

# BWV

---

**Bundesbeauftragter für Wirtschaftlichkeit in der Verwaltung**

**Datenverarbeitung in der Bundesverwaltung II**  
Prüfung der Informationstechnik in der öffentlichen Verwaltung  
nach den Mindestanforderungen der Rechnungshöfe  
des Bundes und der Länder

{Bundesadler}

**BWV Schriftenreihe Band 5**

**1. Auflage**

---

{Kohlhammer}

{Umschlag I}

{Umschlag II}

Bisher sind in der Schriftenreihe des Bundesbeauftragten für Wirtschaftlichkeit in der Verwaltung im gleichen Verlag erschienen:

Band 1

**Personal- und Organisationsaufgaben in der öffentlichen Verwaltung  
am Beispiel oberster Bundesbehörden**

Gutachten des Präsidenten des Bundesrechnungshofes als Bundesbeauftragter für  
Wirtschaftlichkeit in der Verwaltung  
abgeschlossen im Oktober 1987

2. Auflage, 1988

Band 2

**Erfolgskontrolle finanzwirksamer Maßnahmen in der öffentlichen Verwaltung**

Gutachten des Präsidenten des Bundesrechnungshofes als Bundesbeauftragter für  
Wirtschaftlichkeit in der Verwaltung  
abgeschlossen im Juni 1989

1. Auflage, 1989

Band 3

**Datenverarbeitung in der Bundesverwaltung**

Feststellungen des Bundesrechnungshofes und Hinweise des Präsidenten des  
Bundesrechnungshofes als Bundesbeauftragter für Wirtschaftlichkeit in der Verwaltung  
zu Mängeln und Risiken beim Einsatz der Informationstechnik

2. Auflage, 1993

Band 4

**Typische Mängel bei der Ermittlung des Personalbedarfs  
in der Bundesverwaltung**

Gutachten des Präsidenten des Bundesrechnungshofes als Bundesbeauftragter für  
Wirtschaftlichkeit in der Verwaltung  
abgeschlossen im März 1991

2. Auflage, 1993

ISBN 3-17-012820-5

{Umschlag IV}

Schriftenreihe  
des Bundesbeauftragten für  
Wirtschaftlichkeit in der Verwaltung  
Band 5

## Datenverarbeitung in der Bundesverwaltung II

Hinweise des Präsidenten des Bundesrechnungshofes als Bundesbeauftragter für Wirtschaftlichkeit in der Verwaltung für die Prüfung der Informationstechnik in der öffentlichen Verwaltung nach den Mindestanforderungen der Rechnungshöfe des Bundes und der Länder zum Einsatz der Informationstechnik  
(IT-Prüfungshinweise)

**Verlag W. Kohlhammer**  
**Stuttgart Berlin Köln**

## Die Deutschen Bibliothek - CIP-Einheitsaufnahme

**Datenverarbeitung in der Bundesverwaltung** : Hinweise des Präsidenten des Bundesrechnungshofes als Bundesbeauftragter für Wirtschaftlichkeit in der Verwaltung für die Prüfung der Informationstechnik in der öffentlichen Verwaltung nach den Mindestanforderungen der Rechnungshöfe des Bundes und der Länder zum Einsatz der Informationstechnik (IT-Prüfungshinweise) / [Hrsg.: Der Präsident des Bundesrechnungshofes als Bundesbeauftragter für Wirtschaftlichkeit in der Verwaltung]. - Stuttgart ; Berlin ; Köln : Kohlhammer.

Früher mit dem Zusatz zum Hauptsacht.: Feststellungen des Bundesrechnungshofes und Hinweise des Präsidenten des Bundesrechnungshofes als Bundesbeauftragter für Wirtschaftlichkeit in der Verwaltung zu Mängeln und Risiken beim Einsatz der Informationstechnik

2. Prüfung der Informationstechnik in der öffentlichen Verwaltung nach den Mindestanforderungen der Rechnungshöfe des Bundes und der Länder. - 1. Aufl. - 1993

(Schriftenreihe des Bundesbeauftragten für Wirtschaftlichkeit in der Verwaltung ; Bd. 5)  
ISBN 3-17-013820-5

NE: Deutschland / Bundesrechnungshof: Schriftenreihe des Bundesbeauftragten ...

Alle Rechte vorbehalten  
Herausgeber: Der Präsident des Bundesrechnungshofes  
als Bundesbeauftragter für Wirtschaftlichkeit  
in der Verwaltung, 60284 Frankfurt am Main  
Herstellung: Bonner Universitäts-Buchdruckerei  
Verlag: W. Kohlhammer GmbH, Stuttgart-Berlin-Köln

Verlagsort: Stuttgart  
Printed in Germany 1993

## Zum Geleit

Mit der Datenverarbeitung in der Bundesverwaltung befaßt sich bereits Band 3 der BWV-Schriftenreihe. Er enthält Feststellungen und Hinweise zu Mängeln und Risiken der Informationstechnik. Hieran schließt sich als zweite Veröffentlichung zum Thema Datenverarbeitung in der Bundesverwaltung der vorliegende Band 5 der Schriftenreihe an. Er beschäftigt sich mit der Prüfung des Einsatzes der Informationstechnik in der öffentlichen Verwaltung und den dabei zugrundezulegenden Maßstäben.

Die Präsidenten der Rechnungshöfe des Bundes und der Länder haben bei ihrer Konferenz im Mai 1991 in Bremerhaven neue Mindestanforderungen für die Beurteilung von Maßnahmen und Verfahren der Informationstechnik – IT-Mindestanforderungen – beschlossen.

Zur Vorbereitung dieser Neufassung sind unter Federführung des Bundesrechnungshofes die aus dem Jahre 1976 stammenden früheren Mindestanforderungen der Rechnungshöfe des Bundes und der Länder unter Berücksichtigung der technischen Entwicklung der letzten Jahre aktualisiert worden. Hierfür wurde unter Mitarbeit der Firma AGENS Consulting GmbH ausführliches Arbeitsmaterial erstellt. Dieses Arbeitsmaterial sowie die Erfahrungen aus Prüfungen des Bundesrechnungshofes und der beratenden Tätigkeit des Präsidenten des Bundesrechnungshofes als Bundesbeauftragter für Wirtschaftlichkeit in der Verwaltung sind in die im vorliegenden Band enthaltenen Hinweise für die Prüfung der Informationstechnik nach den IT-Mindestanforderungen – IT-Prüfungshinweise – eingeflossen.

Die Veröffentlichung in dieser Schriftenreihe soll dazu beitragen, die IT-Prüfungshinweise über den Kreis der mit Prüfungsaufgaben unmittelbar Betrauten hinaus nutzbar zu machen. Die bereits im Band 3 abgedruckten IT-Mindestanforderungen haben außerhalb der öffentlichen Verwaltung ein beachtliches Echo gefunden. Auch die IT-Prüfungshinweise in Band 5 können über die Verwaltung hinaus für IT-Verantwortliche in der Wirtschaft sowie für Vertragspartner und Lieferanten der öffentlichen Verwaltung von Interesse sein.

Die Hinweise sollen bei Prüfungen die Berücksichtigung der besonderen Aspekte der Informationsverarbeitung erleichtern und Anregungen für die Konzeption und Durchführung von IT-Prüfungen geben. Sie stellen keine grundsätzliche Erweiterung oder Einschränkung der IT-Mindestanforderungen dar und sie entbinden nach der Erfahrung des Bundesrechnungshofes den Prüfer nicht davon, in jedem Einzelfall festzustellen, inwieweit die vorgefundenen Verhältnisse tatsächlich zu Mängeln bei der Ordnungsmäßigkeit und Wirtschaftlichkeit führen.

Um die Umsetzung der Hinweise in konkrete Prüfungsansätze und die dabei mögliche Vielfalt der Vorgehensweise zu veranschaulichen, sind einige Beispiele für Stichwort- und Fragenkataloge aus der Prüfungspraxis des Bundesrechnungshofes und der Vorprüfstellen des Bundes im Anhang 5 abgedruckt.

Die anhaltende Nachfrage nach dem als Band 3 der Schriftenreihe veröffentlichten ersten Band zur Datenverarbeitung in der Bundesverwaltung führte inzwischen zur Herausgabe einer zweiten Auflage. Ich hoffe, daß auch der nun als Band 5 der Schriftenreihe



vorliegende zweite Band mit Hinweisen zur Prüfung der Informationstechnik ein solch reges Interesse finden möge.

Frankfurt am Main, im Juli 1993

*Dr. Heinz Günter Zavelberg*

*Präsident des Bundesrechnungshofes  
als Bundesbeauftragter für Wirtschaftlichkeit in der Verwaltung*

# Inhaltsübersicht

Seite

<b>Zum Geleit.....</b>	<b>3</b>
<b>Abkürzungen.....</b>	<b>7</b>
<b>Vorbemerkung.....</b>	<b>8</b>
<b>1 Allgemeines .....</b>	<b>9</b>
1.1 Anwendung der Mindestanforderungen .....	9
1.2 Informationstechnik (IT).....	10
1.3 Ziele des IT-Einsatzes .....	15
1.4 Dokumentation der IT .....	17
<b>2 Gesamtplanung und Koordinierung.....</b>	<b>20</b>
2.1 Gesamtplanung.....	20
2.2 Koordinierung des IT-Einsatzes .....	23
<b>3 IT-Vorhaben .....</b>	<b>25</b>
3.1 Allgemeines.....	25
3.2 Zuständigkeiten und Vorgehensweise.....	29
3.3 Vor- und Hauptuntersuchung .....	34
3.4 Ausführung eines IT-Vorhabens .....	38
3.4.1 Grundsätzliches .....	38
3.4.2 Beschaffung von Hard- und Software .....	39
3.4.3 Vergabe von Entwicklungsaufträgen.....	42
3.4.4 Entwicklung eines Verfahrens einschließlich Programmierung ..	44
3.4.5 Test und Freigabe.....	47
3.4.6 Einführung eines Verfahrens .....	51
3.5 Verfahrenspflege und -änderungen .....	55
<b>4 Betrieb von IT-Verfahren.....</b>	<b>58</b>
4.1 Grundsätzliches .....	58
4.2 Funktionentrennung und Verantwortlichkeiten .....	61
4.3 Verfahrensbetrieb bei Funktionentrennung.....	64
4.3.1 Datenerfassung und -eingabe .....	64
4.3.2 Arbeitsplanung und -vorbereitung.....	64
4.3.3 Datenverarbeitung .....	66
4.4 Verfahrensbetrieb bei eingeschränkter Funktionentrennung .....	68
4.5 Einsatz von Netzwerken .....	71
4.6 Einsatz von Datenbanksystemen .....	73

<b>5</b>	<b>Erfolgskontrolle.....</b>	<b>75</b>
<b>6</b>	<b>Qualitätssicherung .....</b>	<b>77</b>
<b>7</b>	<b>Sicherheit beim Einsatz der IT.....</b>	<b>78</b>
7.1	Allgemeines .....	78
7.2	Risikoanalyse und Sicherheitskonzept.....	81
7.3	Regelungen zur Sicherheit der IT.....	88
7.4	Notfallplanung und Notorganisation .....	92

#### Anhänge:

1	Verarbeitungsarten in der IT .....	95
2	IT-Funktionen und ihre Aufgaben .....	97
3	Methoden und Werkzeuge .....	101
4	Hinweise zu Wirtschaftlichkeitsbetrachtungen .....	108
5	Beispiele für Prüfungsansätze .....	114

# Abkürzungen

APC	Arbeitsplatzcomputer
BHO	Bundeshaushaltsordnung
BT-Drs.	Bundestagsdrucksache
BVB	Besondere Vertragsbedingungen für die Beschaffung und den Betrieb von DV-Leistungen
BWV	Der Bundesbeauftragte für Wirtschaftlichkeit in der Verwaltung
GMBI	Gemeinsames Ministerialblatt
HKR-ADV-Best (B)	Bestimmungen über den Einsatz von automatisierten Verfahren im Haushalts-, Kassen- und Rechnungswesen
Hrsg.	Herausgeber
IT	Informationstechnik
KBSt	Koordinierungs- und Beratungsstelle der Bundesregierung für Informationstechnik in der Bundesverwaltung im Bundesministerium des Innern
MinBIFin	Ministerialblatt des Bundesministeriums der Finanzen
Vorl.VV-BHO	Vorläufige Verwaltungsvorschriften zur BHO

## Vorbemerkung

Die "Mindestanforderungen, Grundsätze und Empfehlungen für die Durchführung von Projekten der automatisierten Datenverarbeitung, für die Anwendung automatisierter Verfahren im Haushalts-, Kassen- und Rechnungswesen und für die Aufzeichnung von Daten des Haushalts-, Kassen- und Rechnungswesens auf Bildträger" der Rechnungshöfe des Bundes und der Länder aus dem Jahre 1976 sind durch Beschluß der Konferenz der Präsidenten der Rechnungshöfe des Bundes und der Länder durch die Mindestanforderungen der Rechnungshöfe des Bundes und der Länder zum Einsatz der Informationstechnik (IT) – IT-Mindestanforderungen – vom Mai 1991 ersetzt worden.

Die nachfolgenden Hinweise für die Prüfung der IT nach den IT-Mindestanforderungen – IT-Prüfungshinweise – richten sich vor allem an IT-Prüfer sowie an Prüfer, die über Grundkenntnisse der Datenverarbeitung verfügen.

Die IT-Prüfungshinweise zeigen Kriterien auf, denen eine technische Realisierung im Hinblick auf die Ordnungsmäßigkeit, Wirtschaftlichkeit und Sicherheit in der Regel mindestens genügen sollte, und lassen die vielfältigen technischen und organisatorischen Möglichkeiten weitgehend offen, mit denen den IT-Mindestanforderungen Rechnung getragen werden kann. Diese Kriterien sind in einer Büroumgebung mit Einsatz von Arbeitsplatzcomputern (APC) anders auszuformen als in einem Rechenzentrum. Wenn typische Mängel genannt werden oder auf bestimmte Realisierungsmöglichkeiten hingewiesen wird, sind diese nur als beispielhaft anzusehen. Soweit erforderlich gehen die IT-Prüfungshinweise jeweils auf unterschiedliche organisatorische und technische Gegebenheiten ein.

Die Gliederung der IT-Prüfungshinweise folgt der Gliederung der IT-Mindestanforderungen. Jedem Abschnitt ist der entsprechende Text der IT-Mindestanforderungen (*in Kursivschrift*) vorangestellt. Die Verweise auf Textziffern beziehen sich – soweit nicht anders angegeben – auf die entsprechenden Textziffern der IT-Mindestanforderungen einschließlich der dazugehörenden Prüfungshinweise.

In Nr. 1 dieser Hinweise und in den Anhängen 1 bis 3 sind eine Reihe von begrifflichen Festlegungen getroffen worden, die das Verständnis der IT-Prüfungshinweise erleichtern sollen. Anhang 4 enthält darüber hinaus grundsätzliche Ausführungen zu Wirtschaftlichkeitsbetrachtungen in der IT. Anhang 5 gibt Beispiele für Stichwort- und Fragenkataloge wieder, die die Möglichkeiten der Anwendung der IT-Prüfungshinweise veranschaulichen sollen.

# 1 Allgemeines

## 1.1 Anwendung der Mindestanforderungen

1.1.1 *Die Rechnungshöfe des Bundes und der Länder legen bei ihrer Beurteilung von Maßnahmen und Verfahren auf dem Gebiet der Informationstechnik die nachfolgenden Mindestanforderungen zugrunde. Unbeschadet der Mindestanforderungen werden die Rechnungshöfe die jeweiligen Rechts- und Verwaltungsvorschriften (z. B. Bundes-/ Landeshaushaltsordnung einschl. VV wie etwa HKR-ADV-Bestimmungen, Besondere Vertragsbedingungen – BVB -, Personalvertretungsgesetz, Tarifverträge, Datenschutzgesetz) in ihre Prüfungen einbeziehen. Das Recht der Rechnungshöfe, diese Mindestanforderungen nach den Gegebenheiten ihrer jeweiligen Zuständigkeitsbereiche zu ergänzen, bleibt unberührt. Darüber hinaus behalten sie sich vor, diese Mindestanforderungen entsprechend den Prüfungsanforderungen durch gesonderte Hinweise zu konkretisieren.*

1.1.2 *Die IT-Mindestanforderungen ersetzen die ADV-Mindestanforderungen der Rechnungshöfe aus dem Jahre 1976.*

Die IT-Mindestanforderungen sind eine Beurteilungsgrundlage der Rechnungshöfe, mit der diese ihren Maßstab für die Prüfung und Bewertung von Maßnahmen der Verwaltung im Bereich der IT formulieren. Die Rechnungshöfe geben mit der Veröffentlichung der IT-Mindestanforderungen der Verwaltung Kriterien dafür an die Hand, wie nach ihrer Auffassung IT-Maßnahmen durchzuführen sind, wenn den Anforderungen der Ordnungsmäßigkeit, Wirtschaftlichkeit und Sicherheit in angemessener Weise Rechnung getragen wird. Bestehende Rechts- und Verwaltungsvorschriften bleiben unberührt.

