Rechnungshöfe des
Bundes und der Länder

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

– Leitlinien und gemeinsame Maßstäbe für IT-Prüfungen –

(IT-Mindestanforderungen 2020)

Stand: August 2020

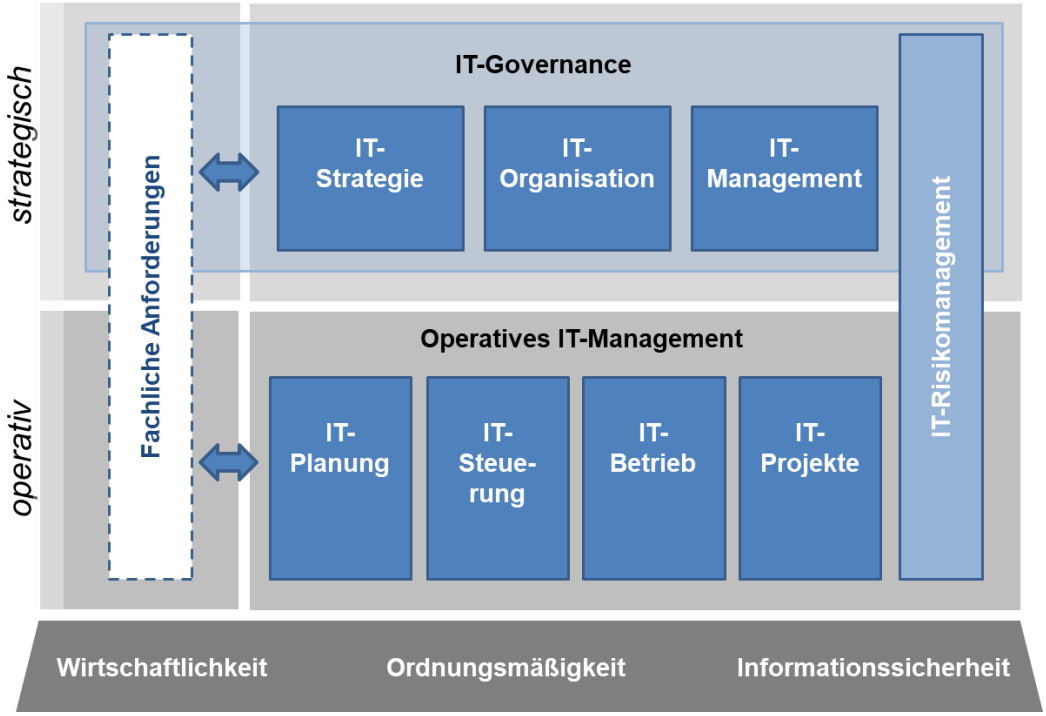
Inhaltsverzeichnis

Anlage:

Fundstellen zu Normen, Standards und Empfehlungen

1 Zweck der IT-Mindestanforderungen

Die IT-Mindestanforderungen[1] beschreiben die wesentlichen beim Einsatz der Informationstechnik (IT)[2] zu beachtenden Handlungsfelder.



Die IT-Mindestanforderungen benennen die grundlegenden Voraussetzungen für einen wirtschaftlichen, ordnungsgemäßen und sicheren IT-Einsatz. Sie basieren auf den Prüfungserkenntnissen der Rechnungshöfe des Bundes und der Länder und schaffen gemeinsame, transparente Prüfungsmaßstäbe. Vorschriften des Bundes oder der Länder bleiben unberührt. Für die Kommunen, Körperschaften, Anstalten und Stiftungen, die den Prüfungsrechten der Rechnungshöfe unterliegen, sind die IT-Mindestanforderungen entsprechend anzuwenden.

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.

[1] Bisher IuK-Mindestanforderungen genannt.

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

2 Grundlegende Anforderungen

2.1 Wirtschaftlichkeit

Nach den im Haushaltsrecht des Bundes und der Länder verankerten Grundsätzen 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 Änderungen bereits laufender Maßnahmen zu folgenden Zeitpunkten zu erstellen:

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 dargestellt sind,
- Ziele operationalisiert/konkretisiert werden,
- die zur Zielerreichung relevanten Lösungsmöglichkeiten betrachtet werden,
- sämtliche im Betrachtungszeitraum voraussichtlich entstehende Kosten – auch nicht haushaltswirksame – einbezogen werden,
- der Nutzen zu berücksichtigen ist, der von der 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.

Bei Maßnahmen innerhalb von *IT-Verbünden* sind neben der Gesamtwirtschaftlichkeit auch Auswirkungen auf die einzelnen Verbundpartner zu betrachten.

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, insbesondere der Gesetze, Haushaltsgrundsätze und Verwaltungsvorschriften.

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 Prüfungszwecke ist lesender Zugriff zu gewährleisten. Für elektronisch gespeicherte Daten sind sicherzustellen:

- Authentizität (Echtheit),
- Integrität (Unveränderlichkeit),
- Vollständigkeit und Nachvollziehbarkeit,
- Verfügbarkeit,
- Vertraulichkeit und Löschbarkeit (Datenschutz),
- Lesbarkeit und
- Verkehrsfähigkeit (Möglichkeit zur Übermittlung elektronischer Dokumente).

Dies gilt im gesamten Lebenszyklus, auch während der gesetzlichen Aufbewahrungsfristen (*Langzeitspeicherung*) und ggf. dauerhaft im Rahmen der *Archivierung*.

2.3 Informationssicherheit

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

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

führen können.

Die Gewährleistung der *Informationssicherheit* ist eine Daueraufgabe.

Zur Erreichung der grundlegenden Sicherheitsziele Vertraulichkeit, Integrität und Verfügbarkeit sind eine übergreifende Sicherheitsstrategie zu entwickeln und angemessene *Informationssicherheitsmanagementsysteme (ISMS)* zu unterhalten. Bei ebenen- und länderübergreifenden IT-Verfahren sowie bei der Absicherung der IT-Netzwerkinfrastruktur der öffentlichen Verwaltung ist bei allen Beteiligten ein einheitliches und angemessenes Mindest-Sicherheitsniveau zu gewährleisten.

Die Leitung der Behörden, Stellen und Einrichtungen ist für die *Informationssicherheit* in ihrem Geschäftsbereich verantwortlich. Sie hat die Maßnahmen und Prozesse des *Informationssicherheitsmanagements (ISM)* zu initiieren, zu steuern und zu überwachen. Die Leitung hat sicherzustellen, dass die hierfür erforderlichen finanziellen, personellen und zeitlichen Ressourcen zur Verfügung stehen.

