenzugriff (GoBD)	Bundesfinanzministerium (BMF), www.bundesfinanzministerium.de | GoBD
		Grundsätze ordnungsmäßiger Buchführung beim Einsatz elektronischer Archivierungsverfahren (IDW RS FAIT 3)	Institut der Wirtschaftsprüfer in Deutschland e. V. (IDW)
Audits (IT-Sicherheit)	2.3	Informationstechnik - IT-Sicherheitsverfahren - Informationssicherheits-Managementsysteme - Anforderungen (DIN ISO/IEC 27001)	DIN, ISO
		IT-Grundschutz	BSI, www.bsi.bund.de | Themen | IT-Grundschutz
		Informationssicherheitsmanagementsystem in 12 Schritten (ISIS12)	Bayerischer IT-Sicherheitscluster e.V., www.it-sicherheit-bayern.de | ISIS12
Audits (Prozesse)	4.2	Qualitätsmanagementsysteme - Grundlagen und Begriffe (DIN EN ISO 9000)	Deutsches Institut für Normung e. V. (DIN), International Organization for Standardization (ISO)
		Informationstechnik - Prozessbewertung (Normenfamilie ISO/IEC 15504)	DIN, ISO
		Europäisches Qualitätsbewertungssystem für Organisationen des öffentlichen Sektors, Common Assessment Framework (CAF)	Deutsches CAF-Zentrum im Bundesverwaltungsamt, www.bva.bund.de | Themen | Beratung/Modernisierung | Deutsches CAF-Zentrum
		Reifegradmodell der Softwareentwicklung - Capability Maturity Model Integration (CMMI)	CMMI Institute, www.cmmiinstitute.com (englisch)
		siehe Rahmenwerke, COBIT	
		Change-Management nach ITIL, siehe Rahmenwerke, ITIL	

Stichwort	Zu Nr.	Norm, Standard, Empfehlung	Quelle, Bemerkung
Barrierefreiheit	2.2	Gesetz zur Gleichstellung behinderter Menschen (BGG)	www.gesetze-im-internet.de | BGG
		Verordnung zur Schaffung barrierefreier Informationstechnik nach dem Behindertengleichstellungsgesetz (Barrierefreie Informationstechnik-Verordnung - BITV) und vergleichbare Landesregelungen	www.gesetze-im-internet.de | BITV
Beauftragung und Einsatz Externer	5.3	Einsatz externer Berater durch die Bundesverwaltung	Gutachten des Beauftragten für die Wirtschaftlichkeit in der Verwaltung, Band 14, 2006, www.bundesrechnungshof.de | Band 14
		Empfehlungen zur Inanspruchnahme von externen Unterstützungsleistungen durch Bundesbehörden im IT-Bereich	KBSt-Empfehlung vom 16. Januar 2001, www.cio.bund.de | Arbeitsgrundlagen (mit weiteren Quellen)
		Kriterien für die Nutzung von Cloud-Diensten der IT-Wirtschaft durch die Bundesverwaltung	Rat der IT-Beauftragten der Ressorts der Bundesverwaltung (IT-Rat Bund), Beschluss vom 29. Juli 2015, www.cio.bund.de | Cloud-Dienste
Computer Emergency Response Team (CERT)	2.3		Ist ein Expertenteam, das als zentrale Anlaufstelle für präventive und reaktive Maßnahmen in Bezug auf sicherheitsrelevante Vorfälle dient.
		Leitlinie für die Informationssicherheit in der öffentlichen Verwaltung - Hauptdokument und Umsetzungsplan -	IT-Planungsrat, www.it-planungsrat.de | Informationssicherheitsleitlinie
Datenaustausch	3.2	siehe auch Schnittstelle	
		Koordinierungsstelle für IT-Standards (KoSIT)	KoSIT, www.xoev.de (Startseite)
Datenschutz	2.2	Bundesdatenschutzgesetz (BDSG), und entsprechende Ländergesetze	www.gesetze-im-internet.de | BDSG
		Richtlinie 95/46/EG zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr	Richtlinie des Europäischen Parlaments und des Rates, www.eur-lex.europa.eu | 31995L0046