Für den Einsatz von automatisierten Verfahren im Haushalts-, Kassen- und Rechnungswesen wird auf die besonderen Verfahrensregelungen<sup>1</sup> nach §79 Abs. 4 und 5 der Bundeshaushaltsordnung (BHO) des Bundesministers der Finanzen (Bestimmungen über den Einsatz von automatisierten Verfahren im Haushalts-, Kassen- und Rechnungswesen – HKR-ADV-Best (B) – ) hingewiesen.

---

<sup>1</sup> Bundesminister der Finanzen [Hrsg.]: Bestimmungen über den Einsatz von automatisierten Verfahren im Haushalts-, Kassen- und Rechnungswesen – HKR-ADV-Best (B) – (abgedruckt als Anlage zum Rundschreiben betr. Einsatz von automatisierten Verfahren im Haushalts-, Kassen- und Rechnungswesen; hier: Verfahrensregelung nach §79 Abs.4 und 5 BHO) vom 21. Dezember 1988 Az. II A 6 – H 1005 – 6/88 – MinBFin 1989, S. 8)

## 1.2 Informationstechnik (IT)

*Die IT erstreckt sich auf Datenverarbeitungstechnik und damit zusammenhängende Kommunikationstechnik. Sie umfaßt technische Einrichtungen und Verfahren, die auf der Grundlage der Mikroelektronik zur automatisierten Erfassung, Darstellung, Speicherung, Verarbeitung, Übermittlung und dem Empfang von Informationen dienen.*

Die Definition der IT in den IT-Mindestanforderungen entspricht derjenigen in den vom Bundeskabinett im August 1988 beschlossenen Richtlinien<sup>2</sup> des Bundes für den Einsatz der Informationstechnik in der Bundesverwaltung – IT-Richtlinien –. Nach dieser Definition kann die IT sowohl technisch – als IT-System (siehe folgende Erläuterungen a bis d) – als auch organisatorisch – als IT-Vorhaben oder IT-Verfahren (siehe folgende Erläuterungen e bis g) – verstanden werden. IT-Vorhaben und der Betrieb von IT-Verfahren erfordern eine entsprechende Organisation und Regelungen für die Arbeitserledigung. Daher sind auch die Regelungen für Entwicklung und Einsatz der IT und die für IT-Vorhaben und -Verfahren erforderliche Organisation bei der Prüfung der IT einzubeziehen; die IT-Mindestanforderungen stellen entsprechende Forderungen auf. Im folgenden sind die Prüfungsgegenstände näher erläutert, die durch die IT-Mindestanforderungen berührt werden.

### a) IT-System

Ein **IT-System** besteht aus dem IT-Basissystem mit Hardware und Systemsoftware, den IT-Verfahren (oder IT-Anwendungen), und den sonstigen Sachmitteln, die zum Betrieb des Systems benötigt werden, wie z. B. Verbrauchsmaterial.

### b) IT-Basissystem

Wegen des engen technischen Zusammenhangs zwischen der Hardware und den für den Betrieb grundlegenden Funktionen betrachtet man häufig die Hardware und die Systemsoftware als Einheit. Das **IT-Basissystem** besteht dementsprechend aus der Hardware und der Systemsoftware.

Zur **Hardware** zählen sämtliche Geräte der IT und ihre Verbindungen untereinander, z. B.

- die Zentraleinheit eines Rechners mit Prozessor (CPU) und Hauptspeicher,
- die Hintergrundspeicher, wie Plattenlaufwerke, Bandlaufwerke, Diskettenlaufwerke und Kassettenlaufwerke,
- die Terminals mit Bildschirm und Tastatur, ggf. ergänzt mit Grafiktablett, Lichtgriffel oder Maus sowie

<sup>2</sup> Bundesminister des Innern [Hrsg.]: Richtlinien des Bundes für den Einsatz der Informationstechnik in der Bundesverwaltung (IT-Richtlinien) vom 18. August 1988 (GMBI 1988, S. 470)

- die Datenfernverarbeitungseinrichtungen.

Zur **Systemsoftware** zählen alle Programme, die der technischen Steuerung der Hardware oder der Bereitstellung von technischen Basisfunktionen für die Entwicklung oder den Betrieb von IT-Verfahren dienen, z. B.

- Betriebssystemsoftware (Betriebssystem),
- Sicherheitssoftware (Zugriffsschutz),
- Datenbanksoftware,
- Dialogsoftware (TP-Monitor),
- Datenübertragungssoftware,
- Übersetzungsprogramme für Programmiersprachen (Compiler),
- Bibliotheksverwaltungssoftware,
- Produktionsplanungs- und -steuerungssoftware sowie
- sonstige Werkzeuge für Verfahrensentwicklung und -betrieb.

Wird ein Verfahren auf einem räumlich im wesentlichen zusammenhängenden IT-Basissystem betrieben, handelt es sich aus der Sicht dieses Verfahrens um ein **zentrales Basissystem**. Das **Rechenzentrum** ist die typische Organisationsform für ein zentrales Basissystem.

Wird ein Verfahren auf mehreren räumlich getrennten Systemen betrieben, handelt es sich aus der Sicht dieses Verfahrens um ein **dezentrales Basissystem**. Eine typische Erscheinungsform für dezentrale Hardware und Systemsoftware sind – ggf. vernetzte – arbeitsplatznahe IT-Systeme oder Arbeitsplatzrechner (**Arbeitsplatzcomputer**). Sie stellen die komplette Verarbeitungsleistung eines Computers, d. h.

- die Eingabe z. B. über Tastatur,
- die Verarbeitung,
- in der Regel die Speicherung und
- die Ausgabe, z. B. über Bildschirm oder Drucker,

am Arbeitsplatz des Endbenutzers zur Verfügung.

### c) **IT-Verfahren**

IT-Verfahren bestehen aus den zur Verfahrenssoftware zählenden Programmen, den Anweisungsfolgen der Ablaufsteuerung (Jobs), den Datenbeständen und den zugehörigen manuellen Arbeitsschritten einschließlich der entsprechenden Regelungen.

**Programme** sind Anweisungsfolgen, die aus korrekten Eingabeinformationen korrekte Ausgabeinformationen erzeugen und formal unkorrekte Eingabeinformationen zurückweisen sollen. Programme bestehen meist aus eigenständig änder- und testbaren Programmbestandteilen (**Modulen**) mit definierten Berührungspunkten (**Schnittstellen**) zwischen den Modulen.



Nach der Zeitspanne zwischen der Dateneingabe, der Verarbeitung und der Datenausgabe sowie nach den Möglichkeiten des Benutzers, das Verarbeitungsgeschehen zu beeinflussen, können die **Verarbeitungsarten**

- Stapelverarbeitung (Batch),
- Dialogverarbeitung und
- Prozeßverarbeitung

unterschieden werden. In Anhang 1 werden die Begriffe näher erläutert.

Der **Verfahrensbetrieb** (auch als **Produktion** oder **Wirkbetrieb** bezeichnet) umfaßt im Idealfall die anforderungsgerechte, ordnungsgemäße, sichere und wirtschaftliche Bereitstellung freigegebener Verfahren zur fachlichen Anwendung. Die Bereitstellung beinhaltet die technische Abwicklung des Verfahrenseinsatzes sowie die Verwaltung und Optimierung der für den Verfahrenseinsatz erforderlichen IT-Systeme, -Programme und -Verfahren (**Produktionsumgebung**).

**Verfahren heißen zentral**, wenn sie auf einem zentralen Basissystem betrieben werden. Die Betriebsverantwortung für diese Verfahren liegt bei einer zentralen Stelle, die organisatorisch getrennt von den jeweils fachverantwortlichen Stellen ist.

**Verfahren heißen dezentral**, wenn sie auf einem dezentralen Basissystem betrieben werden. Meist liegt die Fach- und Betriebsverantwortung bei derselben Stelle, in der Regel beim Fachbereich.

#### **d) Sachmittel**

Zu den Sachmitteln zählen das Verbrauchsmaterial und das sonstige Inventar.

**Verbrauchsmaterial** sind Sachmittel, die beim Betrieb oder der Entwicklung von Verfahren eingesetzt werden und dabei einem hohen Verschleiß oder dem vollständigen Verbrauch unterliegen, z. B.

- Druckerpapier,
- Formulare,
- Magnetbänder,
- Magnetbandkassetten,
- Disketten,
- Druckerfarbband,
- Toner für Laserdrucker und
- Reinigungsmittel.

Das **sonstige Inventar** sind Sachmittel, die beim Betrieb oder der Entwicklung von Verfahren eingesetzt werden. Dazu zählen z.B. Mikrofilmgeräte sowie zur Unterbringung von Datenendgeräten geeignete Büromöbel und Beleuchtungseinrichtungen, die z. B. an Arbeitsplätzen oder im Rechenzentrum benutzt werden und aus ergonomischer Sicht beim Einsatz der IT eine besondere Rolle spielen.

**e) IT-Vorhaben**

Die IT-Mindestanforderungen unterscheiden das IT-Vorhaben (Nr. 3.1.1) und IT-Verfahren (Nr. 4.1.1). Zum IT-Vorhaben zählen die Planung und Entwicklung eines Verfahrens sowie die IT-Beschaffung. Ein IT-Verfahren ist das Ergebnis eines IT-Vorhabens.

**f) Regelungen für die IT**

Die IT-Mindestanforderungen verlangen für wesentliche Aufgabenbereiche der IT Regelungen zum ordnungsgemäßen, wirtschaftlichen und sicheren Einsatz der IT, so für

- Dokumentation (Nr. 1.4.5),
- Vorgehensweise und Zuständigkeiten für IT-Vorhaben (Nr. 3.1.2 und Nr. 3.2.1),
- Programmerstellung (Nr. 3.4.4.1),
- Test und Freigabe (Nr. 3.4.5.8),
- Änderungen von Verfahren (Nr. 3.5.1),
- Fehlerbehebung (Nr. 3.5.2),
- Verantwortungsbereiche beim Betrieb von Verfahren (Nr. 4.2.3),
- Datenerfassung (Nr. 4.3.1.1),
- Arbeitsanweisungen bei der Datenverarbeitung (Nr. 4.3.3.1) und
- Sicherheit der IT (Nr. 7.3).

IT-Regelungen in einer Behörde sollten zweckmäßigerweise einen standardisierten **Aufbau** haben, der die verschiedenen Inhalte in gleichartiger, übersichtlicher Form darstellt.

**Inhaltlich** sollte eine Regelung für die IT je nach Erfordernis die folgenden Punkte umfassen:

- den Gegenstand,
- die Zielsetzung,
- die detaillierte Beschreibung der Arbeitsabläufe sowie anzuwendende Hilfsmittel, z. B. Methoden, Programme und Vorschriften,
- die Beschreibung der Kontrollen und Abstimmungen im Arbeitsablauf,
- die Beschreibung des Verhaltens in Ausnahmesituationen,
- die Abgrenzung der Zuständigkeit und die Entscheidungsbefugnisse,
- den Geltungsbereich und -zeitraum,
- ggf. eine Angabe darüber, welche Regelungen ersetzt werden oder nicht mehr gültig sind,
- den von der Regelung betroffenen Mitarbeiterkreis und
- den Ersteller der Regelungen.

Regelungen müssen so gefaßt werden, daß sie kontrollierbar sind.

Regelungen für die IT müssen zeitnah sich wandelnden Anforderungen angepaßt werden. Zudem sollten jedem Mitarbeiter die ihn betreffenden Regelungen in aktuellem Zustand zur Verfügung stehen und bekannt sein. Neuerungen und Änderungen sind in einem angemessenen Zeitraum vor ihrem Inkrafttreten den betroffenen Mitarbeitern bekanntzugeben, um sicherzustellen, daß die Regelungen unmittelbar nach Inkrafttreten angewandt werden können.

Empfehlenswert ist ein Verzeichnis aller gültiger Regelungen mit einem Hinweis auf den betroffenen Mitarbeiterkreis und den Stand der Regelungen (letzter Änderungsstermin).

Wenn Regelungen fehlen oder mangelhaft angewendet werden, wirkt sich dies häufig dahingehend aus, daß bei gleicher Aufgabenstellung uneinheitlich vorgegangen wird und Vorgehensweisen nicht aufeinander abgestimmt sind.

#### **g) Organisation**

Der Einsatz der IT erfordert entsprechende organisatorische Vorkehrungen. Die IT-Mindestanforderungen nennen hier insbesondere die Festlegung von Zuständigkeiten für Aufgaben im Rahmen von IT-Vorhaben (Nr. 3.2), für den Betrieb von IT-Verfahren (Nr. 4.2) und für die IT-Sicherheit (Nr. 7.2 und Nr. 7.3).

Jede Stelle muß hinsichtlich der Art der Aufgaben so beschrieben sein, daß ihre Tätigkeitsinhalte und die Abgrenzung zu anderen Stellen erkennbar ist. Aus der Beschreibung sollte hervorgehen, ob diese Aufgaben auf unbestimmte Zeit oder zeitlich befristet anfallen. Für jede Stelle sollte ein Qualifikationsprofil erstellt werden, das notwendige Kriterien, wie Anforderungen an

- Ausbildung,
- Fachkenntnisse,
- persönliche Fähigkeiten und
- Berufserfahrung

ausweist.

Bei entsprechender Mitarbeiterzahl sind die Stellen hierarchisch zu gliedern. Dabei ist auf eine angemessene Leitungsspanne – d. h. die Anzahl der Mitarbeiter, die eine Führungskraft direkt führt, – zu achten. In der Regel soll eine Führungskraft nicht mehr als 10 Mitarbeiter direkt führen.

Die hierarchische Einordnung und die Zuständigkeiten der mit IT befaßten Stellen ist in geeigneter Form, z. B. in einem Organigramm mit entsprechenden Erläuterungen, zu dokumentieren.

Die Aufgaben und Verantwortlichkeiten des Bereiches IT als Ganzes sollen gegen die übrigen Bereiche der Organisation eindeutig abgegrenzt sein. Die Berührungspunkte sollen beschrieben werden.

Die von einem Mitarbeiter wahrzunehmenden typischen Aufgaben werden oft auch als **Funktion** definiert. In Anhang 2 sind typische Funktionen einschließlich der Zuständigkeiten genannt, die im Rahmen der IT üblicherweise vorkommen.

### 1.3 Ziele des IT-Einsatzes

*Die IT soll eingesetzt werden, wenn hierdurch die Aufgabenerledigung*

*– in ihrer Wirtschaftlichkeit verbessert werden kann oder*

*– im Rahmen des wirtschaftlich Vertretbaren mit verbesserter Qualität, insbesondere sicherer, einfacher und schneller, durchgeführt werden kann oder*

*– erst durchführbar wird.*

Der **Einsatz der IT** muß der Unterstützung der Aufgaben dienen und dabei den Grundsätzen der Ordnungsmäßigkeit, Wirtschaftlichkeit und Sicherheit genügen. Die Ausführungen in den IT-Mindestanforderungen machen deutlich, daß bei Prüfungen der IT stets auch die Fachaufgabe und die Arbeitsabläufe bei Anwendung der IT in die Bewertung einbezogen werden müssen, da andernfalls nicht entschieden werden kann, inwieweit die Aufgabenerledigung angemessen unterstützt wird.

Die IT-Mindestanforderungen setzen verschiedentlich, z. B. bei der Gesamtplanung (Nr. 2.1), der Erfolgskontrolle und Qualitätssicherung (Nr. 5 und Nr. 6) oder der Risikoanalyse und dem Sicherheitskonzept (Nr. 7.2) Zielsetzungen im einzelnen voraus. Für die Bewertung von Nutzen-Kosten-Untersuchungen und damit der Wirtschaftlichkeit von IT-Maßnahmen sind nachvollziehbare und möglichst quantifizierte Zielsetzungen unabdingbar. Die Prüfbarkeit der Zielsetzungen ist nur dann gegeben, wenn sie dokumentiert sind oder sich durch gesetzliche oder anders bestimmte Vorgaben ohnehin ergeben.

Bei konkurrierenden Zielen ist zu beachten, daß das Bestreben nach Wirtschaftlichkeit das ordnungsgemäße Handeln der Verwaltung und die Sicherheit nicht beeinträchtigen darf. Bei sicherheitsrelevanten IT-Verfahren sind daher den Sicherheitskriterien in den Wirtschaftlichkeitsbetrachtungen entsprechendes Gewicht einzuräumen.

Bei Bundesbehörden müssen sich die Ziele aus den jährlich fortzuschreibenden IT-Rahmenkonzepten ergeben, die mit der Koordinierungs- und Beratungsstelle der Bundesregierung für Informationstechnik in der Bundesverwaltung im Bundesministerium des Innern (KBSt) abzustimmen sind. Dem Bundesbeauftragten für Wirtschaftlichkeit in der Verwaltung (BWV) ist Gelegenheit zur Stellungnahme zu geben (siehe auch IT-Richtlinien Nr. 4 und Nr. 5). Struktur und Inhalt der IT-Rahmenkonzepte sind durch die KBSt einheitlich vorgegeben<sup>3</sup>.