Es ist ein/e Informationssicherheitsbeauftragte/r (ISB) zu benennen. Diese/r soll außerhalb des operativen IT-Managements angesiedelt sein, um Interessen- und Rollenkonflikte zu vermeiden. Für ressortübergreifende, strategische Aufgaben der Planung und Steuerung des ISM ist ein/e Gesamtverantwortliche/r für die Informationssicherheit zu benennen.

Die *Informationssicherheit* ist bei allen Geschäftsprozessen zu berücksichtigen. Die Organisation des Informationssicherheitsprozesses muss sich an den Aufgaben und Prozessen orientieren und nicht an den aufbauorganisatorischen Grenzen. Dabei sollten ebenen-, länder- und ressortübergreifende Kooperationen angestrebt werden.

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

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

Bei den Maßnahmen zur Informationssicherheit ist neben den Grundsätzen der Wirtschaftlichkeit und Sparsamkeit auch die Verhältnismäßigkeit zu beachten.

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

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

3 Strategische Anforderungen

3.1 IT-Governance

Die IT ist kein Selbstzweck. Sie hat sich an den Aufgaben und Zielen der öffentlichen Verwaltung auszurichten (*IT-Governance*). Die strategischen und organisatorischen Anforderungen für den Einsatz der IT leiten sich aus den Grundlagen für ein ordnungsgemäßes, sicheres und wirtschaftliches Verwaltungshandeln ab.

Als Bindeglied zwischen politischer Führung und *IT-Organisation* sollten beim Bund, den Ländern und den Kommunen Beauftragte für IT (beispielsweise Chief Information Officer - CIO[3]) bestellt werden. Ihnen fällt bei der Erstellung der *IT-Strategie*, der Planung der *IT-Organisation* und beim IT-Management eine zentrale Rolle zu.

3.2 IT-Strategie

Der ebenenübergreifende Handlungsrahmen für den IT-Einsatz in der öffentlichen Verwaltung 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 NEGS bündelt *gesellschaftliche und politische Ziele* des Bundes, der Länder und der Kommunen zur IT. Sie berücksichtigt insbesondere den übergreifenden IT-Einsatz zwischen Gebietskörperschaften und Verwaltungsebenen.

Politische Vorgaben und gesetzliche Anforderungen (beispielsweise NEGS, *E-Government*-Gesetze, Onlinezugangsgesetz (OZG)) sind von den Gebietskörperschaften zu konkretisieren (z. B. in einer *E-Government*-Strategie bzw. *Digitalisierung*sstrategie). Dafür sind die CIO verantwortlich.

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

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

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

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

Darüber hinaus sollte die IT-Strategie Aussagen zur Vermeidung technischer und wirtschaftlicher Abhängigkeiten von einzelnen Anbietern, zur Sicherung der Interoperabilität und zur Gewährleistung von Informationssicherheit und Datenschutz enthalten.

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, zu evaluieren und regelmäßig fortzuschreiben. Durch ein begleitendes *Akzeptanzmanagement* ist sicherzustellen, dass alle Beteiligten hinreichend eingebunden werden.

3.3 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 *Föderale IT-Kooperation* (FITKO) unterstützt den *IT-Planungsrat* bei der Aufgabenwahrnehmung.

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:

- grundsätzliche Zieldefinition in einer übergreifenden *IT-Strategie*,
- 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 geeigneter Werkzeuge,
- Organisation des *Informationssicherheitsmanagements* (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,
- Organisation des *IT-Controlling* einschließlich IT-*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-Beschaffung*en.

Darauf aufbauend haben die Dienststellen und Organisationseinheiten die IT-Aufgaben entsprechend der strategischen und organisatorischen Rahmenbedingungen wahrzunehmen. Bei der Wahrnehmung der IT-Aufgaben sollen nach dem Prinzip der Funktionstrennung

- die Definition der fachlichen Anforderung,
- deren IT-fachliche Entwicklung/Umsetzung,

- die *Freigabe* und
- die Betriebsverantwortung für die Informationssysteme

organisatorisch und personell getrennt werden.

Gemäß dem Prinzip „Strategie vor Prozess vor Struktur“ sollten aufbauorganisatorische Veränderungen erst nach Optimierung der Prozesse vorgenommen werden. Weitere Anforderungen an die *IT-Organisation* ergeben sich aus dem Grundsatzpapier der Rechnungshöfe des Bundes und der Länder für die Verwaltungsorganisation.

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

3.4 IT-Management

Die CIO und die Leitungen der Behörden, Stellen und Einrichtungen 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 Bediensteten 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*),
- Vorgaben zur Implementierung eines IT-*Risikomanagements* zu entwickeln.

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

4 Operative Anforderungen

4.1 Operative IT-Planung

Jede Verwaltungsebene muss auf Grundlage der übergeordneten und eigenen strategischen Anforderungen eine operative *IT-Planung* erstellen. Sie sollte ziel- und zukunftsorientiert, angemessen detailliert und aktuell sein. Zur operativen *IT-Planung* gehören:

- Bedarfsanalysen und generelles Anforderungsmanagement,
- Einführungsstrategien,
- Konzeptionen für Schulung und Anwenderbetreuung,
- Festlegungen zur *Informationssicherheit,*
- Aussagen zum Bedarf an Ressourcen: Haushaltsmittel (konsumtiv und investiv), Personal, Technik / Systeme, Infrastruktur,
- Regelungen zur *Bestandsführung* von Hardware, Software, Infrastrukturen,
- Festlegungen zum *Projekt*- und Programm*management*, die alle relevanten Teildisziplinen angemessen berücksichtigen, insbesondere das Termin-, Kosten- und *Risikomanagement,*
- Berücksichtigung der speziellen Erfordernisse bei *IT-Großprojekten*.

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

Die digitale Transformation führt zu einer weiteren Erhöhung der Abhängigkeit von IT sowie zu einer erheblichen Aufgabenmehrung in diesem Bereich. Um den Bedarf an IT-Fachkräften decken zu können, müssen Maßnahmen zur Gewinnung, Bindung und Entwicklung von IT-Personal ergriffen werden. Dazu zählen verstärkte Aus-, Fort- und Weiterbildung entsprechend der fachlichen Anforderungen und des technischen Fortschritts sowie eine gesteuerte Personalentwicklung.

Das IT-Personal muss für die Kernprozesse und eingesetzten Technologien angemessene Kompetenzen besitzen. Dies betrifft auch außerhalb der IT-Bereiche tätige Mitarbeiter, wie bspw. Informationssicherheits- und Datenschutzbeauftragte.