Stichwort	Zu Nr.	Norm, Standard, Empfehlung	Quelle, Bemerkung
Datenschutz		Datenschutz-Grundverordnung. Diese wird ab dem Jahr 2018 die Richtlinie 95/46/EG ersetzen.	Vorschlag der Kommission, www.eur-lex.europa.eu | Datenschutz-Grundverordnung, Überblick des Berufsverbands der Datenschutzbeauftragten Deutschlands, www.bvdnet.de | DSGVO
		IT-Grundschutz (Baustein 1.5 Datenschutz)	Bundesamt für Sicherheit in der Informationstechnik (BSI), www.bsi.bund.de | Baustein 1.5 Datenschutz
		Standard-Datenschutzmodell	Abrufbar auf den Seiten der Datenschutzbeauftragten des Bundes und der Länder, z.B. www.saechsdsb.de | Standard-Datenschutzmodell
		Orientierungshilfen der Beauftragten für den Datenschutz zu verschiedenen Themen	Abrufbar auf den Seiten der Datenschutzbeauftragten des Bundes und der Länder
Dokumentation	2.2 5.4	Grundsatz der Schriftlichkeit (Aktenmäßigkeit)	Online-Verwaltungslexikon, www.olev.de | Schriftlichkeit
		Grundsätze zur ordnungsgemäßen Führung und Aufbewahrung von Büchern, Aufzeichnungen und Unterlagen in elektronischer Form sowie zum Datenzugriff (GoBD) - insbesondere Nr. 10	BMF, www.bundesfinanzministerium.de | GoBD
		§ 12 Abs. 2 der Gemeinsamen Geschäftsordnung der Bundesministerien (GGO) und vergleichbare Landesvorschriften	Bundesministerium des Innern (BMI), www.bmi.bund.de | Moderne Verwaltung und Öffentlicher Dienst | Verwaltungsorganisation | Gemeinsame Geschäftsordnung der Bundesministerien
		Registraturrichtlinie für das Bearbeiten und Verwalten von Schriftgut in Bundesministerien und vergleichbare Landesvorschriften	BMI, www.bmi.bund.de | Registraturrichtlinie
		DIN ISO 15489-1 Information und Dokumentation - Schriftgutverwaltung	DIN
		Verwaltungsvorschriften für Zahlungen, Buchführung und Rechnungslegung (§§ 70 bis 72, 74 bis 80 LHO des Bundes und der Länder)	Kompetenzzentrum für das Kassen- und Rechnungswesen des Bundes (KKR), www.kkr.bund.de | 70 bis 72

Stichwort	Zu Nr.	Norm, Standard, Empfehlung	Quelle, Bemerkung
Dokumentation		IT-Grundschutz Maßnahmenkatalog M 2.219 - Kontinuierliche Dokumentation der Informationsverarbeitung	BSI, www.bsi.bund.de | M 2.219
E-Akte	2.2	Gesetz zur Förderung der elektronischen Verwaltung (EGovG) und vergleichbare Landesvorschriften	www.gesetze-im-internet.de | EGovG
		Organisationskonzept elektronische Verwaltungsarbeit, verschiedene Bausteine, u. a. zur E-Akte	Bundesregierung, www.verwaltung-innovativ.de | Organisationskonzept
		Referenzarchitektur elektronische Verwaltungsarbeit	Der Beauftragte der Bundesregierung für Informationstechnik (CIO Bund), www.cio.bund.de | Architekturmanagement Bundesverwaltung
		Positionspapier zum Thema Aktenführung	Rechnungshöfe des Bundes und der Länder, z. B. www.bundesrechnungshof.de | Aktenführung
		Positionspapier zum Thema E-Akte	Rechnungshöfe des Bundes und der Länder, www.landesrechnungshof-sh.de | E-Akte
		IT-Grundschutz Maßnahmenkatalog M 2.259 - Einführung eines übergeordneten Dokumentenmanagements	BSI, www.bsi.bund.de | M 2.259
		Einführung der E-Akte	Handreichung der Bundes-Arbeitsgemeinschaft der Kommunalen IT-Dienstleister e. V. (VITAKO), www.vitako.de | Handreichung E-Akte
E-Government	2.2	Gesetz zur Förderung der elektronischen Verwaltung (EGovG) und vergleichbare Landesvorschriften	www.gesetze-im-internet.de | EGovG
Elektronische Dokumente	2.2	siehe E-Akte	
Erfolgskontrolle	2.1	Verwaltungsvorschriften zu § / Artikel 7 der Haushaltsordnungen des Bundes und der Länder	z. B. www.verwaltungsvorschriften-im-internet.de | VV-BHO
		Arbeitsanleitung Einführung in Wirtschaftlichkeitsuntersuchungen	BMF, www.verwaltungsvorschriften-im-internet.de | Wirtschaftlichkeitsuntersuchungen