Die IT-Richtlinien nennen neben der Verbesserung der Wirtschaftlichkeit einige weitere allgemeingültige Ziele für den Einsatz der IT (IT-Richtlinien Nr. 2):

- Leistungssteigerung,
- Verbesserung der Kommunikationsmöglichkeiten,

<sup>3</sup> Bundesministerium des Innern [Hrsg.]: Gliederung der IT-Rahmenkonzepte mit Hinweisen und Erläuterungen zu ihrer Erstellung und Fortschreibung Stand 31. Mai 1990 (Schriftenreihe der KBSt; Band 18)

- Erhöhung der Bürgerfreundlichkeit,
- Verbesserung der Arbeitsbedingungen.

Es ist für eine sachgerechte Zielsetzung grundsätzlich nicht ausreichend, lediglich die allgemeinen Ziele aus den IT-Richtlinien zu nennen. Vielmehr müssen diese Ziele auf konkrete Vorhaben bezogen, nachvollziehbar und prüfbar, d. h. möglichst mit quantitativen Angaben benannt sein (siehe auch Nr. 5 und Nr. 6).

## 1.4 Dokumentation der IT

- 1.4.1 *Die Planung und der Einsatz der IT sind zu dokumentieren. Die Dokumentation erstreckt sich auf:*
- *die Gesamtplanung für den Einsatz der IT*
  - *die Durchführung von IT-Vorhaben*
  - *den Betrieb von IT-Verfahren*
- 1.4.2 *Die IT-Dokumentation muß vollständig sein und ist möglichst überschneidungsfrei zu gestalten. Die Dokumentation muß zeitnah, verständlich und richtig sein und den Nachweis aller Änderungen enthalten.*
- 1.4.3 *Die Erstellung, Pflege und Speicherung der Dokumentation soll aus Gründen der Wirtschaftlichkeit möglichst maschinell unterstützt werden. Es ist sicherzustellen, daß die Dokumentation nur durch hierzu berechtigtes Personal geändert werden kann.*
- 1.4.4 *Allen an der Durchführung von IT-Vorhaben und am Betrieb von IT-Verfahren beteiligten Stellen und Mitarbeitern müssen die für die Arbeits erledigung benötigten Teile der Dokumentation nach dem letzten Stand als Mehrausfertigung zur Verfügung stehen.*
- 1.4.5 *Die Einzelheiten der Gestaltung, der Erstellung und des Inhalts sowie der Verteilung und der Aufbewahrung der Dokumentation sind – ggf. im Rahmen geltender Vorschriften – im einzelnen schriftlich zu regeln.*

Für den ordnungsgemäßen Einsatz der IT ist eine aussagekräftige Dokumentation Grundvoraussetzung.

Eine Dokumentation kann als die Beschreibung oder Wiedergabe eines abgegrenzten Dokumentationsgegenstandes in einer unmittelbar lesbaren oder mittelbar in angemessener Zeit lesbar zu machenden Form verstanden werden. Das bedeutet, daß auch Informationen, die zunächst lediglich maschinell verfügbar sind, der Dokumentation hinzuzurechnen sind und den gleichen Kriterien genügen müssen, wie die auf Papier ausgedruckte Dokumentation.

**Dokumentationsgegenstände** bei der Dokumentation der Gesamtplanung, der Durchführung von IT-Vorhaben und dem Betrieb von IT-Verfahren können z. B. sein:

- Verfahren und ihre Bestandteile,
- Hardware und Systemsoftware und ihre Bestandteile,
- Organisation,
- Regelungen.

Aus den IT-Mindestanforderungen lassen sich weitere Hinweise zur IT-Dokumentation und deren Erstellung ableiten:

- Die Dokumentationsgegenstände sind geeignet festzulegen und gegeneinander abzugrenzen. Die Dokumentation zu jedem Dokumentationsgegenstand sollte diesen vollständig beschreiben (Nr. 1.4.2).
- Die Dokumentation ist formal und inhaltlich möglichst einheitlich zu gliedern, d.h. für gleichartige Dokumentationsteile soll ein gleichartiger formaler und inhaltlicher Aufbau gewählt werden, um die Verständlichkeit zu fördern und die Pflege wirtschaftlich zu gestalten. Dieses Ziel kann durch den Einsatz maschineller Hilfsmittel wesentlich unterstützt werden (Nr. 1.4.2, Nr. 1.4.3 und Nr. 1.4.5). Eine einheitliche IT-Dokumentation erleichtert zudem den flexiblen Einsatz des Personals.
- Bei einer maschinell unterstützten Dokumentation empfiehlt es sich, die Dokumentationspflege zentral vorzunehmen und danach die ausgedruckten oder dezentral gespeicherten Kopien zu ersetzen. Auf diese Weise lassen sich Zugriffsrechte einfacher verwalten (Nr. 1.4.3) und die Verfügbarkeit der aktuellen Versionen (Nr. 1.4.4) leichter erreichen.
- Insbesondere wenn unterschiedliche IT-Verfahren und -Systeme eingesetzt sind, muß eine Regelung für die Dokumentation ggf. die besonderen systemtechnischen und verfahrensspezifischen Gegebenheiten berücksichtigen (Nr. 1.4.5).
- Änderungen des Dokumentationsgegenstandes sollten mit Angabe des Änderungstermins bereits beschrieben sein, bevor diese wirksam werden. Zu den Änderungen ist anzugeben, von welchem Zeitpunkt an und wie lange sie wirksam sein werden. So sollte die Verfahrensdokumentation vorliegen, bevor der Betrieb aufgenommen wird, um Test, Freigabe sowie die Verfahrenseinführung ordnungsgemäß und sicher durchführen zu können (Nr. 1.4.2, siehe auch Nr. 3.4.5).
- Die Dokumentation muß für die erforderliche Nutzung oder Prüfung vor Ort in unmittelbar lesbarer Form verfügbar sein oder in angemessener Zeit verfügbar gemacht werden können. Dies gilt bei kassenwirksamen Verfahren auch für nicht mehr aktuelle Dokumentationsstände (HKR-ADV-Best (B) Nr. 3 und 5). Die gesetzlichen Aufbewahrungsfristen sind einzuhalten. Die Dokumentation ist innerhalb der Nutzungsdauer und der Aufbewahrungsfristen sicher aufzubewahren oder zu speichern (Nr. 1.4.3 und Nr. 1.4.4).
- Die Dokumentation muß von der jeweiligen Zielgruppe verstanden und umgesetzt sowie von einem sachverständigen Dritten in angemessener Zeit nachvollzogen und geprüft werden können (Nr. 1.4.2).

Ein sachverständiger Dritter kann z. B. ein Mitglied der Testgruppe, ein mit dem Projekt befaßter Mitarbeiter der Fachabteilung, ein (interner oder externer) Prüfer oder ein IT-Fachmann sein, der im Projekt mitarbeiten soll. Welche Zeit angemessen ist, hängt von den jeweils durchzuführenden Arbeiten ab. So muß sich ein Prüfer rasch einen Überblick verschaffen können, ein IT-Fachmann muß die ihn interessierenden Einzelheiten schnell finden. Den unterschiedlichen Erfordernissen muß in angemessener Weise Rechnung getragen werden.

Besondere Probleme können dann entstehen, wenn in großem Umfang Verfahren unter Mitwirkung externer Firmen entwickelt werden. Über Regelungen zur IT-Dokumenta-



tion (Nr. 1.4.5), die auch Gegenstand der Verträge mit den Externen sein müssen, kann die Weiterverwendbarkeit und Fortführung der Dokumentation durch den Auftraggeber, in der Regel die Verwaltung, sichergestellt werden.

Der Aufwand für eine ordnungsgemäße Dokumentation ist in der Regel ein wesentlicher Teil des gesamten Entwicklungsaufwands. Erfahrungsgemäß erweist sich dieser Aufwand jedoch als wirtschaftlich, insbesondere bei Verfahren, die über einen längeren Zeitraum eingesetzt werden. Dadurch wird die Verfahrenspflege und -erweiterung, z. B. aufgrund von fachlichen Anforderungen, sowie ein ordnungsgemäßer Verfahrensbetrieb erleichtert oder überhaupt erst möglich. Da zudem Software in der Regel länger eingesetzt wird als die Hardware, die häufig entsprechend den aktuellen technischen Möglichkeiten ersetzt wird, sind Anpassungen der Verfahren stets zu erwarten. Eine ordnungsgemäße Dokumentation ist somit auch die Grundlage für die Absicherung der häufig sehr hohen Investitionen in die Verfahrensoftware.

## 2 Gesamtplanung und Koordinierung

### 2.1 Gesamtplanung

2.1.1 *Der Einsatz der IT ist auf der Grundlage einer Gesamtplanung vorzunehmen. Der Gesamtplan soll je nach Planungs- und Entwicklungsstand ausweisen:*

- *Organisation, bestehende IT-Verfahren und technische Einrichtungen sowie eingesetztes IT-Fachpersonal,*
- *allgemeine Darstellung und absehbare Entwicklung der Aufgaben, die mit Hilfe der IT erledigt werden sollen,*
- *Berührungspunkte und Überschneidungen zwischen diesen und mit anderen Aufgaben und Aufgabenfeldern,*
- *Ziele des geplanten IT-Einsatzes,*
- *geplante und in der Durchführung befindliche IT-Vorhaben einschließlich ihrer Prioritäten sowie ihrer organisatorischen und personellen Auswirkungen,*
- *Zeitbedarf für die Realisierung der IT-Vorhaben,*
- *Einführungsstrategien und Schulungsmaßnahmen,*
- *Planungen und Maßnahmen für die Sicherheit beim Einsatz der IT,*
- *Aussagen zur Wirtschaftlichkeit,*
- *Bedarf an Haushaltsmitteln.*

2.1.2 *Bei der Gesamtplanung sind Normen, Standards und geltende Festlegungen zu beachten. Die Gesamtplanung muß regelmäßig überprüft und fortgeschrieben werden.*

Wegen der vielfältigen Wechselwirkungen zwischen den IT-Vorhaben und -Verfahren einer Behörde, dem engen Zusammenhang der IT mit der fachlichen Aufgabenstellung sowie der häufig weitreichenden Auswirkungen des IT-Einsatzes ist es zweckmäßig, für die IT eine Gesamtplanung vorzunehmen. Die IT-Mindestanforderungen nennen die einzelnen Elemente einer Gesamtplanung (Nr. 2.1.1). Es ist dabei zu berücksichtigen, daß nicht alle Teile einer Gesamtplanung mit gleicher Genauigkeit festgelegt sein können, da sich z. B. die Vorhaben in unterschiedlichen Planungs- und Entwicklungsphasen befinden.

Grundsätzlich soll die Gesamtplanung für den IT-Einsatz den Weg zu einem Soll-Zustand unter Berücksichtigung von zeitlichen Vorgaben und den verfügbaren Personal- und Sachmitteln aufzeigen. Dieser Soll-Zustand muß im Einklang mit den Zielen des IT-Einsatzes stehen (Nr. 1.3). Dementsprechend sollte die IT-Planung

- zielorientiert,

- zukunftsorientiert,
- umsetzbar,
- begründet,
- zweckdienlich genau,
- zeitlich lückenlos und
- schrittweise fortschreibbar

sein.

Die Einhaltung der Planung muß im Rahmen von Soll-Ist-Vergleichen kontrollierbar sein, damit bei wesentlichen Soll-Ist-Abweichungen Gegenmaßnahmen eingeleitet werden können. Die Gesamtplanung soll die Entwicklung der IT im Hinblick auf die verwaltungsspezifische Aufgabenstellung zumindest für den Zeitraum der mittelfristigen Finanzplanung behandeln. Sie soll jährlich oder bei Bedarf geprüft und fortgeschrieben werden (Nr. 2.1.2). Die IT-Richtlinien des Bundes fordern eine jährliche Fortschreibung der Gesamtplanung (IT-Rahmenkonzepte).

Aus der Gesamtplanung ergeben sich auch Erfordernisse an die Personalplanung für den IT-Bereich, so

- die Ermittlung des Personalbedarfs,
- die Personalgewinnung sowie
- die Aus- und Fortbildung des Personals.

Bei Bundesbehörden wird bei sachgerechter Anwendung der IT-Richtlinien den Anforderungen der IT-Mindestanforderungen an eine Gesamtplanung Rechnung getragen. Grundlegende Unterlage für die Prüfung ist das IT-Rahmenkonzept der Behörde und die diesem zugrundeliegenden Unterlagen.

Bei knappen personellen Ressourcen kann die Fertigstellung von Verfahren verzögert werden, wenn zu viele Vorhaben zeitgleich durchgeführt werden. Wenn erkennbar wird, daß der für die Durchführung von Maßnahmen angenommene Zeitbedarf nicht ausreicht, ist die Gesamtplanung, insbesondere die Priorität der Vorhaben, entsprechend anzupassen.

Für die Festlegung der Dringlichkeit einzelner Vorhaben und die Entscheidung über die Rangfolge kann die Einsetzung eines vorhabenübergreifenden Gremiums mit Vertretern der Verfahrensentwicklung, des Verfahrensbetriebes und der Fachbereiche sinnvoll sein.

Die Gesamtplanung muß auch die Aufwendungen für die Pflege und Weiterentwicklung in Betrieb befindlicher Verfahren berücksichtigen, da diese teilweise den Aufwand für Neuentwicklungen übersteigen und somit die freien Ressourcen für die Entwicklung maßgeblich bestimmen.

Verfahrenssoftware ist häufig eng mit einer bestimmten Hardware oder Systemsoftware verbunden. System- oder Herstellerwechsel sind dadurch mitunter nur mit großem Aufwand durchführbar. Die Möglichkeiten einer Beschaffung im Wettbewerb und damit auf wirtschaftliche Weise sind dann eingeschränkt. Normen und Standards sind daher bereits bei der Gesamtplanung zu berücksichtigen und ggf. als "Hausstandards"

festzuschreiben. Auch Marktgegebenheiten ("Quasi-Standards") sollten beachtet werden. Die KBSt hat diesbezüglich verschiedene Hinweise gegeben (siehe z. B. Untersuchung zur praktischen Umsetzung des EG-Ratsbeschlusses vom 22. Dezember 1986 über die Normung auf dem Gebiet der Informationstechnik und der Telekommunikation – EGUNIT, Band 12 der Schriftenreihe der KBSt; Stand und Perspektiven für die Entwicklung portabler IT-Anwendungen in der öffentlichen Verwaltung – Untersuchungsbericht, Band 15 der Schriftenreihe der KBSt; KBSt-Forum "Informationstechnik in der Bundesverwaltung" am 26. Oktober 1988 in Bonn "Portable Betriebssysteme – Entwicklung, Normung und Bedeutung", Band 16 der Schriftenreihe der KBSt).

## 2.2 *Koordinierung des IT-Einsatzes*

2.2.1 *Durch die Gesamtplanung und eine zweckmäßige Koordinierung ist insbesondere sicherzustellen, daß*

- die mehrfache Entwicklung von IT-Verfahren für gleichartige Aufgaben unterbleibt,*
- einheitliche Verfahren angewendet und Verbundlösungen angestrebt und*
- die Ressourcen im IT-Bereich wirtschaftlich genutzt werden.*

2.2.2 *Der ressortübergreifenden Koordinierung ist besondere Beachtung zu schenken.*

Die vorhabenübergreifende Abstimmung der Verfahrensentwicklung ist bei Behörden, die eine große Anzahl von Vorhaben zeitgleich durchführen, zweckmäßigerweise über eine mit der Vorhabenkoordinierung betraute Stelle sicherzustellen. Sie sollte

- an der Planung und Kontrolle der einzelnen Projekte beteiligt werden,
- die Mitwirkung von Vertretern der Bereiche Verfahrensentwicklung und Verfahrensbetrieb sowie der fachlich zuständigen Bereiche bei der Koordinierung sicherstellen,
- Empfehlungen über die durchzuführenden Projekte aussprechen,
- hinsichtlich der Koordinierung bereits begonnener Vorhaben insbesondere nachfolgende Aufgaben durchführen:
  - o Hinwirken auf ein aufgabengerechtes Zusammenwirken der an den Vorhaben Beteiligten,
  - o Information aller Beteiligten und
  - o Ausarbeitung von Empfehlungen für die Fortschreibung der Gesamtkonzeption.

Über organisatorische Maßnahmen ist die geordnete Kommunikation aller betroffenen Stellen sicherzustellen, so daß die benötigten Informationen in geeignetem Umfang und rechtzeitig zur Verfügung stehen. Für bestimmte Themen können zudem Ansprechpartner benannt werden, die organisatorisch innerhalb und außerhalb des Bereiches IT angesiedelt sein können. Für die Fachbereiche ist es empfehlenswert, einen Mitarbeiter mit der Koordinierung der fachlichen Anforderungen an die IT zu betrauen, der dem IT-Bereich zugleich als Ansprechpartner dient.