Das vorhandene IT-Personal muss effizient eingesetzt werden. Die Personalressourcen für die IT sind durch *Personalbedarfsberechnungen* zu ermitteln. Die Anforderungen ergeben sich aus den Leitsätzen der Rechnungshöfe des Bundes und der Länder für die Personalbedarfsermittlung. Der Personalbedarf und der Umfang des eingesetzten Personals sind in regelmäßigen Abständen zu überprüfen.

4.2 IT-Risikomanagement

Das IT-*Risikomanagement* umfasst alle Aktivitäten zur systematischen Erkennung, Analyse, Überwachung und Kontrolle von Risiken, die sich für Organisationen aus dem Einsatz von IT ergeben können. Die Vorgaben für das IT-*Risikomanagement* leiten sich aus dem organisationsweiten *Risikomanagement* ab.

Der kontinuierliche Prozess des *Risikomanagements* sollte in den folgenden Schritten ablaufen:

- Risiken identifizieren und in ihrer Art, ihren Ursachen und Auswirkungen beschreiben,
- Risiken bewerten (Eintrittswahrscheinlichkeit und Schadenshöhe ermitteln) und priorisieren,
- Maßnahmen zur Risikobehandlung bestimmen,
- Kosten mit den zu erwartenden Schäden vergleichen und Entscheidung für oder gegen die Umsetzung der Maßnahmen zur Risikobehandlung treffen,
- Restrisiko betrachten,

- Risiken überwachen, Maßnahmen zur Risikobehandlung durchführen und bei Bedarf anpassen.

4.3 Operative IT-Steuerung

Die operative IT-Steuerung beinhaltet kurz- bis mittelfristige Maßnahmen, um die Wirtschaftlichkeit, Ordnungsmäßigkeit und Informationssicherheit der IT-Organisation und -Prozesse zu gewährleisten.

Als Grundlage für die Kontrolle der Zielerreichung und Steuerung ist ein angemessenes *IT-Controlling* einzusetzen. Zu den Controlling-Bereichen zählen IT-Portfolio / IT-Masterplan, IT-Projekte, IT-Produkte, IT-Infrastrukturen und IT-Prozesse. Dabei sind insbesondere folgende Handlungsfelder zu berücksichtigen:

- Zieldefinitionen: Messbarkeit durch Leistungsindikatoren und *Kennzahlen* (*Metriken*), Festlegen entsprechender Zielgrößen,
- Information: Kontinuierliches Überwachen der Kennzahlen (Soll-Ist-Vergleich) und Kommunizieren der Ergebnisse,
- Analyse: Untersuchen von Soll-Ist-Abweichungen und Identifizieren von Optimierungspotenzialen.

Hilfsmittel hierfür sind u. a. der Aufbau eines Zielsystems, der Einsatz von Controlling-Software sowie die Etablierung eines zielorientierten Berichtswesens.

Gesteuert wird auf Basis der Ergebnisse des kontinuierlich durchgeführten *IT-Controllings*.

Zur Bewertung der Leistungsfähigkeit der eigenen IT-Organisation und -Prozesse können *Benchmarks* mit vergleichbaren Organisationen durchgeführt oder *Reifegradmodelle* angewendet werden.

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

4.4 IT-Betrieb

Unter Beachtung von *Wirtschaftlichkeit*, Ordnungsmäßigkeit und *Informationssicherheit* ist der *IT-Betrieb* service- und kundenorientiert auszurichten. Standardisierte Lösungen sind anzustreben. Neue technologische Entwicklungen sollten angemessen berücksichtigt werden.

Beim Erbringen von IT-Diensten ist ein angemessenes *IT-Servicemanagement* anzuwenden. In dieses sind die Prozesse des Informationssicherheitsmanagements einzubetten. Vorgaben aus der IT-Steuerung sind dabei umzusetzen.

Die erforderliche Dienstgüte soll in einem verbindlichen Vertrag zwischen dem Auftraggeber und dem internen oder externen Auftragnehmer vereinbart werden (*Operational Level Agreement* – *OLA*, *Service Level Agreement* – *SLA*). Die IT-Betriebskosten sollen identifiziert, erfasst, überwacht, bewertet und den IT-Diensten verursachungsgerecht zugeordnet werden.

Alle erforderlichen Informationen über die IT-Komponenten und deren Beziehungen untereinander sind zentral und strukturiert vorzuhalten und zu pflegen, z. B. in einer *Configuration Management Database* (CMDB). Die vorgehaltenen Daten müssen den aktuellen Bestand der IT-Komponenten widerspiegeln.

Der *IT-Betrieb* ist ständig mit geeigneten und angemessenen Methoden zu überwachen und zu dokumentieren. Über- oder Unterkapazitäten sind zu vermeiden.

Über einen Service Desk sollten Nutzer Anfragen stellen und Störungen melden können. Störungen des IT-Betriebs müssen aufgezeichnet, klassifiziert, priorisiert, beseitigt und abgeschlossen werden. Ein vorausschauendes Problemmanagement soll auf Basis der aufgezeichneten Störungen Probleme identifizieren und untersuchen. Problemlösungen sind zu dokumentieren.

Backup-Konzepte und Notfallpläne als Bestandteile des *Informationssicherheitsmanagements* sollen die Verfügbarkeit der Services auch bei Störungen gewährleisten. Diese sind regelmäßig auf ihre Wirksamkeit hin zu überprüfen und fortzuschreiben.

Änderungen an laufenden Systemen werden durch ein standardisiertes Änderungs- und Freigabemanagement gesteuert und dokumentiert.

5 Anforderungen an IT-Projekte

5.1 Planung

Sollen Geschäftsprozesse durch IT unterstützt oder abgebildet werden (erstmalig oder auch wegen Erneuerung der IT), so sind diese vor der Planung zu analysieren und ggf. zu optimieren. Dabei sind neben den Fach- und IT-Bereichen die für Organisationsfragen zuständigen Stellen zu beteiligen. Bei behördenübergreifenden IT-Projekten sind Beteiligung und Verantwortung im Einzelnen zu regeln.

Zur Planung eines IT-Projekts[4] gehören

- die Festlegung der Ziele,
- eine Anforderungsanalyse einschließlich der bedarfs- und nutzergerechten IT-Ausstattung,
- die Kalkulation von Budget und Ressourcen,
- eine *Wirtschaftlichkeitsuntersuchung* sowie
- die Festlegung einer geeigneten *Projektmanagementmethodik*.