Stichwort	Zu Nr.	Norm, Standard, Empfehlung	Quelle, Bemerkung
Erfolgskontrolle		Erfolgskontrolle finanzwirksamer Maßnahmen in der öffentlichen Verwaltung	Gutachten des Beauftragten für die Wirtschaftlichkeit in der Verwaltung, Band 2, 1998, www.bundesrechnungshof.de | Band 02
		Erfolgskontrolle in der öffentlichen Verwaltung	Finanzministerium des Landes Mecklenburg-Vorpommern, www.regierung-mv.de | Erfolgskontrolle
Ergonomie	2.2	Bildschirmarbeitsverordnung (BildscharbV)	www.gesetze-im-internet.de | BildscharbV
		Normenreihe DIN EN ISO 9241 „Ergonomische Anforderungen für Bürotätigkeiten mit Bildschirmgeräten”	DIN, ISO
		Leitfaden Usability	Deutsche Akkreditierungsstelle GmbH (DAkkS), www.dakks.de | Usability
gesellschaftliche und politische Ziele	3.1	Digitale Agenda für Europa Strategie für einen digitalen Binnenmarkt	Europäische Kommission, www.ec.europa.eu | Deutsch | Digitaler Binnenmarkt
		Nationale E-Government-Strategie	IT-Planungsrat, www.it-planungsrat.de | NEGS
		Digitale Verwaltung 2020	Bundesregierung, www.verwaltung-innovativ.de | Regierungsprogramm Digitale Verwaltung 2020
Informationssicherheit	2.2 2.3 3.2 4.1	Leitlinie für die Informationssicherheit in der öffentlichen Verwaltung - Hauptdokument und Umsetzungsplan -	IT-Planungsrat, www.it-planungsrat.de | Informationssicherheitsleitlinie
		IT-Grundschutz, Kapitel 2: Informationssicherheitsmanagement	BSI, www.bsi.bund.de | Informationssicherheitsmanagement
		Leitfaden Informationssicherheit	BSI, www.bsi.bund.de | Leitfaden Informationssicherheit
		BSI-Standard 100-1: Managementsysteme für Informationssicherheit	BSI, www.bsi.bund.de | 100-1
		BSI-Standard 100-2: IT-Grundschutz-Vorgehensweise	BSI, www.bsi.bund.de | 100-2

Stichwort	Zu Nr.	Norm, Standard, Empfehlung	Quelle, Bemerkung
Informationssicherheit		BSI-Standard 100-3: Risikoanalyse auf der Basis von IT-Grundschutz	BSI, www.bsi.bund.de | 100-3
		BSI-Standard 100-4: Notfallmanagement	BSI, www.bsi.bund.de | Umsetzungsrahmenwerk 100-4
		BSI IT-Grundschutz-Kataloge	BSI, www.bsi.bund.de | Themen | IT-Grundschutz | Grundschutzkataloge
		BSI IT-Grundschutz GSTOOL	BSI, www.bsi.bund.de | GSTOOL
		Informationssicherheitsrevision - Ein Leitfaden für die IS-Revision auf Basis von IT-Grundschutz -	BSI, www.bsi.bund.de | Leitfaden IS-Revision
		Informationssicherheitsmanagementsystem in 12 Schritten (ISIS12)	Bayerischer IT-Sicherheitscluster e.V., www.it-sicherheit-bayern.de | ISIS12
		Grundsatzpapier zum Informationssicherheitsmanagement	Rechnungshöfe des Bundes und der Länder, z. B. www.bundesrechnungshof.de | Grundsatzpapier Informationssicherheitsmanagement
		Informationstechnik - IT-Sicherheitsverfahren - Informationssicherheits-Managementsysteme - Anforderungen (DIN ISO/IEC 27001)	DIN, ISO
		Leitlinie zur Internet-Sicherheit	BSI, www.bsi.bund.de | Internet-Sicherheit (ISi-Reihe)
		siehe Rahmenwerke, COBIT	
		Kompass der IT-Sicherheitsstandards	Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e.V. (bitkom), www.kompass-sicherheitsstandards.de (Startseite)
		The ISF Standard of Good Practice	Information Security Forum, www.securityforum.org | ISF Standard of Good Practice (englisch)