Die Lösung der fachlichen Aufgaben einer Verwaltung erfordert in der Regel mehrere Verfahren. Enthalten Verfahren gleiche Bestandteile, so soll deren Entwicklung, z. B. mit Hilfe eines Informations- oder Funktionsmodells, so koordiniert werden, daß diese Bestandteile verfahrenübergreifend verwendet werden können:

- Wenn lediglich fallweise, nur mit Blick auf das jeweilige Vorhaben vorgegangen wird und Querverbindungen zu schon bestehenden Verfahren und Vorhaben nicht beachtet werden, können unwirtschaftliche Insellösungen entstehen. Daher sollten alle in der Verwaltung benötigten und erzeugten Informationen einheitlich und

verfahrenübergreifend beschrieben werden, um wiederholte und widersprüchliche Beschreibungen der Informationen in verschiedenen Verfahren zu vermeiden (Informations- oder Datenmodell). Eine eindeutige verfahrenübergreifende Beschreibung der Informationen kann zudem den reibungslosen Informationsfluß zwischen den an verschiedenen Verfahren Beteiligten fördern (siehe auch Nr. 1.4).

- Ebenso sollten die in einer Verwaltung manuell oder maschinell auszuführenden Funktionen nach einheitlichen und verfahrenübergreifenden Regeln beschrieben werden, um wiederholte und widersprüchliche Beschreibungen und technische Realisierungen der Funktionen in verschiedenen Verfahren zu vermeiden (Funktionsmodell).

Ein Funktionsmodell kann zusammen mit dem Informationsmodell die Koordinierung unterstützen.

Weiterhin werden häufig Daten zwischen verschiedenen Verfahren ausgetauscht. Für solche Fälle müssen die Schnittstellen zwischen den Verfahren vollständig und eindeutig festgelegt sein. Die Erfordernisse der Datensicherheit sind beim Datenaustausch zwischen Verfahren zu berücksichtigen. Funktions- und Informationsmodelle können Tätigkeiten in diesem Zusammenhang unterstützen.

Bei der Aufstellung von IT-Rahmenkonzepten oder der Einleitung größerer Vorhaben und Beschaffungen sollte daher geprüft werden, ob übergreifende Standardlösungen oder gemeinsame Maßnahmen verschiedener Stellen möglich sind.

Regelungen für die ressortübergreifende Koordinierung enthalten die IT-Richtlinien des Bundes. Der Bundesrechnungshof hat zum Stand der IT-Koordinierung in der Bundesverwaltung Stellung genommen (Bemerkungen des Bundesrechnungshofes 1992, BT-Drs. 12/3250, Nr. 48, Wahrnehmung der Koordinierungsaufgaben durch die Koordinierungs- und Beratungsstelle der Bundesregierung für Informationstechnik in der Bundesverwaltung).

## 3 IT-Vorhaben

### 3.1 Allgemeines

3.1.1 *IT-Vorhaben beinhalten die Konzeption, die Entwicklung, die Einführung und wesentliche Änderungen von IT.*

3.1.2 *Die Grundsätze zur Gewährleistung einer einheitlichen und systematischen Vorgehensweise bei der Durchführung von IT-Vorhaben, einschließlich der Bildung sachgerechter Abschnitte mit entsprechenden Teilzielen, sind schriftlich zu regeln. Dabei sind eine zweckmäßige Vorhabensteuerung und -überwachung vorzusehen sowie Festlegungen über den Einsatz standardisierter Arbeitstechniken (Methoden und Werkzeuge) zu treffen.*

Entsprechend den Erläuterungen zum Begriff IT (Nr. 1.2) umfassen die IT-Mindestanforderungen auch IT-Vorhaben und darin Maßnahmen wie die Beschaffung von IT, die Erarbeitung von Regelungen im Bereich der IT oder Projekte. Projekte werden in den IT-Mindestanforderungen als zielgerichtete, zeitlich, personell und sachlich abgegrenzte IT-Vorhaben zur Entwicklung und Pflege von Verfahren verstanden. Sie sind somit IT-Vorhaben, deren Ergebnis IT-Verfahren sind. Da die gleichen Anforderungen gelten, werden die Begriffe IT-Vorhaben und Projekt in den IT-Prüfungshinweisen synonym gebraucht.

Bei der Durchführung von IT-Vorhaben sind vorhabenübergreifende von vorhabensspezifischen Gesichtspunkten zu unterscheiden. Vorhabensspezifische Gesichtspunkte sind unter Nr. 3.4 und Nr. 3.5 dargestellt.

Vorhabenübergreifend ist eine einheitliche und systematische Vorgehensweise – zumeist als **Vorgehensmodell** bezeichnet – festzulegen, mit dem eine ordnungsgemäße, sichere und wirtschaftliche Verfahrensentwicklung unterstützt und alle Maßnahmen für den späteren ordnungsgemäßen, sicheren und wirtschaftlichen Verfahrensbetrieb berücksichtigt werden sollen. Das Vorgehensmodell ist bei der Verfahrensentwicklung verbindlich anzuwenden. Abweichungen von der allgemein gewählten Vorgehensweise sind vor Projektbeginn zu begründen und schriftlich niederzulegen.

Das Vorgehensmodell sollte gleichermaßen für die Neu- und Weiterentwicklung von Verfahren sowie für die Verfahrenspflege gelten. Deshalb sollte ein Vorgehensmodell insbesondere im Hinblick auf die Bedeutung einzelner Projektabschnitte, die Durchführung bestimmter Tätigkeiten sowie Art und Umfang der einzelnen Ergebnisse den jeweiligen Erfordernissen angepaßt werden können. Viele Vorgehensmodelle haben den Nachteil, daß sie zwar für größere Neuentwicklungen, nicht aber für kleinere Änderungen bestehender Verfahren oder wenig aufwendige Entwicklungen auf APC geeignet sind. Dies führt dazu, daß die Vorgehensmodelle nicht oder nur teilweise angewendet werden, weil der Aufwand zu hoch ist. Darunter leidet dann häufig die Akzeptanz eines Vorgehensmodells insgesamt.

Die KBSt hat eingehende Hinweise<sup>4</sup> für ein Vorgehensmodell zur Planung und Durchführung von IT-Vorhaben in der Bundesverwaltung in den Bänden 27/1 und 27/2 der Schriftenreihe der KBSt gegeben .

Durch das Vorgehensmodell sind zweckmäßige **Projektabschnitte** vorzugeben. Jedem Projektabschnitt sind Ergebnisse zuzuordnen, die bei Beendigung des Projektabschnittes vorliegen müssen (Meilensteine). Diese Ergebnisse können zur Abstimmung und Entscheidung über die Fortführung des Projektes genutzt werden.

Die Projektabschnitte sollen in **einzelne Tätigkeiten** untergliedert werden, für die

- der Arbeitsablauf,
- die benötigten Informationen, z. B. in Form vorauszusetzender, im Rahmen des Projektes bereits erstellter Ergebnisse, und
- die zu erzeugenden Informationen, z. B. in Form zu erstellender Ergebnisse,

zu beschreiben sind.

Die Tätigkeiten sollen alle Aufgaben des Projektes von der Erteilung des Projektauftrages bis zur Pflege des entwickelten Verfahrens vollständig abdecken und sind klar gegeneinander abzugrenzen. Sie können dann für eine Vollständigkeitskontrolle genutzt werden. Dabei sind auch Tätigkeiten der Projektsteuerung und der Qualitätssicherung (Nr. 6) zu berücksichtigen. Grundsätzlich sollte keine Tätigkeit begonnen werden, bevor nicht die vorausgesetzten Anfangsbedingungen (Vorliegen der erforderlichen Ergebnisse vorangegangener Tätigkeiten) erfüllt sind.

Das Vorgehensmodell soll auch die einzusetzenden Methoden und Werkzeuge festlegen.

**Methoden** beschreiben einen – in der Regel theoretisch begründeten – allgemeinen Lösungsweg für einen bestimmten Aufgabentyp. Geeignete Methoden sollen Bestandteil des Vorgehensmodells sein und dazu beitragen,

- die Einheitlichkeit,
- die Verständlichkeit,
- die Vollständigkeit,
- die Widerspruchsfreiheit und
- die Wiederholungsfreiheit

der Ergebnisse sichern zu helfen.

Unter **Werkzeugen** werden in der IT Softwareprodukte verstanden, die ihren Benutzer bei der Anwendung von Methoden zur Lösung verschiedener informationstechnischer Aufgaben unterstützen.

Neben den Werkzeugen, die bestimmte Methoden der Verfahrensentwicklung unterstützen, sind meist auch allgemeine Werkzeuge eingesetzt, die methodenunabhängig die Arbeitsabwicklung bei IT-Vorhaben fördern. Bei der Auswahl von Werkzeugen ist

---

<sup>4</sup> Bundesministerium des Innern [Hrsg.]: Planung und Durchführung von IT-Vorhaben in der Bundesverwaltung Vorgehensmodell (V-Modell) Stand: August 1992 (Schriftenreihe der KBSt; Band 27/1 und Band 27/2)



darauf zu achten, daß die damit erstellten Ergebnisse leicht zu ändern und fortzuentwickeln sind, d. h. die Werkzeuge müssen über entsprechende Verwaltungs-, Auswertungs- und Änderungsfunktionen verfügen.

Methoden und Werkzeuge sollen durchgängig aufeinander abgestimmt sein, d. h. die Ergebnisse eines Vorhabensabschnittes sollten mit ggf. anderen Werkzeugen eines folgenden Vorhabensabschnittes weiterbearbeitet werden können, ohne daß eine manuelle Umsetzung oder Überarbeitung erforderlich wird. Da die am Markt erhältlichen Produkte aber nicht gleich gut für alle Arbeitsschritte geeignet oder an bestimmte Systemumgebungen gebunden sind, ist oftmals der Einsatz unterschiedlicher Werkzeuge erforderlich, der die Weiterverwendung bereits erarbeiteter Ergebnisse erschwert. In Anhang 3 sind Beispiele für verbreitete Methoden und Werkzeuge genannt.

Im Rahmen des Vorgehensmodells sollten auch Grundsätze für die Programmierung festgelegt sein. Dabei sollten Verfahren für einen gleichartigen Aufbau von Programmen bzw. Modulen und die gleichartige Codierung bestimmter Programmfunktionen, z. B. Ein-/Ausgabefunktionen, beschrieben sein. Zur Vereinfachung sollen Beispiele vorgegeben werden, um den Aufwand zur Erstellung, Pflege und Prüfung der Programme zu verringern und deren Qualität zu steigern. Die Grundsätze sollten sich insbesondere beziehen auf

- die Standardteile (Programmrahmen) für verschiedene Arten von Programmen,
- den Standardaufbau der Übergabebereiche zwischen Modulen,
- die Verwendung allgemeiner Module,
- die Kommunikation der Programme mit der Datenverwaltungs- und Dialogsteuerungssoftware (Datenbanksysteme und TP-Monitore),
- die Anwendung von Methoden und Werkzeugen zur Programmierung (z. B. strukturierte und normierte Programmierung) und
- die Einschränkung oder Empfehlung der Verwendung einzelner Sprachelemente, z. B. aus Gründen der Nachvollziehbarkeit oder der Systembelastung.

Grundsätzlich sollten nur gängige, möglichst standardisierte Programmiersprachen verwendet werden. Weitergehende Hinweise zu Regelungen für die Programmierung finden sich in Nr. 3.4.4.

Allgemeine Module, die in mehreren Verfahren eingesetzt werden oder werden können, sind verfahrenübergreifend zu beschreiben und in allen Projekten einzusetzen. Diese Module darf nur autorisiertes Personal zentral ändern. Der Einsatz von vorhandenen allgemeinen Modulen ist verbindlich vorzuschreiben, um die Erstellung von Programmen zu vereinfachen und wirtschaftlich zu gestalten.

Eine einheitliche Benutzeroberfläche vereinfacht ebenfalls die Verfahrensentwicklung und -pflege, da dann in großem Umfang Standardprogrammteile und allgemeine Module verwendet werden können. Zudem kann der Schulungsaufwand verringert werden. Daher sollte bei Stellen, die viele unterschiedliche Verfahren einsetzen, verfahrenübergreifend ein allgemeiner **Standard für eine Benutzeroberfläche** festgelegt sein, der insbesondere folgende Vorgaben enthalten soll:

- das Aufbauschema von Bildschirmmasken zur Verfahrens- und Funktionsauswahl (Menüs/Fenster),
- das Aufbauschema von Bildschirmmasken zur Funktionsbearbeitung,
- die allgemeingültigen Funktionstasten und Kommandos,
- die Meldungen für das Betriebspersonal,
- die Fehlerbehandlung,
- die Hilfefunktion und
- das Aufbauschema von Listen und sonstigen Belegen.

Die verfahrensspezifische Ausgestaltung der Benutzeroberfläche geschieht im Rahmen der Verfahrensentwicklung (siehe Nr. 3.4.4.3).

Soweit unterschiedliche Standardprodukte für Endbenutzer eingesetzt sind, sollte auf leichte und möglichst ähnliche Bedienbarkeit geachtet werden, um den Schulungs- und Einarbeitungsaufwand zu verringern. Eine Vielzahl von APC-Standardprodukten, die jeweils hinsichtlich ihres speziellen Einsatzzwecks optimal gestaltet sind, bringen häufig nicht den erwarteten Nutzen, wenn die Bedienung zu unterschiedlich ist und der Benutzer gezwungen ist, sich immer wieder einzuarbeiten. Bei der Beschaffung sollten daher Funktionalität und Bedienbarkeit gegeneinander abgewogen werden.

Die vorgenannten verfahrenübergreifenden Festlegungen und die Entwicklungsumgebung sollten entsprechend Nr. 1.4 verfahrenübergreifend dokumentiert sein und bei der Gesamtplanung (Nr. 2.1) berücksichtigt werden.

## 3.2 Zuständigkeiten und Vorgehensweise

3.2.1 Bei Beginn eines IT-Vorhabens sind die Zuständigkeiten und die Vorgehensweise festzulegen. Soweit mehrere Stellen zuständig sind, sind Beteiligung und Verantwortung im einzelnen zu regeln.

3.2.2 Grundlage für ein IT-Vorhaben ist der IT-Gesamtplan. Ein IT-Vorhaben soll grundsätzlich umfassen:

– Vor- und Hauptuntersuchung

und

– Ausführung des Vorhabens.

Grundsätzlich ist neben der Fach- und Betriebsverantwortung (siehe Nr. 4.2) die Entwicklungsverantwortung für Verfahren zu unterscheiden. Anhang 2 enthält in Nr. 1 Hinweise zur Entwicklungsverantwortung.

Bei größerem Umfang sollte die Entwicklung von neuen Verfahren und die wesentliche Änderung bestehender Verfahren im Rahmen von besonderen Projekten durchgeführt werden, d. h. organisatorisch, zeitlich, personell und sachlich abgegrenzt sein. Ein Projekt erfordert eine Reihe organisatorischer Maßnahmen und Festlegungen. Zunächst ist die geordnete Einrichtung von Projekten sicherzustellen. Die Einrichtung eines Projektes umfaßt

- die positive Entscheidung zur Durchführung,
- die Bereitstellung von Haushaltsmitteln und
- die Bildung einer Projektgruppe.

Projekte sollten nicht ohne Abstimmung mit den koordinierenden Stellen (siehe auch Nr. 2.2) und nicht ohne Genehmigung der Entscheidungsträger eingerichtet werden. Die Entscheidung über die Einleitung eines Projektes und die ggf. wiederholte Entscheidung über die Fortführung an geeigneten Stellen der Projektabwicklung ist durch einen gesamtverantwortlichen Entscheidungsträger zu fällen.

### a) Projektorganisation

Bei den beteiligten Stellen sind die erforderlichen organisatorischen Maßnahmen zu berücksichtigen, d. h. es sind insbesondere die Zuständigkeit, Weisungsbefugnis, Aufgabenverteilung und Verantwortlichkeit im Rahmen der Projektorganisation festzulegen.

Dabei soll ein **Projektleiter** die Planung, Koordination und Kontrolle innerhalb des Projektes übernehmen. Die Rechte und Pflichten eines Projektleiters müssen vor Beginn des Projektes festgelegt werden. Diese Festlegung bestimmt den Umfang der Verantwortung und der Entscheidungsbefugnis des Projektleiters. Zu den Rechten und Pflichten können beispielsweise gehören:

- Der Projektleiter schlägt im Benehmen mit den betroffenen Bereichen Mitarbeiter für die Projektgruppe vor.
- Der Projektleiter plant und überwacht Termine, Aufwand und Haushaltsmittelverbrauch sowie den Einsatz von Personal und Sachmitteln.
- Der Projektleiter plant und erteilt Arbeitsaufträge für Projektmitarbeiter und kontrolliert die Durchführung. Der Projektleiter hat Weisungsbefugnis gegenüber den Mitarbeitern und die Kontrolle über die Art und Dauer der Arbeitsaufträge im Rahmen des Projekts.
- Der Projektleiter muß bei Schwierigkeiten der Projektabwicklung, insbesondere wenn sie außerhalb der ihm erteilten Entscheidungsvollmachten liegen, die Entscheidungsträger über Termin- oder Aufwandsverschiebungen unverzüglich informieren.
- Der Projektleiter berichtet in regelmäßigen Abständen über den Projektverlauf.
- Der Projektleiter soll den tatsächlichen Aufwand bei der Projektarbeit zeitnah ermitteln und kontrollieren.
- Für die Zeit der Abwesenheit des Projektleiters ist ein sachkundiger Vertreter zu benennen.
- Der Projektleiter steht den Projektmitarbeitern für Besprechungen und Rückfragen zur Verfügung.
- Der Projektleiter ist für die Qualität der Arbeiten verantwortlich.