Das *Projektmanagement* sollte u. a. umfassen

- die Entscheidung über eine Projektorganisation,
- eine Zeitplanung,
- das *Qualitätsmanagement*,
- das *Risikomanagement* sowie
- das Kommunikations- und Veränderungsmanagement.

Bei der Planung sind insbesondere folgende Alternativen zu prüfen:

- der Einsatz von Standard-Produkten,
- die Übernahme von in anderen Organisationseinheiten vorhandenen Produkten,
- die *Entwicklung* durch eigene Mitarbeiter,

[4] IT-Projekte (auch bezeichnet als IT-Vorhaben, IT-Maßnahmen) umfassen die Konzeption, *Entwicklung*, Beschaffung und Einführung von IT-Verfahren, IT-Infrastruktur und IT-Diensten sowie wesentliche Änderungen im *IT-Betrieb*.

- die *Entwicklung* durch Externe und
- die Beteiligung an oder Initiierung von *IT-Verbünden*.

Sicherheitsanforderungen an Soft- und Hardware sollen schon während der Entwicklungsphase eines Produktes berücksichtigt werden.

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

5.2 Beschaffung

Bei der *Beschaffung* sind die Grundsätze der *Wirtschaftlichkeit und Sparsamkeit* zu beachten und die jeweils wirtschaftlichste Beschaffungsart (z. B. Kauf/Miete/Leasing, Dienst-/Werkvertrag) auszuwählen. Das niedrigste Angebot muss nicht immer das wirtschaftlichste sein. Wartung und Pflege sind zu berücksichtigen.

Die IT-Standardisierung sollte vorangetrieben werden. Zentrale Beschaffungsstellen können Einsparpotenziale realisieren, indem sie die Bedarfe bündeln. Bei der Vergabe sollten Beschaffungsvarianten des Vergaberechts wie z. B. Rahmenvereinbarungen und In-House-Vergaben geprüft sowie Nachhaltigkeits-Aspekte und Lebenszykluskosten berücksichtigt werden.

Bei der *IT-Beschaffung* sind insbesondere folgende Aufgaben wahrzunehmen:

- Lösungsalternativen in *Wirtschaftlichkeitsuntersuchungen* bewerten,
- Vergabewert und maßgeblichen EU-Schwellenwert nachvollziehbar ermitteln,[5]
- eindeutige und umfassende Leistungsbeschreibung einschließlich Dokumentationsvorgaben sowie der Rahmenbedingungen eines Test- und Abnahmeverfahrens erstellen,
- *Vergabeart* festlegen und *Vergabeverfahren* durchführen,
- Verträge gestalten, ggf. standardisierte *Vertragsmuster* auswählen,
- mit lieferantenbezogenen Risiken umgehen,

[5] Im Unterschwellenbereich gilt das Haushaltsrecht von Bund, Ländern und Gemeinden. Im Oberschwellenbereich sind die bundeseinheitlichen Regelungen, die die EU-Richtlinien umsetzen, anzuwenden.

- Leistungserbringung kontrollieren und steuern.

Bei der Beauftragung von IT-Dienstleistungen und dem *Einsatz Externer* kommen weitere Aufgaben hinzu, wie z. B.:

- Zulässigkeit und Erforderlichkeit der Beauftragung Externer prüfen,
- Probleme beschreiben und Ziele des Einsatzes Externer festlegen,
- Abhängigkeit von Externen vermeiden,
- Know-how-Transfer gewährleisten und
- nachvollziehbare Entscheidungen über Vertragsart (Werk-/Dienstvertrag) sowie Vertragsgestaltung, z. B. im Hinblick auf Reisekosten und -zeiten treffen.

Auch Sicherheitsbelange müssen angemessen berücksichtigt werden. Beratungsergebnisse dürfen nicht unreflektiert übernommen werden. Zur Steuerung der Externen und zum fachlichen Austausch muss auf Seiten der Auftraggeber entsprechendes Know-how vorhanden sein.

Werden Externe mit der *Entwicklung* von Software beauftragt, soll auch nach Vertragsende der Zugriff auf den aktuellen Quellcode sichergestellt werden. Auch sonstige wichtige Entwicklungsergebnisse sollen verfügbar sein. Die notwendigen *Nutzungsrechte* u. a. für den Quellcode und sonstige Ergebnisse sind zu vereinbaren.

Der Auftraggeber muss durch ein wirksames Management sicherstellen, dass die von Auftragnehmern erbrachten Leistungen seinen Anforderungen entsprechen und dabei Kosten, Nutzen und Risiken transparent bleiben.

5.3 Entwicklung, Test, Abnahme und Freigabe

Bei der *Entwicklung*[6] sind die Vorgaben (z. B. *Projektmanagement* / -organisation) aus Planung und ggf. Beschaffung umzusetzen und kontinuierlich anzuwenden. Dazu gehören u. a.:

- das Berichtswesen,
- das Bereitstellen notwendiger finanzieller und personeller Ressourcen,

[6] Der Begriff „*Entwicklung*“ umfasst sowohl die *Entwicklung* von Software und Systemen als auch die Anpassung von Standardprodukten.

- die Kontrolle von Teilzielen / Meilensteinen und
- das Überwachen des Budgets.

Die Anforderungen aus der Planung sind zu verifizieren. Dabei sollten auch die zukünftigen Nutzer beteiligt werden.

Die *Dokumentation* sollte aktuell und *revisionssicher* sein. Sie muss die Pflege, die Wartung und einen ordnungsgemäßen *IT-Betrieb* unterstützen sowie eine effektive und effiziente Nutzung durch die Anwender ermöglichen.

Die möglichst standardisierten und vorzugsweise quelloffenen *Schnittstellen* zu anderen Systemen und die spätere organisatorische Einbindung des Systems in den Betrieb sind zu beachten. Besonderer Wert ist auf die Dokumentation der *Schnittstellen* zu legen. Details des *Test- und Abnahmeverfahrens* sind zu regeln. Funktionale und nicht-funktionale Tests müssen nach festgelegten Testszenarien durchgeführt und dokumentiert werden. Die fachlich zuständigen Stellen haben hierfür Testfälle zu erstellen. Diese sollten auch komplexe Konstellationen mit umfassen. Die Migration ggf. zu übernehmender Daten ist einzubeziehen. Soweit ein IT-System von mehreren Organisationen eingesetzt werden soll, können eigene Tests mit Tests dieser anderen Organisationen kombiniert oder deren Testergebnisse berücksichtigt werden. Auch diese sind zu dokumentieren.