Stichwort	Zu Nr.	Norm, Standard, Empfehlung	Quelle, Bemerkung
Informationssicherheits-management (ISM)	2.3		Planungs- und Lenkungsaufgabe, die erforderlich ist, um einen durchdachten und planmäßigen Informationssicherheitsprozess aufzubauen und kontinuierlich umzusetzen.
		Grundsatzpapier zum Informationssicherheitsmanagement mit Fragenkatalog	Rechnungshöfe des Bundes und der Länder, z. B. www.bundesrechnungshof.de | Grundsatzpapier Informationssicherheitsmanagement
Informationssicherheits-managementsystem (ISMS)	2.3		Teil des Managementsystems, der auf der Basis eines risikobasierten Ansatzes die Entwicklung, Implementierung, Durchführung, Überwachung, Überprüfung, Instandhaltung und Verbesserung der Informationssicherheit abdeckt.
		Informationstechnik - IT-Sicherheitsverfahren - Informationssicherheits-Managementsysteme - Anforderungen (DIN ISO/IEC 27001)	DIN, ISO
		Informationssicherheitsmanagementsystem in 12 Schritten (ISIS12)	Bayerischer IT-Sicherheitscluster e.V., www.it-sicherheit-bayern.de | ISIS12
Internes Kontrollsystem (IKS)	2.2	Empfehlungen für Interne Revisionen in der Bundesverwaltung	BMI, www.bmi.bund.de | Interne Revisionen
		Grundsätze zur ordnungsgemäßen Führung und Aufbewahrung von Büchern, Aufzeichnungen und Unterlagen in elektronischer Form sowie zum Datenzugriff (GoBD)	BMF, www.bundesfinanzministerium.de | GoBD
		Grundsätze ordnungsmäßiger Buchführung bei Einsatz von Informationstechnologie (IDW RS FAIT 1)	IDW
		Grundsätze ordnungsmäßiger Buchführung beim Einsatz elektronischer Archivierungsverfahren (IDW RS FAIT 3)	IDW
		Abschlussprüfung bei Einsatz von Informationstechnologie (IDW PS 330)	IDW

Stichwort	Zu Nr.	Norm, Standard, Empfehlung	Quelle, Bemerkung
Internes Kontrollsystem (IKS)		Informationssicherheitsrevision - Ein Leitfaden für die IS-Revision auf Basis von IT-Grundschutz -	BSI, www.bsi.bund.de | Leitfaden IS-Revision
		siehe Rahmenwerke, COBIT	
		Aufbau eines Internen Kontrollsystems (IKS)	Eidgenössischen Finanzkontrolle, www.efk.admin.ch | Aufbau IKS
		Richtlinien für die internen Kontrollnormen im öffentlichen Sektor	Internationale Organisation der Obersten Rechnungskontrollbehörden (INTOSAI), www.intosai.org | guidelines Kontrollnormen im öffentlichen Sektor
		ISSAI - Die Internationalen Normen und Richtlinien für die staatliche Finanzkontrolle	INTOSAI, de.issai.org | INTOSAI-Leitlinien für Good Governance
IT-Beschaffungen	3.2 5.2	Unterlage für Ausschreibung und Bewertung von IT-Leistungen (UfAB VI)	CIO Bund, www.cio.bund.de | UfAB VI
		Ergänzenden Vertragsbedingungen für die Beschaffung von Informationstechnik (EVB-IT)	CIO Bund, www.cio.bund.de | EVB-IT
		Leitfäden für produktneutrale Ausschreibungen	bitkom, www.itk-beschaffung.de (Startseite)
		Umfassende Liste von Normen und Rechtsgrundlagen	Beschaffungsamt des BMI, www.bescha.bund.de | Normen und Rechtsvorschriften
IT-Betrieb	3.2 4.1 4.3 5.4	siehe IT-Servicemanagement	
IT-Controlling	3.2 3.3 4.2	siehe Rahmenwerke, COBIT	
		Informationstechnik - Unternehmensführung in der Informationstechnik (ISO/IEC 38500)	DIN, ISO