Projektmitarbeiter sind in Bezug auf die Projektarbeit dem Projektleiter fachlich zu unterstellen. Der Projektmitarbeiter muß seine Arbeitsaufträge sachlich richtig und termingerecht durchführen und bei Problemen den Projektleiter umgehend informieren. Soweit Mitarbeiter aus anderen Bereichen im Projekt mitarbeiten, sind sie entsprechend dem Anteil der Projektarbeit an der Arbeitskapazität von den übrigen Aufgaben zu entlasten.

Bereiche, die durch fachliche oder technische Auswirkungen des Projekts betroffen sind, aber nicht unmittelbar in der Projektgruppe vertreten sind, sollten – soweit erforderlich – **projektbezogene Ansprechpartner** benennen. Neben der Verfahrensentwicklung sind z. B. regelmäßig die Funktionsbereiche Systemtechnik, Datenorganisation oder Arbeitsvorbereitung betroffen.

Häufig fehlt bei Projekten eine klare Abgrenzung der Aufgaben und eine ausreichende Abstimmung zwischen den Beteiligten. Die Trennung zwischen den fachlich zuständigen Bereichen (Bauherr, Bedarfsträger) und der IT (Bedarfsdecker) führt vielfach dazu, daß eine Gesamtverantwortung für ein Projektergebnis nicht gegeben ist, sondern jeweils nur die Teilverantwortung für die fachlichen Vorgaben und für die technische Umsetzung. Besonders bei komplexer Aufgabenstellung besteht dann die Gefahr, daß Teilverantwortliche wichtige Gesamtzusammenhänge nicht erkennen, die für die Funktionsfähigkeit der Lösung von Bedeutung sind. So stellen Fachbereiche beispielsweise Forderungen auf, ohne zu erkennen, daß diese nur mit hohem Aufwand zu realisieren sind. Die IT-Verantwortlichen sehen häufig nicht, daß diese Forderungen herabgesetzt werden könnten, ohne die Funktionalität der Gesamtlösung entscheidend zu beeinträchtigen. Dadurch können Projekte unwirtschaftlich werden und sogar scheitern. Eine

sachgerechte Projektorganisation mit einem gesamtverantwortlichen Projektleiter kann dem entgegenwirken.

Die **organisatorische und technische Umgebung**, in der die Verfahrensentwicklung durchgeführt wird, ist festzulegen und zu dokumentieren. Die Beschaffung und Pflege der Entwicklungsumgebung wird wegen ihrer Komplexität und des Kostenaufwandes häufig als eigenes IT-Vorhaben durchgeführt. Daher gelten die Anforderungen an die verfahrensspezifische Dokumentation auch für die Entwicklungsumgebung.

#### **b) Projektsteuerung**

Die **Projektsteuerung** soll einen ordnungsgemäßen und wirtschaftlichen Ablauf des Projektes sicherstellen. Zur Projektsteuerung zählen

- die Projektplanung,
- die Projektüberwachung,
- das Projektberichtswesen und
- die Wirtschaftlichkeitsbetrachtungen.

Die Projektsteuerung soll im Rahmen der projektbezogen festgelegten Rechte und Pflichten in der Verantwortung des Projektleiters liegen. Die projektsteuernden Aufgaben im einzelnen sollten vor Projektbeginn festgelegt werden. Ebenso sollten die Methoden und Werkzeuge zur Projektsteuerung bestimmt werden, die

- die Aufwandsschätzung,
- die Planung und Überwachung von Terminen und Aufwand sowie
- das Projektberichtswesen

unterstützen sollen.

Die **Projektplanung** ist die projektinterne Feinplanung des Projektablaufes und des Einsatzes der zugeordneten Ressourcen im Rahmen des Projektauftrages und der übergreifenden Planung der Vorhaben. Bei der Projektplanung sollen folgende Punkte berücksichtigt werden:

- Übereinstimmung mit der Rahmenplanung und der Planung der Vorhaben,
- Termine,
- Personal,
- Sachmittel und
- Aufwand und Haushaltsmittelverbrauch.

Der Detaillierungsgrad der Planung soll dem Planungszeitraum so angepaßt werden, daß die Planwerte hinreichend genau und begründbar sind.

Die Projektplanung ist im Projektverlauf ständig fortzuschreiben. Dabei sind die Zusammenhänge mit der IT-Gesamtplanung (Nr. 2.1) sowie die Verfügbarkeit und Qualifikation der Projektmitarbeiter zu beachten. Die Planung der Sachmittel muß deren Verfügbarkeit berücksichtigen. Die Planung des Aufwandes soll die benötigte Arbeits-

kapazität je beteiligter Stelle und die Kosten der Sachmittel unter Berücksichtigung der zur Verfügung stehenden Haushaltsmittel umfassen.

Als Methoden für eine Aufwandsschätzung sind z. B. zu nennen:

- Analogieverfahren
- Faktorverfahren
- Function Point-Methode.

Zur **Projektüberwachung** ist die Projektplanung regelmäßig und zeitnah einem Soll-Ist-Vergleich zu unterziehen. Der Projektleiter muß Maßnahmen zur Korrektur der Abweichung erarbeiten sowie die Planung entsprechend anpassen und fortschreiben.

Für die Planung und Überwachung von Terminen und Aufwand gibt es Werkzeuge, die mit unterschiedlicher Qualität und jeweils mehr oder weniger manueller Zuarbeit

- vorgegebene und errechnete Termine und Aufwände behandeln,
- vor Termin- und Aufwandsüberschreitungen warnen,
- die zeitlichen und logischen Abhängigkeiten von Ergebnissen und Tätigkeiten berücksichtigen,
- die Verfügbarkeit der Projektmitarbeiter und der Sachmittel berücksichtigen,
- Planungsalternativen simulieren helfen,
- Soll-Ist-Vergleiche erstellen,
- die Plandaten mehrerer zeitgleich durchgeführter und sachlich zusammenhängender Projekte verwalten und
- die Auswirkungen von Detailplanungen auf die Rahmenplanung automatisch fortschreiben.

Derartige Werkzeuge beruhen häufig auf Methoden der Netzplantechnik.

Im Rahmen des **Projektberichtswesens** muß der Projektleiter die Entscheidungsträger und die betroffenen Stellen nach der Erstellung der Projektplanung und dann in regelmäßigen Abständen oder bei wesentlichen Abweichungen über den Projektstand informieren. Dazu soll er die jeweils aktuell fortgeschriebene Projektplanung einschließlich des Soll-Ist-Vergleiches und ggf. der Beschreibung der eingeleiteten Maßnahmen verwenden. Andernfalls wird erst unmittelbar vor dem vorgesehenen Ende des Realisierungstermins deutlich, daß der Projektstand die Einführung des IT-Verfahrens nicht zuläßt. Für entsprechende Gegenmaßnahmen, z. B. die Verringerung des Funktionsumfangs auf ein unbedingt notwendiges Maß, ist es dann häufig zu spät.

Ein Projektberichtswesen soll möglichst wenig zusätzlichen Aufwand erzeugen und daher auf das sachlich notwendige Maß beschränkt werden. Es ist empfehlenswert, die Projektplanung so zu gestalten und zu dokumentieren, daß diese sich leicht für das Projektberichtswesen verwenden läßt.

Aus der Projektsteuerung ergeben sich Grunddaten für **Wirtschaftlichkeitsbetrachtungen** (siehe Anhang 4). Diese Daten können entsprechend dem Projektfortschritt genauer bestimmt werden. Im Verlauf eines Projektes kann es, z. B. durch Mehraufwand, Verzögerungen, Änderungen des organisatorischen Umfeldes oder durch Verfahrens-

funktionen, die nicht wie vorgesehen realisiert werden können, dazu kommen, daß Mehrkosten entstehen oder nur ein geringerer Nutzen als vorgesehen zu erwarten ist und die Wirtschaftlichkeit des Vorhabens nicht mehr gegeben ist. Nutzen-Kosten-Untersuchungen sind daher entsprechend anzupassen. Auch im Hinblick auf eine Erfolgskontrolle (Nr. 5) sind wirklichkeitsnahe Wirtschaftlichkeitsbetrachtungen unerlässlich. Sie sollten im Projektberichtswesen berücksichtigt werden.

### 3.3 Vor- und Hauptuntersuchung

- 3.3.1 *Vor der Ausführung eines IT-Vorhabens sind grundsätzlich eine Vor- und eine Hauptuntersuchung durchzuführen.*
- 3.3.2 *Zweck der Voruntersuchung ist es, überschlägig festzustellen, ob und durch welche Lösungsvarianten der Einsatz von IT zur Erfüllung einer Aufgabe fachlich und technisch durchführbar, zweckmäßig und wirtschaftlich ist. Auf dieser Grundlage ist zu entscheiden, ob und für welche Lösungsvarianten eine Hauptuntersuchung gerechtfertigt ist.*
- 3.3.3 *Zweck der Hauptuntersuchung ist es, aufbauend auf den Ergebnissen der Voruntersuchung ins Einzelne gehende Untersuchungen durchzuführen.*
- 3.3.4 *Vor- und Hauptuntersuchungsbericht sollen in entsprechend grober bzw. detaillierter Form insbesondere enthalten:*
- Bezeichnung des Vorhabens, Bearbeiter oder Arbeitsgruppe,*
  - Zielsetzung, Inhalt und Umfang des Vorhabens,*
  - Ist-Analyse mit einer Beschreibung und Bewertung der gegenwärtigen Aufbau- und Ablauforganisation aus technischer und organisatorischer Sicht,*
  - Darstellung der Gestaltungsalternativen unter Berücksichtigung der Möglichkeiten des Einsatzes vorhandener Verfahren oder Verfahrensteile sowie von Standard- oder Fremdsoftware und mögliche Übernahme von Datenbeständen,*
  - Soll-Vorschlag mit einem Entwurf der neuen Aufbau- und Ablauforganisation, zu beachtender oder zu ändernder Vorschriften, Beschreibung des systemtechnischen Konzepts und der Anforderungen an die Hardware-Konfiguration und die System- und Anwender-Software, Entwurf der Datenbasis (u.a. Datenorganisation, Mengengerüst), des Datenflusses und der Informationsbeziehungen,*
  - Darlegung der aus einer Risikoanalyse abgeleiteten Maßnahmen zur Gewährleistung von Ordnungsmäßigkeit und Sicherheit des Verfahrens,*
  - Zeit-, Personal- und Sachmittelbedarf für die Durchführung des Vorhabens einschließlich der Schulungsmaßnahmen, der räumlichen Ausstattung, etwaiger baulicher Maßnahmen und für den Verfahrensbetrieb,*
  - Wirtschaftlichkeitsuntersuchung sowie in geeigneten Fällen eine Nutzen-Kosten-Untersuchung.*
- 3.3.5 *Vor- und Hauptuntersuchung können – soweit dies sachlich gerechtfertigt ist – unter Darlegung der Gründe zusammengefaßt werden.*



*3.3.6 Die Ergebnisse der Vor- und der Hauptuntersuchung sind jeweils in einem Bericht zu dokumentieren. Die Berichte enden mit einem Entscheidungsvorschlag. Die Entscheidung ist schriftlich festzuhalten.*

In welchem Umfang Vor- und Hauptuntersuchung durchgeführt werden, ist von der Art und der Bedeutung des IT-Vorhabens abhängig. Der Aufwand für die Untersuchung muß in jedem Fall in einem wirtschaftlich angemessenen Verhältnis zum Entwicklungsaufwand und zur Bedeutung des zu entwickelnden Verfahrens stehen (Nr. 3.3.1 und Nr. 3.3.5). Dementsprechend ist auch zu überlegen, in welchem Umfang und mit welchem Detaillierungsgrad die in Nr. 3.3.4 aufgeführten Unterlagen zu erstellen sind. Zusätzlich zu den unter Nr. 3.3.4 genannten Ergebnissen können je nach Verfahren, Detaillierungsgrad des Entwurfs und nach den eingesetzten Werkzeugen noch weitere Teile zur Dokumentation der Ergebnisse von Vor- und Hauptuntersuchung gehören (siehe auch Anhang 3).

Bei der Voruntersuchung und der Hauptuntersuchung, die auf den Ergebnissen der Voruntersuchung aufbaut, sind gemäß den geforderten Ergebnissen (Nr. 3.3.4) jeweils mit angemessenem Aufwand grundsätzlich folgende Tätigkeiten erforderlich (Nr. 3.3.2 und Nr. 3.3.3):

- Ist-Erhebung und -Analyse der bestehenden Verfahren aus technischer und organisatorischer Sicht unter Beachtung der bestehenden Berührungspunkte zu anderen Verfahren (bei der Hauptuntersuchung detaillierter, da aufbauend auf der groben Ist-Erhebung und -Analyse aus der Voruntersuchung),
- fachlicher Grobentwurf des Verfahrens mit der Festlegung und Gliederung der benötigten Funktionen und Informationen aus fachlicher Sicht auf der Basis der Ist-Analyse unter Berücksichtigung der rechtlichen und fachlichen Anforderungen an den Soll-Zustand,
- technischer Grobentwurf des Verfahrens mit der aus dem fachlichen Grobentwurf abgeleiteten Zuordnung von Funktionen zu Programmen oder Modulen und von Informationen zu Dateien oder Datenbanken sowie der Ermittlung der erforderlichen Hardware- und Systemsoftwareumgebung unter Berücksichtigung der technischen Anforderungen an den Soll-Zustand,
- fachlicher Entwurf (ggf. als Feinentwurf) des Verfahrens, insbesondere mit der detaillierten Festlegung
  - o des Informationsflusses,
  - o der Verarbeitung,
  - o des Automatisierungsgrades,
  - o des Bildschirm-, Listen- und Formularaufbaus,
  - o der maschinellen und manuellen Kontrollen und Abstimmungen,
  - o der Behandlung fachlicher Fehler,
  - o der Zugriffsberechtigungen und Vollmachtregelungen,sowie
- technischer Entwurf (ggf. als Feinentwurf) des Verfahrens, insbesondere mit der aus dem fachlichen Feinentwurf abgeleiteten detaillierten Festlegung

- o des Datei- und Datenbankaufbaus,
- o der Programm- und Modulvorgaben,
- o der Maßnahmen zum Schutz der Daten vor unberechtigter Kenntnisnahme, Verfälschung und Verlust,
- o der Behandlung technischer Fehler mit Berücksichtigung der Wiederherstellung eines gültigen Datenbestandes und dem Wiederanlauf des Verfahrens (siehe auch Nr. 7.2.2 bis Nr. 7.2.4).

Unabhängig von der Größe des Vorhabens sind stets erforderlich:

- die Abgrenzung des Vorhabens (gegen andere Vorhaben),
- eine grobe Ist-Erhebung oder -Analyse des bestehenden Verfahrens aus technischer und organisatorischer Sicht unter Beachtung der Berührungspunkte zu anderen Verfahren sowie
- eine grobe Soll-Konzeption mit Ermittlung der Anforderungen und Wünsche an das neue bzw. zu ändernde Verfahren und Überlegungen zur technischen und organisatorischen Durchführbarkeit unter Beachtung der bestehenden und entstehenden Berührungspunkte zu anderen Verfahren.

Der Entwurf muß auch die Erfordernisse des Verfahrensbetriebes, insbesondere die Ablaufsteuerung und -kontrolle, sowie die optimale Ausnutzung der Hardware und Systemsoftware (IT-Basissystem, siehe Nr. 1.2) beachten. Die Anforderungen des Fachbereiches in Bezug auf die Benutzerfreundlichkeit und die Einbindung des zu entwickelnden Verfahrens in die tatsächlichen Arbeitsabläufe im Fachbereich sind ebenfalls zu berücksichtigen. Personal aus dem Bereich Verfahrensbetrieb oder dem Fachbereich kann zu diesem Zweck als Projektmitarbeiter oder Ansprechpartner in die Projektarbeit eingebunden werden (siehe auch Nr. 3.2). In der Regel werden die (groben) fachlichen Anforderungen der Fachseite in einem iterativen Vorgehen in einen detaillierten fachlichen Feinentwurf umgesetzt. Bei größeren Vorhaben werden dabei automatisierte Werkzeuge z.B. für die grafische Darstellung des Informationsflusses eingesetzt. Wenn diese Umsetzung – insbesondere bei größeren Vorhaben – vom Entwicklungsbereich durchgeführt wird, muß auch dann das Ergebnis (der fachliche Feinentwurf) für die Mitarbeiter des Fachbereiches verständlich, nachvollziehbar und prüfbar sein, um Mängel der fachlichen Spezifikation möglichst frühzeitig erkennen zu können. In der Regel erfordert dies die Ausbildung der Fachbereichsvertreter in den eingesetzten Methoden und Werkzeugen. Spezifikationsmängel sind nach Fertigstellung der Verfahren in der Regel nur mit sehr hohem Aufwand zu beseitigen. Eine Möglichkeit, den fachlich Zuständigen möglichst frühzeitig eine Anschauung von der technischen Realisierung zu geben, ist die modellhafte Entwicklung wesentlicher Funktionen des Systems (Prototyping), z. B. wichtiger Eingabefunktionen.