Die Ergebnisse des abschließenden Tests sind unter Beteiligung des IT-Bereichs von den am Vorhaben beteiligten Fachbereichen zu kontrollieren, zu bewerten und abzunehmen. Tests sollten nicht im produktiven System durchgeführt werden. Nur bei Vorliegen unabweisbarer Gründe kann davon abgewichen werden. Die sich hieraus ergebenden Risiken müssen bewertet und dokumentiert werden. Insbesondere die Ergebnisse des Abschlusstests sind *revisionssicher* zu dokumentieren.

Bei komplexen IT-Systemen können Teilsysteme nach deren Test und Abnahme vorab in Betrieb genommen werden. Nach Fertigstellung des Gesamtsystems muss ein umfassender Abschlusstest durchgeführt und die Gesamtabnahme erklärt werden.

Es ist zu prüfen, ob gesetzliche Vorgaben oder andere Richtlinien eine *Freigabe* erfordern und welche notwendigen Voraussetzungen dafür sicherzustellen sind.

5.4 Inbetriebnahme

Für die Inbetriebnahme ist insbesondere rechtzeitig zu gewährleisten, dass

- alle notwendigen rechtlichen Voraussetzungen vorliegen,
- die Einführungsstrategie festgelegt ist,
- das neue IT-System in das *IT-Servicemanagement* und die *Informationssicherheit*skonzeption eingebunden wurde,
- die erforderliche Hard- und Softwareumgebung eingerichtet ist,
- die notwendigen Datenbestände übernommen wurden und
- die Benutzer bedarfsgerecht und zeitnah geschult werden.

Eine im Umfang angemessene und auf den Nutzer ausgerichtete Dokumentation ist bereitzustellen.

Bei der Einführung sind die Aspekte des organisationalen Wandels und des *Akzeptanzmanagements* zu beachten. Für eine fortlaufende Beratung und Schulung der Nutzer muss Vorsorge getroffen werden.

Als Bestandteil der *Erfolgskontrolle* ist eine abschließende *Wirtschaftlichkeitsuntersuchung* durchzuführen. Die Planung und *Entwicklung* als auch der Betrieb sollten nach angemessener Zeit evaluiert werden.

IT-Mindestanforderungen

Anlage:
Fundstellen zu Normen, Standards und Empfehlungen

August 2020

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

Die nachfolgenden 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 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.

Sollte ein Link nicht mehr funktionieren, so kann mit den in der Spalte „Quelle, Bemerkung“ angegebenen Stichworten gesucht werden.

Stichworte

Stichwort	Zu Nr.	Norm, Standard, Empfehlung	Quelle, Bemerkung
A			
Agiles Projektmanagement	4.4		Agile Vorgehensweisen umfassen Maßnahmen, die ein schnelles Reagieren auf veränderte Anforderungen ermöglichen. Die Entwicklung erfolgt in vielen kleinen abgeschlossenen Zyklen, es findet eine verstärkte Kommunikation zwischen den Beteiligten statt. Änderungen können auf diese Weise flexibel in den Entwicklungsprozess übernommen werden.
Akzeptanzmanagement	3.2 5.4		Planung und Durchführung von Maßnahmen, die bei Veränderungen von Arbeitsorganisation oder -prozessen darauf ausgerichtet sind, möglichst frühzeitig alle Interessensgruppen und Betroffenen über den Veränderungsprozess zu informieren und daran zu beteiligen.
Arbeitsschutz	2.2	Arbeitsschutzgesetz (ArbSchG)	www.gesetze-im-internet.de | ArbSchG
		Verordnung über Arbeitsstätten (ArbStättV), Anlage Nr. 6 - Maßnahmen zur Gestaltung von Bildschirmarbeitsplätzen	www.gesetze-im-internet.de | ArbStättV
Archivierung	2.2		Zeitraum nach Abschluss der Langzeitspeicherung
		Grundsätze zur ordnungsmäßigen 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 (Informationssicherheit)	2.3	Informationstechnik - IT-Sicherheitsverfahren - Informationssicherheits-Managementsysteme - Anforderungen (DIN ISO/IEC 27001)	Deutsches Institut für Normung e. V. (DIN), International Organization for Standardization (ISO)

Stichwort	Zu Nr.	Norm, Standard, Empfehlung	Quelle, Bemerkung
		IT-Grundschutz	Bundesamt für Sicherheit in der Informationstechnik (BSI), www.bsi.bund.de | Themen | IT-Grundschutz
		Informationssicherheitsmanagementsystem in 12 Schritten (ISIS12)	Bayerischer IT-Sicherheitscluster e.V., https://isis12.it-sicherheitscluster.de/
Audits (Prozesse)	4.2	Qualitätsmanagementsysteme - Grundlagen und Begriffe (DIN EN ISO 9000)	DIN, ISO
		Informationstechnik - Prozessbewertung (Normenfamilie ISO/IEC 3300x)	DIN, ISO
		Reifegradmodell der Softwareentwicklung - Capability Maturity Model Integration (CMMI)	CMMI Institute, www.cmmiinstitute.com (englisch)
		siehe Rahmenwerke, COBIT	
		Change-Management nach ITIL, siehe Rahmenwerke, ITIL	
B			
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	5.2	Einsatz externer Berater in der Bundesverwaltung	Diverse Veröffentlichungen des Bundesrechnungshofs https://www.bundesrechnungshof.de | externe Berater
		Eckpunkte „Einsatz Externer in der Informationstechnik der Bundesverwaltung“ Empfehlungen zur Inanspruchnahme von externen Unterstützungsleistungen durch Bundesbehörden im IT-Bereich	IT-Rat Bund, Beschluss 2016/8 vom 29. Juni 2016, www.cio.bund.de | 2016/8
		Kriterien für die Nutzung von Cloud-Diensten der IT-Wirtschaft durch die Bundesverwaltung	IT-Rat Bund, Beschluss 2015/5 vom 29. Juli 2015, www.cio.bund.de | Cloud-Dienste