Stichwort	Zu Nr.	Norm, Standard, Empfehlung	Quelle, Bemerkung
IT-Governance	3	siehe Rahmenwerke, COBIT	
		siehe Rahmenwerke, ITIL	
		Informationstechnik - Unternehmensführung in der Informationstechnik (ISO/IEC 38500)	DIN, ISO
		Spezifikationen und für IT Service Management (Normenreihe ISO/IEC 20000)	DIN, ISO
IT-Großprojekte	4.1	siehe IT-Projektmanagement	
		S-O-S-Methode© für Großprojekte	Bundesverwaltungsamt, www.bva.bund.de | SOS-Methode
IT-Organisation	3.2	Handbuch für Organisationsuntersuchungen und Personalbedarfsermittlung	BMI, www.orghandbuch.de (Startseite)
IT-Planung	4.1	siehe Rahmenwerke, COBIT	
		siehe Rahmenwerke, ITIL	
		IT-Rahmenkonzept des Bundes und vergleichbare Landesregelungen /-vorgaben	z. B. CIO Bund, www.cio.bund.de | Strategische Themen | IT-Steuerung Bund
IT-Planungsrat	3.1 3.2	Beschlüsse und Empfehlungen des IT-Planungsrates des Bundes und der Länder (IT-Planungsrat)	www.it-planungsrat.de
IT-Service / IT-Servicemanagement	2.3 3.2 4.1		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.
		siehe Rahmenwerke, ITIL	
		Standardfamilie für ein „leichtgewichtiges IT Service Management“ (FitSM)	Frei verfügbare Ergebnisse des EU-geförderten Projekts „Implementing service management in federated e-Infrastructures“ (FedSM), www.fitsm.itemo.org

Stichwort	Zu Nr.	Norm, Standard, Empfehlung	Quelle, Bemerkung
IT-Service / IT-Servicemanagement		Spezifikationen und für IT Service Management (Normenreihe ISO/IEC 20000)	DIN, ISO
		Sicherheit und Schutz des Gemeinwesens - Business Continuity Management System - Anforderungen (ISO 22301)	DIN, ISO
		Qualitätsmanagementsysteme - Grundlagen und Begriffe (ISO 9000)	DIN, ISO
IT-Strategie	3.1 3.3	IT-Steuerung Bund und evtl. IT-Steuerungsregeln, Organisationserlasse und sonstige Planungsregeln der Länder	Konzept des Bundesministeriums des Innern und des Bundesministeriums der Finanzen, Kabinettbeschluss vom 5. Dezember 2007, www.cio.bund.de | Strategische Themen | IT-Steuerung Bund
		Grobkonzept zur IT-Konsolidierung Bund	Bundeskabinett, Beschluss vom 20.05.2015, http://www.cio.bund.de | IT-Konsolidierung Bund
IT-Systemarchitekturen	3.2	Standards und Architekturen für E-Government-Anwendungen (SAGA) für die Bundesverwaltung und landesspezifische Regelungen und Vorgaben	IT-Rat Bund, Beschluss vom 03.11.2011, www.cio.bund.de | SAGA
IT-Systemkomponenten	3.2	siehe IT-Systemarchitekturen	
Kennzahlen, Metriken	4.2	siehe Rahmenwerke, COBIT	
		siehe Rahmenwerke, ITIL	
Langzeitspeicherung	2.2		Zeitraum vom Ablegen eines Vorgangs bis zur Aussonderung.
		Organisationskonzept elektronische Verwaltungsarbeit, verschiedene Bausteine, u. a. zur E-Langzeitspeicherung	Bundesregierung, www.verwaltung-innovativ.de | Organisationskonzept
		Technische Richtlinie: Vertrauenswürdige elektronische Langzeitspeicherung; Beweiswerterhaltung kryptographisch signierter Dokumente	BSI, www.bsi.bund.de | TR-03125
		Ergebnisse des Projekts NaLa - Nationale Langzeitspeicherung	IT-Planungsrat, www.it-planungsrat.de | NaLa