Anhang 3 enthält Beispiele für Entwurfsmethoden und entsprechende Werkzeug.

Da auch die möglichen Sicherheitsmaßnahmen maßgeblich durch den Entwurf festgelegt werden, sind fachliche und technische Risiken soweit erforderlich bereits beim Verfahrensentwurf in einer verfahrensbezogenen Risikoanalyse zu ermitteln. Die Maßnahmen, die sich aus der Risikoanalyse ergeben, müssen in Form eines verfahrensspe-

zifischen Sicherheitskonzeptes in den Entwurf eingebracht werden. Die verfahrenübergreifende Risikoanalyse und das verfahrenübergreifende Sicherheitskonzept sind dabei als Grundlage heranzuziehen (siehe Nr. 7.2). Im Rahmen des Sicherheitskonzeptes sind auch die nach Durchführung der Maßnahmen verbleibenden Restrisiken in die Entscheidung zur Fortführung des Projektes einzubeziehen. Bei Netzen und dem Einsatz von APC gehen die IT-Mindestanforderungen direkt auf Risiken und ihre Bedeutung für eine Zielkonzeption ein (siehe Nr. 4.4.5 und Nr. 4.5.3). Ggf. ist das verfahrenübergreifende Sicherheitskonzept im Hinblick auf die verfahrensbezogenen Anforderungen anzupassen.

Die Tätigkeiten im Rahmen einer Vor- und Hauptuntersuchung müssen ausreichend sichere Informationen für die jeweiligen Wirtschaftlichkeitsbetrachtungen liefern und damit eine Entscheidungsbasis für die Fortführung oder Einstellung des Vorhabens bieten.

Eine Wirtschaftlichkeitsbetrachtung mit der Darstellung von Kosten und Nutzen muß grundsätzlich für jedes einzelne Vorhaben angestellt werden. In die Kosten sollten sämtliche Aufwendungen für Personal und Sachmittel für Entwicklung und Betrieb des Verfahrens einfließen. Der Nutzen soll quantifizierbare und nicht quantifizierbare Vorteile aufzeigen. Nicht quantifizierbarer Nutzen soll – z. B. über Punktbewertungsverfahren – soweit wie möglich quantifizierbar gemacht werden (Hinweise zu Wirtschaftlichkeitsbetrachtungen enthält Anhang 4).

Bei Änderungen der Gesamtplanung, der Planung einzelner Vorhaben, bei Beginn eines Projektes und ggf. bei wesentlichen kosten- oder nutzenrelevanten Änderungen sollten Wirtschaftlichkeitsbetrachtungen fortgeschrieben werden. Es empfiehlt sich zudem, bei kostenintensiven Verfahren in regelmäßigen Abständen Kosten und Nutzen der bestehenden Verfahren mit Kosten und Nutzen möglicher Alternativen – z. B. Neuentwicklung, Weiterentwicklung oder Ablösung durch Fremdsoftware – zu vergleichen und ggf. entsprechende Maßnahmen zu ergreifen, um nicht mehr zeitgemäße oder unwirtschaftliche Verfahren rechtzeitig ablösen zu können (siehe auch Nr. 3.2, Nr. 5 und Nr. 6).

Beim technischen Entwurf ist die Möglichkeit des Einsatzes von Fremdsoftware, d. h. von nicht in der eigenen Verwaltung neu zu entwickelnder Software, für das gesamte Verfahren oder für einzelne Teile zu prüfen. Bei positivem Ergebnis ist die geeignete Fremdsoftware systematisch auszuwählen. Die Anforderungen an eine Auswahl sind unter Nr. 3.4.2 dargestellt.

Ggf. muß die bis dahin vorliegende IT-Planung (Nr. 2.1 und Nr. 2.2) aufgrund der Ergebnisse der Vor- und der Hauptuntersuchung fortgeschrieben werden.

## 3.4 Ausführung eines IT-Vorhabens

### 3.4.1 Grundsätzliches

3.4.1.1 Aufgrund des Ergebnisses der Hauptuntersuchung ist über die Ausführung eines IT-Vorhabens zu entscheiden. Die Ausführung umfaßt insbesondere

- Beschaffung von Hard- und Software,
- Vergabe von Entwicklungsaufträgen und/oder Verfahrensentwicklung einschließlich Programmierung,
- Test und Freigabe sowie
- Einführung des Verfahrens.

3.4.1.2 Die Einzelheiten der Ausführung eines IT-Vorhabens sind jeweils zu dokumentieren.

Ergebnis der Ausführung eines IT-Vorhabens ist ein in einer Organisation eingeführtes Verfahren, das auf der getesteten und freigegebenen Software beruht. Diese Verfahrensoftware muß in der Lage sein, die zu erfüllenden Aufgaben richtig, vollständig, sicher, in angemessener Zeit und zu angemessenen Kosten zu erfüllen und die Verfahrensergebnisse in der vom Fachbereich benötigten Form zur Verfügung zu stellen. Dabei ist von den in der Vor- und Hauptuntersuchung getroffenen Festlegungen auszugehen (siehe Nr. 3.3). Die Aufgabengerechtigkeit kann insbesondere durch eine geordnete Vorgehensweise bei Ausführung des Vorhabens (siehe auch Nr. 3.1 und Nr. 3.2) mit Einbindung der fachlich zuständigen Bereiche und mit entsprechender Gestaltung des Systems aus Hardware und Systemsoftware gefördert werden (Nr. 3.4.2).

Grundsätzlich muß die Verfahrensoftware so gestaltet sein, daß das Verfahren unter optimaler Ausnutzung des Systems aus Hardware und Systemsoftware auch in Spitzenzeiten termingerecht und sicher abgewickelt werden kann.

Im Hinblick auf die Aufgabengerechtigkeit und die Sicherheit ist auch dafür zu sorgen, daß die Verfahrensoftware ausschließlich die ihr gestellten Aufgaben erfüllt (Vermeidung von unerwünschten Nebenwirkungen, siehe Nr. 3.4.5).

Die im Sicherheitskonzept (Nr. 7.2) festgelegten Maßnahmen sind bei der Ausführung des Vorhabens angemessen zu berücksichtigen. Erfahrungsgemäß führt das nachträgliche Einbringen von Sicherheitsmechanismen zu Mehrkosten und häufig auch zu Sicherheitslücken, da die technischen Optimierungsmöglichkeiten mit fortschreitender Ausführung eines IT-Vorhabens geringer werden (siehe auch Nr. 3.3).

Im Zusammenhang mit der Ausführung des Vorhabens sind alle vorhabenbezogenen Sachverhalte zu beschreiben, die sich nicht in den Ergebnissen der Verfahrensentwicklung wiederfinden (Nr. 3.4.1.2). Das bedeutet, daß der Verlauf der Arbeiten im Hinblick auf

- die Planungs-, Abstimmungs- und Entscheidungsvorgänge,
- den Mittelverbrauch für Personal und Sachmittel in Verfahrensentwicklung und -betrieb sowie
- die aufgetretenen Probleme, z. B. bei Aufwand oder Terminen,

so zu dokumentieren ist, daß die Entwicklung nachvollziehbar und die Fortführung der Arbeiten durch andere Personen sichergestellt ist.

Alle wesentlichen Änderungen der geplanten Vorgehensweise oder der Ergebnisse bei der Ausführung eines IT-Vorhabens bedürfen einer Abstimmung mit den zuständigen Bereichen.

### 3.4.2 Beschaffung von Hard- und Software

*Bei der Hardware ist unter dem Gesichtspunkt der Wirtschaftlichkeit die günstigste Gerätekonfiguration und Beschaffungsart (Kauf, Miete, Leasing) auszuwählen. Das System aus Hard- und Software soll ausreichend dimensioniert und erweiterbar sein. Die Abhängigkeit von einzelnen Herstellern ist soweit wie möglich zu vermeiden. Die Bestandteile des Systems aus Hard- und Software sollen untereinander und mit bereits vorhandenen Komponenten und Verfahren verträglich (kompatibel) sein.*

Bei der Beschaffung von Hardware und Software wird entsprechend den begrifflichen Erläuterungen in Nr. 1.2 zweckmäßigerweise zwischen der Beschaffung des IT-Basis-systems (Hardware und Systemsoftware) und der Anwendungssoftware unterschieden.

Aufgrund seiner Komplexität und engen Verbindung mit allen – auf dem System ablaufenden oder mit ihm zusammenhängenden – IT-Verfahren ist die **Beschaffung des IT-Basissystems** von besonderem Interesse für die Prüfung.

Die wirtschaftliche Beschaffung des IT-Basissystems setzt eine ausreichend langfristig angelegte Planung voraus, die im Einklang mit der Gesamtplanung (Nr. 2.1) stehen muß. Bei der Planung des IT-Basissystems müssen in einer Bedarfsanalyse

- die Zielvorstellungen zur Leistung des Systems,
- die Anforderungen der vorhandenen und geplanten Vorhaben und Verfahren,
- die erforderliche und künftige Kapazität,
- die technische Ausgestaltung und
- die Beschaffungsalternativen (z. B. Kauf oder Miete)

berücksichtigt werden. Aus der Planung sollten die einmaligen und die laufenden Kosten erkennbar sein.

Die Planung muß einerseits den Funktions- und Kapazitätsbedarf für den Betrieb und die Pflege vorhandener Verfahren berücksichtigen. Dabei sind auch wegfallende Kapazitäten oder nicht mehr benötigte Software durch einzustellende oder abzulösende Verfahren zu beachten. Andererseits sind die aus der Gesamtplanung abzuleitenden

Funktions- und Kapazitätsanforderungen für die Entwicklung, den Betrieb und die Pflege neuer oder wesentlich geänderter Verfahren einzubeziehen (siehe auch Nr. 2.1 und Nr. 2.2).

Im Rahmen der Gesamtplanung ist ein Konzept für das Basissystem aufzustellen, das die grundlegenden Ressourcen für Entwicklung und Betrieb von Verfahren festlegt und ihre Kompatibilität gewährleistet. Das Konzept muß die aus der Gesamtplanung zu folgernden Anforderungen berücksichtigen, langfristige Gültigkeit haben und zukunftsorientiert sein. Auf die entsprechenden Ausführungen in Nr. 11, Nr.12 und Nr. 23 der IT-Richtlinien wird hingewiesen.

Aus dem Konzept soll insbesondere hervorgehen,

- welche Systembestandteile erforderlich sind und eingesetzt werden sollen,
- welche Erweiterungsmöglichkeiten bestehen,
- welche Aufgaben die einzelnen Systembestandteile erfüllen sollen,
- wie die einzelnen Systembestandteile, z. B. die Hardware in einem Netzwerk oder die Softwarekomponenten, verbunden werden sollen und
- welche Anforderungen – vor allem in Bezug auf verwaltungs- bzw. herstellerspezifische, nationale oder internationale Normen, Standards und Konventionen – bei der Auswahl zu stellen sind (siehe auch Nr. 2.1.2).

Die Abhängigkeit des IT-Basissystems von einzelnen Systembestandteilen und die Herstellerabhängigkeit können durch die Beachtung von Standards, Normen und Konventionen und einer klaren funktionalen Gliederung des Systems mit festgelegten, standardisierten Schnittstellen der einzelnen Bestandteile verringert werden. Ist eine vollständige Herstellerunabhängigkeit nicht zu erreichen, soll durch die Auswahl von Herstellern, deren Fortbestand gesichert erscheint, und vertragliche Regelungen die Unterstützung der wesentlichen Systembestandteile langfristig gesichert werden.

Die Kompatibilität muß auch bei Erweiterungen oder dem Austausch einzelner Bestandteile erhalten bleiben. Die Beschaffung der Bestandteile bei einem Hersteller kann die Kompatibilität fördern, führt aber ggf. zu einer Abhängigkeit von diesem Hersteller und zu unwirtschaftlichen Beschaffungen. Die Beschaffung von Teilen des IT-Basissystems soll daher anhand eines funktionsorientierten Anforderungskataloges, der auch Normen und Standards sowie die Schnittstellen beachtet, grundsätzlich im Wettbewerb geschehen. Liefertermine sowie Qualität und Umfang der Lieferung sind zu kontrollieren.

Bei örtlich verteilt eingesetzten (dezentralen) Systemen ist die Übereinstimmung zwischen Konzept, Planung und Beschaffung zweckmäßigerweise über die Zuständigkeit einer zentralen Stelle sicherzustellen.

Das IT-Basissystem muß eine den abzuwickelnden Verfahren angemessene Sicherheit im Hinblick auf den Schutz der Daten vor unberechtigter Kenntnisnahme, Verfälschung und Verlust sowie im Hinblick auf die Richtigkeit und Zuverlässigkeit der Funktionen bieten. Insbesondere die Regelung von Zugriffsberechtigungen auf Datenbestände und Programme soll unumgebar vorgeschrieben werden können. Die Datensicherheit soll

vom System durch entsprechende Hardware und Systemsoftware unterstützt werden (siehe auch Nr. 7).

Auch die Zuverlässigkeit des Systems muß bei der Beschaffung bedacht werden. Da in der Regel mehrere Verfahren auf einem Basissystem betrieben werden, ist die Stabilität am Bedarf des Verfahrens mit den höchsten Ansprüchen an die Zuverlässigkeit zu orientieren. Wenn die Anforderungen an die Sicherheit zu unterschiedlich sind, müssen ggf. aus wirtschaftlicher Sicht getrennte IT-Basissysteme eingesetzt werden, um den verfahrensspezifischen Gegebenheiten Rechnung tragen zu können. So werden typischerweise VS-Daten oder auch die Aufgaben der Netzsteuerung auf gesonderten IT-Systemen bearbeitet.

Maßnahmen zur Förderung der Stabilität bei der Beschaffung von Hardware und Software können grundsätzlich sein:

- die Auswahl erprobter Hardware und Systemsoftware,
- eine an den Sicherheitserfordernissen, insbesondere Ausfallhäufigkeit der Systemteile, orientierte Wartung sowie
- eine geordnete Vorgehensweise bei der Änderung des Systems mit hinreichenden Tests (siehe auch Nr. 3.5).

Das IT-Basissystem muß so ausgelegt sein, daß die zu betreibenden Verfahren sachgerecht abgewickelt werden können. So ist bei Dialogverfahren eine angemessene, den Arbeitsablauf nicht hemmende Antwortzeit zwischen Benutzereingabe und Systemausgabe einzuhalten. Alle vorhersehbaren Belastungsspitzen dürfen nicht zu einer unangemessenen Überlastung einzelner Systembestandteile oder des Systems führen. Ebenso wie eine Unterkapazität ist allerdings auch eine Überkapazität aus Gründen der Wirtschaftlichkeit zu vermeiden.

Erweiterungen oder der Austausch einzelner Bestandteile des IT-Basissystems sollten insbesondere keine Änderungen der Verfahrenssoftware notwendig machen. Wenn die Grenzen der Erweiterbarkeit im Rahmen der erwarteten Entwicklung mittelfristig erreicht werden, soll eine Überarbeitung des Konzeptes und ein rechtzeitiger Wechsel der betroffenen Systembestandteile vorgenommen werden. Ggf. soll auch die Möglichkeit der Verkleinerung des Systems bei sich verringernden Anforderungen in die Überlegungen einbezogen werden.

Wenn Anwendungssoftware beschafft werden soll, müssen die Anforderungen bereits vor der Untersuchung ggf. geeigneter Produkte festgelegt werden. Die Anforderungen können z. B. aus dem fachlichen und technischen Entwurf abgeleitet werden (siehe Nr. 3.3.4). Ggf. sind die Anforderungen im Verlauf des Auswahlverfahrens anzupassen.

Besondere Berücksichtigung muß bei der Beschaffung die Verträglichkeit der Software mit der vorhandenen Hardware- und Softwareumgebung finden. Ein Anpassungsaufwand sollte möglichst gering gehalten werden, da andernfalls die Vorteile des Softwarekaufs, wie z. B. die schnellere und häufig wirtschaftlichere Bereitstellung der Software, nicht mehr ins Gewicht fallen.

Bei den Anforderungen wird zweckmäßigerweise zwischen Muß- und Kann-Anforderungen unterschieden, da eine vorgefertigte Software in der Regel nicht alle Anforderungen gleichermaßen abdeckt. Die Muß-Anforderungen muß die auszuwählende Software uneingeschränkt erfüllen; Kann-Anforderungen sollen erfüllt werden, können aber ganz oder teilweise entfallen. Für die Kann-Anforderungen kann eine Gewichtung, z. B. über ein Punktbewertungsverfahren, festgelegt werden. Bei der Auswahl sollen grundsätzlich mehrere Möglichkeiten berücksichtigt werden. Dadurch können Vor- und Nachteile der Alternativen klarer erkannt werden. Auch bei dezentralen Verfahren sollte Fremdsoftware zentral ausgewählt werden, um die Konsistenz mit der Gesamtplanung sicherzustellen.