Stichwort	Zu Nr.	Norm, Standard, Empfehlung	Quelle, Bemerkung
Beschaffung	5.2	siehe IT-Beschaffung	
		Umfassende Liste von Normen und Rechtsgrundlagen	Beschaffungsamt des BMI, www.bescha.bund.de | Normen und Rechtsvorschriften
Bestandsführung	4.1	Buchführung und Rechnungslegung für das Vermögen und die Schulden des Bundes (VV-ReVuS)	BMF, www.bundesfinanzministerium.de | VV-ReVuS
		Information technology - IT asset management - Part 1: IT asset management systems - Requirements (ISO/IEC 19770-1:2017-12)	ISO
C			
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	IT-Planungsrat, www.it-planungsrat.de | Informationssicherheitsleitlinie
Configuration Management Database (CMDB)	4.4		Die CMDB ist ein Speicherort für Daten über alle Betriebsmittel der IT (Configuration Items - CIs).
		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.eu | FitSM Standard | Downloads
		siehe Rahmenwerke, ITIL	
		Spezifikationen und für IT Service Management (Normenreihe ISO/IEC 20000)	DIN, ISO
D			
Datenaustausch	3.3	siehe auch Schnittstelle	
		Standards des IT-Planungsrats	IT-Planungsrat, www.it-planungsrat.de | Standards

Stichwort	Zu Nr.	Norm, Standard, Empfehlung	Quelle, Bemerkung
		Koordinierungsstelle für IT-Standards (KoSIT)	KoSIT, www.xoev.de (Startseite)
Datenschutz	2.2	Bundesdatenschutzgesetz (BDSG), und entsprechende Ländergesetze	www.gesetze-im-internet.de | BDSG
		Standard-Datenschutzmodell 2.0	Abrufbar auf den Seiten der Datenschutzbeauftragten des Bundes und der Länder, z. B. www.datenschutz-mv.de | Datenschutzmodell
		Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung)	ABl. L 119 vom 04.05.2016 www.eur-lex.europa.eu | DSGVO
		IT-Grundschutz Grundschutzkompendium Baustein CON.2: Datenschutz	BSI, www.bsi.bund.de | CON.2
		Orientierungshilfen der Beauftragten für den Datenschutz zu verschiedenen Themen	Abrufbar auf den Seiten der Datenschutzbeauftragten des Bundes und der Länder
Digitalisierung	3.2	siehe gesellschaftliche und politische Ziele	
Dokumentation	2.2 5.3	Grundsatz der Schriftlichkeit (Aktenmäßigkeit)	Online-Verwaltungslexikon, www.olev.de | Schriftlichkeit
		Grundsätze zur ordnungsmäßigen 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 | GGO
		Registraturrichtlinie für das Bearbeiten und Verwalten von Schriftgut in Bundesministerien und vergleichbare Landesvorschriften	BMI, www.bmi.bund.de | Registraturrichtlinie

Stichwort	Zu Nr.	Norm, Standard, Empfehlung	Quelle, Bemerkung
		DIN ISO 15489-1 Information und Dokumentation - Schriftgutverwaltung	DIN
		Verwaltungsvorschriften für Zahlungen, Buchführung und Rechnungslegung (§§ 70 bis 72, 74 bis 80 BHO des Bundes und der Länder)	Kompetenzzentrum für das Kassen- und Rechnungswesen des Bundes (KKR), www.kkr.bund.de | Zahlungen Buchführung
		IT-Grundschutz Grundschutzkompendium OPS.1.1.3.M11 - Kontinuierliche Dokumentation der Informationsverarbeitung	BSI, www.bsi.bund.de | OPS.1.1.3.M11
E			
E-Akte / elektronische Dokumente	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
		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
		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	
Entwicklung	5.1 5.2 5.3 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

Stichwort	Zu Nr.	Norm, Standard, Empfehlung	Quelle, Bemerkung
		Föderales Informationsmanagement mit den Bausteinen - Leistungen, - Datenfelder und - Prozesse	FIM-Portal; www.fimportal.de (Startseite)
		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)
Erfolgskontrolle	2.1 5.4	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
		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	Verordnung über Arbeitsstätten (ArbStättV), Anlage Nr. 6 - Maßnahmen zur Gestaltung von Bildschirmarbeitsplätzen	www.gesetze-im-internet.de | ArbStättV
		Normenreihe DIN EN ISO 9241-210 „Menschzentrierte Gestaltung interaktiver Systeme”	DIN, ISO
		Veröffentlichungen der Bundesanstalt für Arbeitsschutz und Arbeitsmedizin	www.baua.de | Softwareergonomie

Stichwort	Zu Nr.	Norm, Standard, Empfehlung	Quelle, Bemerkung
F			
Föderale IT-Kooperation (FITKO)	3.3	Gesetz zum Ersten IT-Änderungsstaatsvertrag	www.gesetze-im-internet.de | GGArt91cÄndVtr1G
		Beschlüsse des IT-Planungsrates zur Errichtung einer Anstalt des öffentlichen Rechts (AöR) in gemeinsamer Trägerschaft aller Länder und des Bundes mit Sitz in Frankfurt am Main zum 1. Januar 2020	IT-Planungsrat, www.it-planungsrat.de | FITKO FITKO www.fitko.de (Startseite)
Freigabe	3.3 5.3	Informationsangebote der Datenschutzbeauftragten	z. B. Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein, www.datenschutzzentrum.de (Startseite)
		Bestimmungen über die Mindestanforderungen für den Einsatz automatisierter Verfahren im Haushalts-, Kassen- und Rechnungswesen des Bundes (BestMaVB - HKR) und entsprechende Landesregelungen,	www.verwaltungsvorschriften-im-internet.de | BestMaVB-HKR
G			
gesellschaftliche und politische Ziele	3.2	Digitalstrategie der EU Gestaltung der digitalen Zukunft Europas	Europäische Kommission, www.ec.europa.eu | Deutsch | Ein Europa für das digitale Zeitalter
		Nationale E-Government-Strategie	IT-Planungsrat, www.it-planungsrat.de | NEGS
		Digitalstrategie der Bundesregierung und vergleichbare Landesvorschriften	Bundesregierung, www.bundesregierung.de | Digitalisierung
		Gesetz zur Verbesserung des Onlinezugangs zu Verwaltungsleistungen (Onlinezugangsgesetz - OZG)	www.gesetze-im-internet.de | OZG
I			
Informationssicherheit	2.2 2.3 3.3 4.1 5.4	Leitlinie für die Informationssicherheit in der öffentlichen Verwaltung	IT-Planungsrat, www.it-planungsrat.de | Informationssicherheitsleitlinie