Stichwort	Zu Nr.	Norm, Standard, Empfehlung	Quelle, Bemerkung
Projektmanagement	3.2 4.1	V-Modell XT und V-Modell XT Bund	CIO Bund, www.cio.bund.de | V-Modell XT, www.cio.bund.de | V-Modell XT Bund
		Projects in Controlled Environments (PRINCE2)	AXELOS, www.axelos.com | PRINCE2 (englisch)
		HERMES	Schweizerische Eidgenossenschaft, www.isb.admin.ch | Themen | Projektmanagement | HERMES
		A Guide to the Project Management Body of Knowledge (PMBOK® Guide)	IEEE Standards Association, www.ieee.org | PMBOK (englisch)
		Projektmanagementsysteme (Normenfamilie DIN 69901)	DIN
		Qualitätsmanagementsysteme - Leitfaden für Qualitätsmanagement in Projekten (ISO 10006)	DIN, ISO
Qualität / Qualitätsmanagement	3.2 4.2	Qualitätsmanagementsysteme - Grundlagen und Begriffe (DIN EN ISO 9000)	DIN, ISO
Rahmenwerke	3.3	Spezifikationen und für IT Service Management (Normenreihe ISO/IEC 20000)	DIN, ISO
		IT Infrastructure Library (ITIL)	IT Service Management Forum (itSMF), www.itsmf-library.org | eKnowledge, Sprachauswahl Deutsch BSI, www.bsi.bund.de | ITIL AXELOS, www.itil-officialsite.com (englisch) ITIL.org, www.itil.org
		Control Objectives for Information and Related Technology (COBIT)	Information Systems Audit and Control Association (ISACA), Internationaler Berufsverband von IT-Revisoren, -Sicherheitsmanagern und -Experten, www.isaca.org | COBIT

Stichwort	Zu Nr.	Norm, Standard, Empfehlung	Quelle, Bemerkung
Rahmenwerke		Standardfamilie für ein „leichtgewichtiges IT Service Management“ (FitSM)	Frei verfügbare Ergebnisse des EU-geförderten Projekts „Implementing service management in federated e-Infrastructures“ (FedSM), www.fitsm.itemo.org
Revisionsfähigkeit / revisionsfähig	2.2 5.5	Grundsätze zur ordnungsgemäßen Führung und Aufbewahrung von Büchern, Aufzeichnungen und Unterlagen in elektronischer Form sowie zum Datenzugriff (GoBD)	BMF, www.bundesfinanzministerium.de | GoBD
		Grundsätze ordnungsmäßiger Buchführung bei Einsatz von Informationstechnologie (IDW RS FAIT 1)	IDW
		Grundsätze ordnungsmäßiger Buchführung beim Einsatz elektronischer Archivierungsverfahren (IDW RS FAIT 3)	IDW
		Abschlussprüfung bei Einsatz von Informationstechnologie (IDW PS 330)	IDW
		§ 9 BDSG i. V. m. der Anlage zu § 9 und vergleichbare Landesvorschriften	www.gesetze-im-internet.de | BDSG
Risikoanalysen/ Risikomanagement	2.3 3.2 4.1 4.3	BSI-Standard 100-3: Risikoanalyse auf der Basis von IT-Grundschutz	BSI, www.bsi.bund.de | 100-3
		BSI IT-Grundschutz-Kataloge	BSI, www.bsi.bund.de | Themen | IT-Grundschutz | Grundschutzkataloge
		Risikoanalyse bei automatisierten Verfahren im Haushalts-, Kassen- und Rechnungswesen	Verwaltungsvorschriften Nr. 6.6 zu §§ 70 bis 72 und 74 bis 80 BHO und vergleichbare Landesregelungen, z. B. www.verwaltungsvorschriften-im-internet.de | Zahlungen, Buchführung und Rechnungslegung

Stichwort	Zu Nr.	Norm, Standard, Empfehlung	Quelle, Bemerkung
Risikoanalysen/ Risikomanagement		Dokumentation der Risikoanalyse	Nr. 7 der Bestimmungen über die Mindestanforderungen für den Einsatz automatisierter Verfahren im Haushalts-, Kassen- und Rechnungswesen des Bundes (BestMaVB - HKR) und entsprechende Landesregelungen, z. B. www.verwaltungsvorschriften-im-internet.de | BestMaVB-HKR
		Datenschutzrechtliche Regelungen zur Risikoanalyse	z. B. § 4 Abs. 2 Landesverordnung über die Sicherheit und Ordnungsmäßigkeit automatisierter Verarbeitung personenbezogener Daten (www.gesetze-rechtsprechung.sh.juris.de | DSVO) i. V. m. § 5 Abs. 3 Schleswig-Holsteinisches Gesetz zum Schutz personenbezogener Informationen (www.gesetze-rechtsprechung.sh.juris.de | LDSG) sowie vergleichbare Normen des Bundes und der anderen Länder
		Abschlussprüfung bei Einsatz von Informationstechnologie (IDW PS 330)	IDW
		Grundsätze ordnungsmäßiger Buchführung bei Einsatz von Informationstechnologie (IDW RS FAIT 1)	IDW
		Grundsätze ordnungsmäßiger Buchführung beim Einsatz elektronischer Archivierungsverfahren (IDW RS FAIT 3)	IDW
		Anforderungen an die Ordnungsmäßigkeit und Sicherheit IT-gestützter Konsolidierungsprozesse (IDW RS FAIT 4)	IDW
		Grundsätze ordnungsmäßiger Buchführung bei Auslagerung von rechnungslegungsrelevanten Prozessen und Funktionen einschließlich Cloud Computing (IDW RS FAIT 5)	IDW
		Informationssicherheits-Risikomanagement (ISO/IEC 27005)	DIN, ISO