Bei größeren Beschaffungen ist ein Probetrieb im Rahmen der Angebotsauswertung zweckmäßig, um die Erfüllung der Anforderungen prüfen zu können.

Hardware und Software soll grundsätzlich im Wettbewerb beschafft werden.

In jedem Einzelfall sollte die günstigste Beschaffungsart geprüft werden. Erfahrungsgemäß erweist sich in der IT häufig der Kauf bereits bei einer Nutzungszeit von weniger als 3 Jahren als günstiger als die Miete (siehe auch Anhang 4).

Wenn die Unterschiede zwischen den einzelnen Beschaffungsarten kostenmäßig nur gering sind, muß eine Entscheidung anhand anderer Kriterien, wie Flexibilität, Handhabung der Verträge oder Herstellerunabhängigkeit, getroffen werden.

In vielen Behörden besteht, z. B. aufgrund der Auswahl eines bestimmten Betriebssystems, eine Abhängigkeit von einzelnen Herstellern. Zudem läßt die Angebotspolitik mancher Hersteller bei einzelnen Komponenten mitunter die freie Wahl zwischen unterschiedlichen Beschaffungsarten nicht zu. In diesen Fällen kann langfristige auf den Einsatz weitgehend standardisierter Produkte hingewirkt werden. Voraussetzung dafür ist, daß die Programme der eingesetzten Verfahren eine Übertragung auf andere IT-Basisssysteme auf wirtschaftliche Weise zulassen (siehe Nr. 3.4.4).

Beim Übergang von IT-Anlagen in das Eigentum der Behörden ist das Problem zu sehen, daß die Geräte am Ende ihrer wirtschaftlichen Nutzungszeit veräußert oder entsorgt werden müssen. Dadurch entstehende Einnahmen oder Ausgaben sind möglichst bei den Wirtschaftlichkeitsbetrachtungen zu berücksichtigen. In Einzelfällen kann dies außerordentlich schwierig sein, da die Marktentwicklung nicht für den gesamten Nutzungszeitraum vorhergesagt werden kann.

### 3.4.3 Vergabe von Entwicklungsaufträgen

*Externe Stellen sollen nur dann eingesetzt werden, soweit eigene Mitarbeiter für die ordnungsgemäße Erfüllung des Vorhabens nicht zur Verfügung stehen oder die Einschaltung aus besonderen Gründen geboten ist. Werden IT-Vorhaben, insbesondere die Entwicklung von Software, an externe Stellen vergeben, so ist grundsätzlich die Beachtung dieser Mindestanforderungen sicherzustellen. Die Abwicklung solcher Vorhaben ist entsprechend zu überwachen.*



Der Einsatz von nicht zum eigenen Personal zählenden (externen) Mitarbeitern und externen Stellen, z. B.

- freie Mitarbeiter,
- Serviceunternehmen und
- Unternehmensberatungen,

soll nur mit zeitlich begrenzter Aufgabenstellung und nur unter den genannten Bedingungen in Anspruch genommen werden. Besondere Gründe können insbesondere fehlendes Spezialwissen, zu geringe Qualifikation der eigenen Mitarbeiter, kurzfristige Bedarfsspitzen oder Kostenvorteile sein. Grundsätzlich ist davon auszugehen, daß der Einsatz des eigenen Personals kostengünstiger ist. Dieser Kostenvorteil kann jedoch durch schnellere Bereitstellung der Ergebnisse oder ggf. bessere Qualität der Arbeiten ausgeglichen werden.

Die Vergabe von Aufträgen soll grundsätzlich im Wettbewerb erfolgen.

Im Rahmen einer Auftragserteilung sind detaillierte Festlegungen zu treffen, insbesondere über

- die zu erfüllenden Aufgaben,
- die einzuhaltenden Termine,
- die einzuhaltenden Kosten,
- die Zahlungsbedingungen,
- das Abstimmungs- und Abnahmeverfahren für die Ergebnisse,
- die fachliche Kontrolle und Führung,
- das Berichtswesen,
- die Gewährleistungsbestimmungen sowie
- die Einhaltung maßgeblicher Regelungen, z. B. für die Dokumentation.

Bei komplexen Entwicklungsvorhaben ist es häufig nicht möglich, bereits bei Beginn der Arbeiten die erwarteten Ergebnisse mit ausreichender Genauigkeit zu beschreiben. Zudem ändern sich die fachlichen Anforderungen während der oft sehr langen Entwicklungszeiten. Es werden Nacharbeiten erforderlich, die in der Regel – zumindest kurzfristig – nur von dem beauftragten externen Unternehmen durchgeführt werden können. Der Auftragnehmer kann dann den Aufwand und damit die Kosten für die Arbeiten maßgeblich mitbestimmen, während eine Vergabe der Arbeiten im Wettbewerb faktisch nicht möglich ist. Es empfiehlt sich daher, größere Vorhaben möglichst in zeitlich und inhaltlich überschaubaren Abschnitten abzuwickeln, deren Ergebnis kontrollierbar ist (siehe auch Nr. 3.2). Zudem sollten mehrere Änderungsanforderungen – soweit keine zwingenden Gründe wie z. B. Terminvorgaben bestehen – zusammengefaßt und erst nach Abschluß der vorangegangenen Vorhabensabschnitte eingebracht werden (Release- oder Versionenkonzept). Einzelne Vorhabensabschnitte oder die Erstellung bestimmter Verfahrensvarianten können dann im Wettbewerb vergeben werden.

Auf die von der KBSt herausgegebenen Besonderen Vertragsbedingungen für die Beschaffung und den Betrieb von DV-Leistungen (BVB) wird hingewiesen.

Die Arbeitsergebnisse sollen zeitnah bezüglich

- der qualitativen und quantitativen Anforderungserfüllung,
- der Terminerfüllung,
- der Kosteneinhaltung und
- der Einhaltung dieser Mindestanforderungen

überwacht werden. Die Leistung darf erst abgenommen werden, wenn die im Abstimmungs- und Abnahmeverfahren festgelegten Kriterien erfüllt sind. In den Verträgen sollen Regelungen für den Fall einer teilweisen oder vollständigen Nichtabnahme der Leistungen vorgesehen werden.

Verfahren sollten grundsätzlich mit eigenem Personal gepflegt werden. Wenn externe Mitarbeiter in großem Umfang eingesetzt werden, geht häufig Know-how bei den eigenen Mitarbeitern verloren. Zu starker Abhängigkeit von den externen Mitarbeitern beim späteren Verfahrensbetrieb kann mit einer kontinuierlichen und nachhaltigen Mitwirkung eigener Kräfte in den Vorhaben entgegen gewirkt werden.

#### *3.4.4 Entwicklung eines Verfahrens einschließlich Programmierung*

*3.4.4.1 Es sind Regelungen zur Erstellung von Programmen und zur Verwendung von Programmiersprachen zu treffen, die der Vereinfachung, Vereinheitlichung und Standardisierung des Programmierens und der Programme dienen.*

*3.4.4.2 Programme sollen im Hinblick auf Ordnungsmäßigkeit, Sicherheit und Wirtschaftlichkeit der Entwicklung, der Pflege und des Betriebs aus eigenständig änder- und testbaren Programmbestandteilen mit definierten Berührungspunkten (Schnittstellen) aufgebaut werden. Die Programme sind nach den Vorgaben so zu entwickeln, daß sie von einem anderen Programmierer fortgeführt werden können.*

*3.4.4.3 Der Benutzerfreundlichkeit der IT ist besondere Beachtung zu schenken. Es sind Festlegungen insbesondere für*

- das Aufbauschema von Bildschirmmasken,*
  - die allgemeingültigen Funktionstasten und Kommandos,*
  - die Meldungen für die Benutzer und das Betriebspersonal,*
  - die Fehlerbehandlung,*
  - die Hilfefunktion und*
  - das Aufbauschema von Druckausgaben*
- zu beachten oder zu treffen.*

3.4.4.4 Die Verfahrensdokumentation muß alle Verfahrensfunktionen, insbesondere die der Programme, nachvollziehbar belegen. Zur Verfahrensdokumentation gehören u.a.:

- Auftrag und Aufgabenstellung,
- Kennziffern-, Schlüssel-, Symbol- und Abkürzungsverzeichnisse,
- Beschreibung der Dateien und ggf. der Datenbanken bis zur Tiefe der Datenfeldebene mit Angaben zum Aufbau sowie Beschreibung von Maßnahmen zum Schutz und zur Archivierung der Daten,
- Verzeichnis der Programme bzw. der Programmteile in ihren jeweils gültigen Versionen,
- eine Darstellung aller programmierten und organisierten Kontrollen,
- Darstellung des Programmablaufs und des Datenflusses, ggf. Auflistung der Primärprogramme mit Programmübersetzung,
- Beschreibung der Bildschirmmasken, Listen und Formulare,
- Darstellung der Einbindung in das technische Umfeld und der technischen Berührungspunkte zu anderen Verfahren und Beschreibung der Überleitung in andere technische Umgebungen,
- Dienst-, Arbeits- und Bedienungsanweisungen sowie Änderungsaufträge und -nachweise.

Vereinfachung, Vereinheitlichung und Standardisierung des Programmierens und der Programme sollen dazu beitragen, die Software-Qualitätskriterien

- Aufgabengerechtigkeit,
- Stabilität,
- Änder- und Erweiterbarkeit sowie
- Übertragbarkeit und
- Personenunabhängigkeit

zu erreichen. Häufig werden Festlegungen für die Methoden der Programmierung verfahrensbezogen oder von jeder Organisationseinheit gesondert getroffen. Dadurch wird der Personaleinsatz bei der Programmerstellung erschwert und zusätzlicher Einarbeitungsaufwand notwendig (siehe auch Nr. 3.2 und Nr. 3.4.1).

Die bei Standardprodukten vorhandenen Möglichkeiten der Programmierung mit eigenen Programmiersprachen, z. B. die Befehle einer Datenbankabfragesprache oder sog. Sprachen der 4. Generation, sind ebenso in einer Regelung zu berücksichtigen wie gängige Programmiersprachen, z. B. COBOL, da IT-Verfahren in der Regel auch Teile enthalten, die jeweils mit unterschiedlichen Programmiersprachen erstellt sind. Diese Regelung könnte z. B. im Vorgehensmodell (siehe Nr. 3.1) enthalten sein.

Unabhängig von der im einzelnen gewählten Methode sollen bei der Programmierung folgende Prinzipien beachtet werden:

- die Gliederung der Programme in eigenständige, mehrfach verwendbare Module,
- das Blockkonzept mit jeweils genau einem Eingang und Ausgang je Programm, Modul und Block innerhalb eines Moduls,
- die Verwendung weniger, einheitlicher Konstruktionselemente sowie
- die Lesbarkeit und Verständlichkeit des Quelltextes durch Kommentierung und Verwendung selbstbeschreibender Datennamen.

Einige Werkzeuge für die Programmierung sind in Anhang 3 beispielhaft aufgeführt.

Grundsätzlich sollten möglichst wenige Programmiersprachen für die Verfahrensentwicklung eingesetzt werden, sofern die Aufgabenstellungen dies zulassen, um den Programmieraufwand möglichst gering zu halten, den Personaleinsatz zu erleichtern und den Schulungsaufwand zu verringern. Unterschiedliche Aufgabenstellungen oder der Einsatz unterschiedlicher Standardwerkzeuge mit entsprechenden Programmiermöglichkeiten stehen dem häufig noch entgegen.

Die Programmierung muß den Programmvorgaben des technischen Entwurfes (Nr. 3.3) folgen. Fehler oder fehlende Punkte im fachlichen oder technischen Entwurf sind zunächst dort zu korrigieren bzw. zu ergänzen, bevor die Programmierung fortgesetzt wird. Das trägt dazu bei, die Entwurfsdokumentation und die Programme konsistent zu halten, womit eine wesentliche Voraussetzung für die Pflege und Änderung der IT-Verfahren geschaffen wird.

Die Abhängigkeit in der Pflege der Verfahrenssoftware von

- einem Hersteller,
- einzelnen Mitarbeitern oder
- Bestandteilen des IT-Basisystems (Hardware und Systemsoftware)

soll aus Gründen der Sicherheit und Wirtschaftlichkeit gering gehalten werden. Die Abhängigkeit kann verringert werden durch

- den Einsatz von standardisierten Programmiersprachen, wie COBOL oder SQL, mit der Beschränkung auf den standardisierten Sprachumfang,
- die Modularisierung der Verfahrenssoftware mit der Auslagerung systemspezifischer Funktionen, z. B. die Steuerung der Ein-/Ausgabe, in wenige austauschbare Module,
- die durchgängige Vermeidung von Personenabhängigkeiten durch eine geordnete Vorgehensweise bei der Verfahrensentwicklung und -pflege und einer vollständigen, nachvollziehbaren Dokumentation,
- den Einsatz von Programmgeneratoren und
- die Beachtung von verwaltungsspezifischen, nationalen und internationalen Standards, Normen und Konventionen.

Ist eine vollständige Unabhängigkeit nicht zu erreichen, sollte die Unterstützung der entsprechenden Bestandteile der Verfahrenssoftware oder des IT-Basisystems aus Hard-

ware und Systemsoftware durch die Bindung eines Herstellers, dessen Fortbestand gesichert erscheint, langfristig geregelt werden (siehe auch Nr. 3.4.2).

Benutzerfreundliche IT-Verfahren können den Arbeitsablauf fördern und die Wahrscheinlichkeit von Bedienungsfehlern verringern. Daher sollte die Verfahrenssoftware eine ergonomische, zweckmäßige, die Möglichkeiten des IT-Systems nutzende und verfahrenübergreifend einheitliche Benutzeroberfläche besitzen. Die Benutzeroberfläche und die Druckausgaben sollten die benötigten Informationen, insbesondere in Inhalt, Umfang und Zusammenfassungsgrad, aufgabengerecht und übersichtlich bereitstellen. Die allgemeinen Festlegungen zum Benutzeroberflächenstandard sind dabei zu beachten (siehe Nr. 3.1).

Die Programm- bzw. Moduldokumentation muß für jedes Programm bzw. Modul vollständig und auf dem neuesten Stand vorliegen, bevor es in den Verfahrensbetrieb übernommen werden kann (siehe Nr. 3.4.5).

Die IT-Mindestanforderungen beinhalten eine beispielhafte Aufzählung von Elementen einer Verfahrensdokumentation. Diese kann je nach den verwendeten Programmierwerkzeugen und der Systemumgebung unterschiedlich ausgestaltet sein.

Allgemein soll die verfahrensspezifische Dokumentation sicherstellen, daß

- das Verfahren ordnungsgemäß, sicher und wirtschaftlich betrieben werden kann,
- die Abstimmungsgrundlage für die am Projekt Beteiligten während der Verfahrensentwicklung gebildet und die von bestimmten Personen unabhängige Fortführbarkeit des Projektes gewährleistet wird (Nr. 3.4.4.1),
- das Verfahren auch nach dem Einsatz unabhängig von bestimmten Personen zuverlässig pflegbar ist (Nr. 3.4.4.2) und
- das Verfahren insgesamt oder anhand einzelner Fälle auf Ordnungsmäßigkeit, Sicherheit, Wirtschaftlichkeit prüfbar ist (Nr. 3.4.5).

Deshalb ist die verfahrensspezifische Dokumentation so zu gestalten und zu gliedern, daß die für die Verfahrensentwicklung und den -betrieb und die fachlich zuständigen Bereiche sowie interne und externe Prüfer die sie betreffenden Sachverhalte aus der Dokumentation entnehmen können (siehe auch Nr. 1.4 zu den Grundsätzen einer ordnungsgemäßen Dokumentation).

Auf dieser Grundlage sollten die fachlich zuständigen Bereiche im Rahmen der Abstimmung während des Verfahrensentwurfs entscheiden können, ob ihre Anforderungen berücksichtigt worden sind. Oft wird erst nach Fertigstellung der Programme klar, daß bereits der Entwurf nicht den fachlichen Vorstellungen entsprach; aufwendige Nachbesserungen sind dann die Folge.

### *3.4.5 Test und Freigabe*

*3.4.5.1 IT-Verfahren sind vor ihrer Freigabe für den Betrieb, bei komplexen Verfahren auch schrittweise während der Erstellung der Programme, in allen Funktionen*

zu testen. Dabei ist den Berührungspunkten zu anderen Verfahren und der späteren organisatorischen Einbindung in den Betrieb besondere Beachtung zu schenken. Mit Hilfe der Tests muß insbesondere auch sichergestellt werden, daß jedes Programm nur die erforderlichen, in Vorgaben festzulegenden Funktionen erfüllt und keine unerwünschten Nebenwirkungen beinhaltet. Tests müssen unter Berücksichtigung aller Hard- und Software-Komponenten so durchgeführt werden, daß der Verfahrensbetrieb nicht beeinträchtigt wird.