Stichwort	Zu Nr.	Norm, Standard, Empfehlung	Quelle, Bemerkung
		Cyber-Sicherheitsstrategie für Deutschland	BMI; www.bmi.bund.de | Cyber-Sicherheitsstrategie
		Umsetzungsplan Bund, Leitlinie für Informationssicherheit in der Bundesverwaltung und vergleichbare Regelungen der Länder	BMI; https://www.bmi.bund.de | Umsetzungsplan Bund
		Standards des BSI	BSI, www.bsi.bund.de | Standards
		IT-Grundschutz Kompendium einschließlich Umsetzungshinweise	BSI, www.bsi.bund.de | IT-Grundschutz-Kompendium
		Mindeststandards Bund des BSI nach § 8 Abs. 1 Satz 1 BSIG	BSI, www.bsi.bund.de | Mindeststandards 8 BSIG
		BSI IT-Grundschutz-Profile (z. B. für oberste Landesbehörden und Kommunen)	BSI, www.bsi.bund.de | "Übersicht veröffentlichter IT-Grundschutz-Profile"
		Leitfaden zur Basis-Absicherung nach IT-Grundschutz	BSI, www.bsi.bund.de | Leitfaden Basisabsicherung
		Informationssicherheitsrevision - Ein Leitfaden für die IS-Revision auf Basis von IT-Grundschutz -	BSI, www.bsi.bund.de | Leitfaden IS-Revision
		Leitlinie zur Internet-Sicherheit	BSI, www.bsi.bund.de | Internet-Sicherheit (ISi-Reihe)
		Technische Richtlinien des BSI	www.bsi.bund.de | Technische Richtlinien
		Grundsatzpapier zum Informationssicherheitsmanagement mit Fragenkatalog	Rechnungshöfe des Bundes und der Länder, z. B. www.bundesrechnungshof.de | Grundsatzpapier Informationssicherheitsmanagement
		Informationssicherheitsmanagementsystem in 12 Schritten (ISIS12)	Bayerischer IT-Sicherheitscluster e.V., https://isis12.it-sicherheitscluster.de/
		Sicherheit für Kommunen in Schleswig-Holstein (SiKoSH)	www.itvsh.de | SiKoSH

Stichwort	Zu Nr.	Norm, Standard, Empfehlung	Quelle, Bemerkung
		ISK.RLP Informationssicherheit bei den kommunalen Verwaltungen in Rheinland-Pfalz	www.securion.de (Startseite)
		Informationstechnik - IT-Sicherheitsverfahren - Informationssicherheits-Managementsysteme - Anforderungen (DIN ISO/IEC 27001)	DIN, ISO
		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 for Information Security	Information Security Forum, www.securityforum.org | ISF Standard of Good Practice for Information Security (englisch)
Informationssicherheits-management (ISM)	2.3 3.3		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., https://isis12.it-sicherheitscluster.de/
Internes Kontrollsystem (IKS)	2.2	Empfehlungen für Interne Revisionen in der Bundesverwaltung	BMI, www.bmi.bund.de | Interne Revisionen

Stichwort	Zu Nr.	Norm, Standard, Empfehlung	Quelle, Bemerkung
		Grundsätze zur ordnungsmäßigen 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
		Informationssicherheitsrevision - Ein Leitfaden für die IS-Revision auf Basis von IT-Grundschutz -	BSI, www.bsi.bund.de | Leitfaden IS-Revision
		siehe Rahmenwerke, COBIT	
		Standards und Grundsätze der Finanzkontrolle	Internationale Organisation der Obersten Rechnungskontrollbehörden (INTOSAI), www.intosai.org | ISSAI 100 bis 400
IT-Beschaffung	3.3 5.2	Unterlage für Ausschreibung und Bewertung von IT-Leistungen (UfAB)	CIO Bund, www.cio.bund.de | UfAB
		Ergänzende 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
		Zentralstelle für IT-Beschaffung des Bundes	Beschaffungsamt des BMI, www.bescha.bund.de | Beschaffung | Zentralstelle für IT-Beschaffung

Stichwort	Zu Nr.	Norm, Standard, Empfehlung	Quelle, Bemerkung
IT-Betrieb	3.3 4.1 4.3 5.3	siehe IT-Servicemanagement	
IT-Controlling	3.3 3.4 4.2	siehe Rahmenwerke, COBIT	
		Informationstechnik - Unternehmensführung in der Informationstechnik (ISO/IEC 38500)	DIN, ISO
IT-Governance	3.1	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	3.1 3.3	Handbuch für Organisationsuntersuchungen und Personalbedarfsermittlung (Organisationshandbuch) Organisationshandbuch neu (in Erstellung)	BMI, www.orghandbuch.de (Startseite)
		Grundsatzpapier der Rechnungshöfe des Bundes und der Länder für die Verwaltungsorganisation	Rechnungshöfe des Bundes und der Länder, z. B. www.bundesrechnungshof.de | Verwaltungsorganisation
		Leitsätze für die Personalbedarfsermittlung	Rechnungshöfe des Bundes und der Länder, z. B. www.bundesrechnungshof.de | Personalbedarfsermittlung
IT-Planung	4.1	siehe Rahmenwerke, COBIT	
		siehe Rahmenwerke, ITIL	

Stichwort	Zu Nr.	Norm, Standard, Empfehlung	Quelle, Bemerkung
		IT-Rahmenkonzept des Bundes und vergleichbare Landesregelungen /-vorgaben	z. B. CIO Bund, www.cio.bund.de | Strategische Themen | IT-Steuerung Bund
IT-Planungsrat	3.2 3.3	Beschlüsse und Empfehlungen des IT-Planungsrates des Bundes und der Länder (IT-Planungsrat)	IT-Planungsrat www.it-planungsrat.de | Entscheidungen
IT-Service / IT-Servicemanagement	3.3 4.4 5.4		IT-Servicemanagement (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.eu | Downloads
		Spezifikationen und Empfehlungen 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
		siehe Operational Level Agreement (OLA), Service Level Agreement (SLA)	
IT-Strategie	3.1 3.2 3.3 3.4	IT-Strategie Bund oder vergleichbare Grundlagen in den Ländern	IT-Rat Bund, Beschluss vom 19.01.2017, www.cio.bund.de | IT-Strategie Bund
IT-Systemarchitekturen	3.3	Architekturrichtlinie für die IT des Bundes	BMI, www.cio.bund.de | Architekturrichtlinie