Stichwort	Zu Nr.	Norm, Standard, Empfehlung	Quelle, Bemerkung
Risikoanalysen/ Risikomanagement		Risikomanagement - Vokabular	DIN, ISO
Schnittstelle	5.5	XML in der öffentlichen Verwaltung (XÖV)-Standardisierung	Koordinierungsstelle für IT-Standards (KoSIT), www.xoev.de | XÖV-Rahmenwerk CIO Bund, www.cio.bund.de | XÖV-Standardisierung
Sicherheit	4.3 5.5	siehe Informationssicherheit	
Softwareentwicklung	5.4	Projektmanagementmethoden V-Modell XT und V-Modell XT Bund	CIO Bund, www.cio.bund.de | V-Modell XT, www.cio.bund.de | V-Modell XT Bund
		Standards und Architekturen für E-Government-Anwendungen (SAGA) für die Bundesverwaltung und landesspezifische Regelungen und Vorgaben	IT-Rat Bund, Beschluss vom 03.11.2011, www.cio.bund.de | SAGA
		Unified Modeling Language (UML)	Object Management Group (OMG), www.uml.org (Startseite)
		Offene verteilte Verarbeitung - Vereinheitlichte Modellierungssprache (UML) (ISO/IEC 19501)	DIN, ISO
		Prozessmodellierung: Business Process Modeling Notation (BPMN)	OMG, www.bpmn.org (Startseite)
Test- und Freigabeverfahren	5.5	Die Prüfung von Softwareprodukten (IDW PS 880)	IDW
		Projektmanagementmethoden V-Modell XT und V-Modell XT Bund	CIO Bund, www.cio.bund.de | V-Modell XT Bund
		Informationsangebote der Datenschutzbeauftragten	z. B. Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein, www.datenschutzzentrum.de
Verbindliche Vereinbarungen	3.3	siehe IT-Service / IT-Servicemanagement	Service Level Agreement (SLA) Operational Level Agreement (OLA)

Stichwort	Zu Nr.	Norm, Standard, Empfehlung	Quelle, Bemerkung
Wirtschaftlichkeit und Sparsamkeit / Wirtschaftlichkeitsunter-suchung	2.1 2.3 4.3 5.1 5.2 5.3	Verwaltungsvorschriften zu § / Artikel 7 der Haushaltsordnungen des Bundes und der Länder	z. B. www.verwaltungsvorschriften-im-internet.de | VV-BHO
		Einführung in Wirtschaftlichkeitsuntersuchungen	BMF, www.verwaltungsvorschriften-im-internet.de | Wirtschaftlichkeitsuntersuchungen
		WiBe Fachkonzept IT	IT-Rat Bund, Anwendung für die Bundesverwaltung vorgesehen nach Beschluss vom 19.02.2015, www.cio.bund.de | WiBe Fachkonzept IT, ggf. landesspezifische Vorgaben.
		Anforderungen an Wirtschaftlichkeitsuntersuchungen finanzwirksamer Maßnahmen nach § 7 Bundeshaushaltsordnung	Gutachten des Beauftragten für die Wirtschaftlichkeit in der Verwaltung, Band 18, 2013, www.bundesrechnungshof.de | Band 18
		Quellen, Informationen und Einzelbeispiele	WiBe-Team, www.wibe.de | WiBe Quellen
		Erfolgskontrolle in der öffentlichen Verwaltung	Finanzministerium des Landes Mecklenburg-Vorpommern, www.regierung-mv.de | Erfolgskontrolle