Stichwort	Zu Nr.	Norm, Standard, Empfehlung	Quelle, Bemerkung
IT-Verbund	2.1 3.2 5.1		Insbesondere zum gemeinsamen Einkauf, zur Entwicklung, zur Pflege und zum Betrieb von Software haben sich IT-Verbünde, IT-Kooperationen und sonstige Formen der Zusammenarbeit der öffentlichen Verwaltung zwischen Bund, Ländern und Kommunen etabliert. Beispiele sind der Entwicklungsverbund KONSENS, die IT-Verbünde der Justiz sowie die Projekte und Anwendungen des IT-Planungsrats.
		Gutachten zur Evaluierung der Kieler Beschlüsse	IT-Planungsrat, Beschluss vom 16.10.2014 www.it-planungsrat.de | evakb
		Leitfaden zur Gestaltung von Softwarekooperationen vom 20.08.2014	IT-Planungsrat, Beschluss vom 16.10.2014 www.it-planungsrat.de | Leitfaden Softwarekooperationen
		Handreichung „IT-Verbünde und IT-Kooperationen“ der Rechnungshöfe des Bundes und der Länder vom Mai 2020	Rechnungshöfe des Bundes und der Länder, z. B. www.bundesrechnungshof.de | Handreichung IT-Verbünde und IT-Kooperationen
K			
Kennzahlen, Metriken	3.2 3.4 4.2	siehe Rahmenwerke, COBIT	
		siehe Rahmenwerke, ITIL	
L			
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

Stichwort	Zu Nr.	Norm, Standard, Empfehlung	Quelle, Bemerkung
		Ergebnisse des Projekts NaLa - Nationale Langzeitspeicherung	IT-Planungsrat, www.it-planungsrat.de | NaLa
N			
Nutzungsrechte	5.2	siehe IT-Beschaffungen, EVB-IT	
O			
Operational Level Agreement (OLA), Service Level Agreement (SLA)	4.4	siehe IT-Service / IT-Servicemanagement	Ein OLA ist eine dokumentierte Vereinbarung zwischen einem Service-Provider und einem anderen Teil der Organisation des Service Providers über die Bereitstellung einer Servicekomponente oder eines unterstützenden Service, die / der erforderlich ist, um Services für Kunden erbringen zu können. Ein SLA ist eine dokumentierte Vereinbarung zwischen einem Kunden und einem Service-Provider, die den zu erbringenden Service und die Serviceziele, die der Bereitstellung des Service zugrunde gelegt werden, spezifiziert.
P			
Personalbedarfsberechnung	4.1	Handbuch für Organisationsuntersuchungen und Personalbedarfsermittlung (Organisationshandbuch) Organisationshandbuch neu (in Erstellung)	BMI, www.orghandbuch.de (Startseite)
		Leitsätze für die Personalbedarfsermittlung	Rechnungshöfe des Bundes und der Länder, z. B. www.bundesrechnungshof.de | Personalbedarfsermittlung
Projektmanagement	3.3 4.1 5.1 5.3	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
		Praxisleitfaden „Projektmanagement für die öffentliche Verwaltung“	BMI https://www.bmi.bund.de | Praxisleitfaden Projektmanagement

Stichwort	Zu Nr.	Norm, Standard, Empfehlung	Quelle, Bemerkung
		Projects in Controlled Environments (PRINCE2)	AXELOS (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
		siehe Agiles Projektmanagement	
Q			
Qualität / Qualitätsmanagement	3.3 5.1	Qualitätsmanagementsysteme - Grundlagen und Begriffe (DIN EN ISO 9000)	DIN, ISO
R			
Rahmenwerke	3.4	Spezifikationen und Empfehlungen für IT Service Management (Normenreihe ISO/IEC 20000)	DIN, ISO
		IT Infrastructure Library (ITIL)	IT Service Management Forum (itSMF), AXELOS (englisch)
		COBIT	Information Systems Audit and Control Association (ISACA), Internationaler Berufsverband von IT-Revisoren, -Sicherheitsmanagern und -Experten, www.isaca.org | COBIT
		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.eu | Downloads
Reifegradmodelle / Benchmarking	4.3	Capability Maturity Model Integration (CMMI) - Familie von Referenzmodellen für unterschiedliche Anwendungsgebiete	CMMI Institute, www.cmmiinstitute.com (englisch)

Stichwort	Zu Nr.	Norm, Standard, Empfehlung	Quelle, Bemerkung
		ISO / IEC 3300x Information Technology - Process assessment	ISO
Revisionsfähigkeit / revisionsfähig	2.2 5.3	Grundsätze zur ordnungsmäßigen 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 3.3 3.4 4.1 4.2 5.1	BSI-Standard 200-3: Risikomanagement	BSI, www.bsi.bund.de | 200-3
		Risikoanalyse bei automatisierten Verfahren im Haushalts-, Kassen- und Rechnungswesen	Verwaltungsvorschriften Nr. 6.3 zu §§ 70 bis 72 und 74 bis 80 BHO und vergleichbare Landesregelungen, z. B. www.verwaltungsvorschriften-im-internet.de | Zahlungen, Buchführung und Rechnungslegung
		Dokumentation der Risikoanalyse	Nr. 6 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

Stichwort	Zu Nr.	Norm, Standard, Empfehlung	Quelle, Bemerkung
		COBIT 5 for Risk, COBIT 2019	ISACA
		DIN ISO 31000 - Risikomanagement - Leitlinien	DIN, ISO
		COSO ERM – Enterprise Risk Management Framework	The Committee of Sponsoring Organizations of the Treadway Commission
		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
		Risikomanagement - Vokabular	DIN, ISO
S			
Schnittstelle	3.2 5.3	Standards in der öffentlichen Verwaltung	Koordinierungsstelle für IT-Standards (KoSIT), www.xoev.de | XÖV-Rahmenwerk
Schutzbedarfsanalyse	2.3	siehe Informationssicherheit, IT-Grundschutz	

Stichwort	Zu Nr.	Norm, Standard, Empfehlung	Quelle, Bemerkung
T			
Test- und Abnahmeverfahren	5.3	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
		siehe IT-Beschaffung, EVB-IT	
V			
verbindliche Vereinbarungen	3.4 4.4	siehe IT-Service / IT-Service Management	
Vergabeart	5.2	siehe Beschaffung und IT-Beschaffung	
Vergabeverfahren	5.2	siehe Beschaffung und IT-Beschaffung	
Vertragsmuster		siehe IT-Beschaffung, EVB-IT	
W			
Wirtschaftlichkeit und Sparsamkeit / Wirtschaftlichkeitsunter-suchung	2.1 2.3 4.3 5.1 5.2 5.4	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 5.0, Konzept zur Durchführung von Wirtschaftlichkeitsbetrachtungen in der Bundesverwaltung, insbesondere beim Einsatz der 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.

Stichwort	Zu Nr.	Norm, Standard, Empfehlung	Quelle, Bemerkung
		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