- 3.4.5.2 Tests müssen aufgrund von Testfällen mit im voraus festgelegten Eingaben und erwarteten Ausgaben durchgeführt werden. Die Ergebnisse des abschließenden Tests sind unter gebotener Beteiligung des Bereichs Datenverarbeitung von den am Vorhaben beteiligten Fachbereichen zu kontrollieren, zu bewerten und abzunehmen. Die fachlich zuständigen Stellen haben hierfür Testfälle zu erstellen, die hinsichtlich des technischen Ablaufs vom Bereich Datenverarbeitung zu ergänzen sind. Die Testfälle sollen wiederverwendet werden können.
- 3.4.5.3 Die Testergebnisse sind zu dokumentieren. Die Dokumentation über den Abschlußtest als Teil der Verfahrensdokumentation soll enthalten:
- den fachlichen und technischen Hintergrund für den Test (z. B. Einführung eines neuen Verfahrens, Fehlerkorrektur, wesentliche Änderung),
  - die Beschreibung der Testumgebung (getestete Programme mit Angabe der Versionen, getesteter Ablauf, die angeschlossenen Dateien und Datenbanken, die Hardware- und Systemsoftwareumgebung mit Angabe der Versionen),
  - die Testfälle mit Eingabe- und erwarteten Ausgabedaten,
  - die Testergebnisse einschließlich des Systemverhaltens und der Systemmeldungen mit der fachlichen und technischen Bewertung der Testergebnisse durch die am Test beteiligten Stellen sowie
  - die Abnahmeerklärung der beteiligten Stellen.
- 3.4.5.4 Die zuständige Stelle, in der Regel der federführende fachlich zuständige Bereich, gibt auf der Grundlage der Abnahmeerklärung zum Abschlußtest das Verfahren frei und übernimmt damit die Gesamtverantwortung für die Ordnungsmäßigkeit und die Sicherheit des Verfahrens.
- 3.4.5.5 Die Freigabebescheinigung als Teil der Verfahrensdokumentation muß enthalten:
- die Verfahrensbezeichnung,
  - den Anlaß für Test und Freigabe,
  - den Zeitpunkt für den erstmaligen Einsatz der betreffenden Verfahrensversion,
  - die genaue Bezeichnung der freigegebenen Programme mit Versionsnummern,
  - die Bestätigung, daß die vorgeschriebenen Prüfungen durchgeführt wurden sowie

– die Freigabeerklärung.

3.4.5.6 Ein Verfahren darf grundsätzlich nur freigegeben werden, wenn die Dokumentationsunterlagen vollständig vorliegen.

3.4.5.7 Auch nicht selbst entwickelte Verfahren sind vor ihrem Einsatz entsprechend zu testen und förmlich freizugeben.

3.4.5.8 Einzelheiten des Test- und Freigabeverfahrens sind schriftlich zu regeln.

3.4.5.9 Nach einer Freigabe ist sicherzustellen, daß bis zur Übernahme in die Produktion keine Änderungen mehr vorgenommen werden.

Voraussetzung für ein sachgerechtes Testen der Programme ist eine Testumgebung, die eine möglichst wirklichkeitsnahe Erprobung aller Funktionen des IT-Verfahrens erlaubt. Hierzu gehört insbesondere die Möglichkeit, geeignete Testfälle zu erzeugen. Die Testumgebung muß getrennt vom Verfahrensbetrieb sein. Für die Abnahmetests (Nr. 3.4.5.2 und 3.4.5.3) sollte sie auch von der Entwicklungsumgebung getrennt sein.

Sehr umfangreiche Verfahrensoftware ist bereits bei der Programmierung im Hinblick auf die Kriterien technische Richtigkeit, optimales Zeitverhalten, sparsamer Ressourceneinsatz und Übereinstimmung mit dem fachlichen und technischen Entwurf zu testen. Dieser Test sollte in der Verantwortung der IT-Bereiche liegen und, von ihr durchgeführt und kontrolliert werden. Tests von Verfahrensteilen im Rahmen der Qualitätssicherung (Nr. 6) sollten möglichst nicht von Personen vorgenommen werden, die mit der Entwicklung dieser Verfahrensteile betraut sind.

Nach Beendigung der Programmierung muß für die Abnahme ein Abschlußtest des gesamten Verfahrens (einschließlich der manuellen Bearbeitungsschritte) und der späteren organisatorischen Einbindung im Nutzungsumfeld vorgenommen werden. Ziel dieses Abschlußtests ist der Nachweis der fachlichen Vollständigkeit und Richtigkeit des Verfahrens sowie der Erfüllung der technischen Vorgaben. Er sollte von den am Projekt beteiligten Fachbereichen durchgeführt, bewertet und abgenommen werden (Nr. 3.4.5.2). Soweit Anteile betroffen sind, die in die Betriebsverantwortung des IT-Systembetriebes fallen, z.B. bei Datenbank-Software, wirkt der IT-Bereich als verantwortlicher Fachbereich. Beim Test ist auch zu prüfen, ob vorsätzlich oder fahrlässig nicht aufgabengerechte Funktionen oder Nebenwirkungen integriert wurden (Nr. 3.4.5.1).

Die Vorgabe von Testmethoden trägt dazu bei, durch eine geordnete Vorgehensweise Fehler zu finden oder einen bestimmten Grad der Fehlerfreiheit einzelner Verfahrensbestandteile, des gesamten Verfahrens und des Zusammenwirkens zwischen dem Verfahren und seiner fachlichen und technischen Umgebung nachzuweisen. Da der Nachweis der völligen Fehlerfreiheit nur mit großem Aufwand zu erbringen ist, sollte auch beim Testumfang auf die Wirtschaftlichkeit der Vorgehensweise geachtet werden. So wird z. B. bei kassenwirksamen Verfahren regelmäßig ein größerer Aufwand gerechtfertigt sein als bei Standardsoftware, die auf einem APC eingesetzt werden soll. Im Idealfall müßten sich Hinweise auf den erforderlichen Testumfang aus dem Sicherheitskonzept ableiten lassen (Nr. 7.2). Einige Methoden und Werkzeuge für das Testen sind in

Anhang 4 beispielhaft angeführt. Eingehende Hinweise<sup>5</sup> zum Testen von Softwaresystemen in der öffentlichen Verwaltung sind im Band 9 der Schriftenreihe der KBSt enthalten.

Die Freigabe von Verfahren oder Verfahrensteilen für den Verfahrensbetrieb ist streng zu regeln und zu kontrollieren. Sie muß zeitlich und inhaltlich detailliert nachvollziehbar sein. Jeder Test und jede Freigabe eines Verfahrens oder von Teilen eines Verfahrens, der zu einer erstmaligen oder erneuten Übernahme in den Verfahrensbetrieb führen soll, ist daher zu dokumentieren.

Voraussetzungen für die Verfahrensfreigabe sind das abgenommene Ergebnis des Abschlußtests, das Vorliegen der vollständigen Verfahrensdokumentation und die Freigabeentscheidung des Entscheidungsträgers. Bei der Verarbeitung personenbezogener Daten ist der Datenschutzbeauftragte zu beteiligen (Nr. 3.4.5.4).

Der Umfang der Arbeiten bei der Freigabe nicht selbst entwickelter Programme oder von Standardsoftware hängt vom Einzelfall ab (Nr. 3.4.5.7). Wenn APC-Standardsoftware nicht angepaßt werden muß, kann es genügen, nur den Einsatz zu dokumentieren, d. h. insbesondere Version, Einsatzdatum, das verwendete IT-System festzuhalten. Wenn dagegen die neue Version eines Standard-Datenbanksystems mit entsprechender Datenbankabfragesprache eingesetzt wird, auf dem bereits eigene Anwendungen aufbauen, kann der Aufwand für die Freigabe und die damit zusammenhängenden Arbeiten, wie Test, Umstellungsarbeiten und Dokumentation, erheblich sein, wenn ein zuverlässiges Weiterführen der Anwendungen gewährleistet werden muß (siehe auch Nr. 4.6).

Die Verfahrenssoftware darf nicht unkontrolliert aus der Entwicklungsumgebung in die Produktionsumgebung des Verfahrensbetriebs übernommen werden. Im Zuge der Funktionentrennung wird die Nutzung eines besonderen Abnahme-/Freigabebereichs empfohlen, in den die zuständige Stelle die zu übernehmende Verfahrenssoftware einstellt und aus dem der Bereich Verfahrensbetrieb diese entnimmt. Bei Großrechnern gibt es dazu eine Reihe von Möglichkeiten, Rechensysteme logisch oder physisch in einen Entwicklungs- und einen Produktionsteil zu trennen und dabei einen Freigabebereich vorzusehen. Bei APC und arbeitsplatznah eingesetzten Mehrplatzsystemen kann es zweckmäßig sein, für die Erprobung der Software sowie die Vorbereitung des flächendeckenden Einsatzes und die Freigabe einen gesonderten Rechner (Erprobungs-, Test- und Freigabesystem) bereitzustellen.

Die Übergabe der Verfahrenssoftware aus der Entwicklungsumgebung in den Abnahme-/Freigabebereich ist bei compilierbaren Programmiersprachen auf den Quelltext zu beschränken. Dieser ist erst im Abnahme-/Freigabebereich wieder zu ablauffähigen Programmen umzuwandeln und zu binden. Die Programme werden anschließend im Abnahme-/Freigabebereich getestet und nach Abnahme des Tests unverändert in die Produktionsumgebung übernommen (Nr. 3.4.5.9). Bei während der Abnahmetests notwendigen Änderungen, z.B. aufgrund von festgestellten Fehlern, ist sicherzustellen, daß

---

<sup>5</sup> Bundesminister des Innern [Hrsg.]: Verfahrenshandbuch "Testen von Softwaresystemen in der öffentlichen Verwaltung" Stand: November 1987 (Schriftenreihe der KBSt; Band 9)



die Änderungen an Verfahrenselementen (z.B. Daten, Programme) nur unter der Kontrolle der für die Abnahme Verantwortlichen erfolgt und die relevanten Teile der Abnahmetests wiederholt werden.

Bei bedeutsamen Verfahren sollte darüber hinaus jede Umwandlung, Bindung und Entnahme möglichst maschinell protokolliert und nur von hierzu berechtigtem Personal vorgenommen werden. Bei geänderten Programmen ist die neue Version, wenn möglich maschinell, mit der alten zu vergleichen. Die Unterschiede sind – ggf. stichprobenweise – auf Übereinstimmung mit dem Änderungsauftrag zu prüfen. Insbesondere ist zu überwachen, daß keine nicht aufgabengerechten Funktionen oder Nebenwirkungen vorsätzlich oder fahrlässig in die Programme integriert wurden (Nr. 3.4.5.1, Nr. 3.4.5.9).

In der Praxis stellen sich häufig bereits kurz nach Freigabe der Programme Fehler heraus. In diesen Fällen wird oft nach der Fehlerbeseitigung auf einen Test und eine erneute Freigabe der Programme verzichtet, da es sich in der Regel lediglich um wenig aufwendige Änderungen handelt. Mitunter wird auch direkt von den für die Verfahrensentwicklung zuständigen Bereichen auf Programme und Daten der Produktionsumgebung zugegriffen, und es werden entsprechende Fehlerbehebungsmaßnahmen durchgeführt. Die ordnungsgemäße und sichere Verarbeitung ist dann nicht mehr gewährleistet. Eine derartige Vorgehensweise ist allenfalls dann gerechtfertigt, wenn die ordnungsgemäße, insbesondere zeitgerechte Abwicklung der Arbeiten gefährdet würde. In jedem Fall sind Test, Freigabe und Dokumentation unverzüglich nachzuholen (siehe auch Nr. 3.5).

### *3.4.6 Einführung eines Verfahrens*

*3.4.6.1 Nach der Übernahme von Verfahrenssoftware in die Produktionsumgebung dürfen unbefugte Änderungen nicht mehr möglich sein. Die Bereitstellung zum Verfahrensbetrieb soll maschinell protokolliert werden und darf nur von ausdrücklich hierzu berechtigtem Personal vorgenommen werden. Eine geordnete Verwaltung von Programmversionen ist sicherzustellen.*

*3.4.6.2 Für die Einführung eines Verfahrens ist rechtzeitig insbesondere*

- die Einrichtung der Hard- und Softwareumgebung für den Verfahrensbetrieb,*
  - soweit erforderlich die Übernahme von Datenbeständen eines abzulösenden Verfahrens sowie*
  - die Schulung des Personals*
- sicherzustellen.*

*3.4.6.3 Für eine fortlaufende Beratung und Schulung auch nach der Verfahrenseinführung muß Vorsorge getroffen werden.*

Sobald die Verfahrenssoftware in die Produktionsumgebung übernommen worden ist, sind alle Änderungen der Verfahrenssoftware zu protokollieren. Insbesondere bei kas-

senwirksamen Verfahren ist festzuhalten, welche Verarbeitungsläufe mit welcher Programmversion durchgeführt wurden. Dazu muß jede Programmversion eindeutig identifizierbar sein, z. B. über eine Versionsnummer und ein Freigabedatum. Entsprechende Standardprodukte zur Programmverwaltung und Protokollierung sind am Markt verfügbar. Dies gilt sinngemäß auch für Anwendungen auf APC, wo häufig überwiegend Standardprogramme eingesetzt sind. Schon im Interesse einer sachgerechten Benutzerbetreuung muß klar sein, welche Programmversionen auf den einzelnen Geräten eingesetzt sind (Nr. 3.4.6.1).

Die für den Verfahrensbetrieb erforderlichen Voraussetzungen sollten so früh wie möglich festgelegt werden, um die Einrichtung der Hardware und Softwareumgebung, z. B. die Festlegung von Systemparametern oder die Anpassung von Prozeduren, zu ermöglichen. Die Anforderungen können z. B. Vorgaben enthalten

- zur maximalen Programmgröße,
- zur maximalen Programmlaufzeit,
- zu maximalen Antwortzeiten,
- zur Verwendung allgemein nutzbarer Module und Systemsoftwarefunktionen,
- zur Hauptspeicherbelegung,
- zur Hintergrundspeicherbelegung,
- zur Belegung von Magnetband- und Magnetbandkassettengeräten oder
- zur Druckausgabe.

Zudem sind die für die technische Handhabung des Verfahrens benötigten Informationen zusammenzustellen, z. B. in Produktionsunterlagen, die je nach Verfahren (bei dezentralen Verfahren sinngemäß) beispielsweise nachfolgende Punkte enthalten:

- Kurzeinführung in das Verfahren, seine fachliche Zielsetzung und die einzelnen Verfahrensteile,
- Überblick über Programme und Datenfluß,
- benötigte Hardware und Systemsoftware (z. B. Zentraleinheit, Band- oder Kassettenstationen, Betriebssystem, Datenbanksystem, TP-Monitore),
- Bedarf an Haupt- und Hintergrundspeicher für den Betrieb des Verfahrens,
- durchschnittliche Laufzeiten,
- erforderliche und erzeugte Dateien und Datenbanken mit Angabe der Organisationsform und des Datenträgers,
- benötigte Formulare für die Druckausgabe,
- Vorgaben zur Ablaufsteuerung (Job-Vorgaben und Job-Control),
- Voraussetzungen für einen ordnungsgemäßen Betrieb auch im Hinblick auf andere Verfahren mit Hinweisen für die Produktionsvor- und -nachbereitung, z. B.
  - o zeitlicher oder ereignisgebundener Auslöser für den Betrieb je Verfahrensteil (z. B. täglich, zum Jahresabschluß, nach Durchführung eines bestimmten anderen Verfahrens),
  - o Starten einzelner Verfahrensteile,
  - o Datensicherung,

- o Archivierung mit Aufbewahrungsfristen,
- o Reorganisation der Datenbestände,
- o Bearbeiten und Verteilen der Druckausgaben,
- o Datenerfassungshinweise bei zentraler Datenerfassung,
- o sonstige manuelle Vor- oder Nachbereitung durch das Bedienungspersonal,
- maschinelle und manuelle Kontrollen, soweit sie der Erkennung von Fehlern durch das Bedienungspersonal (Operating) dienen,
- Beschreibung der Maßnahmen bei Abbruch oder Fehlern in einzelnen Verfahrensteilen mit der Beschreibung der Wiederherstellung eines gültigen Datenbestandes und des Wiederanlaufes des Verfahrens sowie
- Kontaktstelle für Rückfragen.

Die Übernahme von Datenbeständen anderer IT-Verfahren kann großen Aufwand verursachen. Zweckmäßigerweise sollte spätestens beim Test des Verfahrens (siehe Nr. 3.4.5) die Übernahme von Altdaten erprobt werden.

Ggf. sollte der Einführung eines Verfahrens eine Pilotierungsphase unter besonders sorgfältiger Beobachtung des Systemverhaltens vorangehen. Bei IT-Systemen, die über Datenfernübertragung im Verbund arbeiten, ist eine Pilotierungsphase regelmäßig vorzusehen.

Die für die fachliche Handhabung des Verfahrens benötigten Informationen werden zweckmäßigerweise in einem Benutzerhandbuch zusammengestellt. Das Benutzerhandbuch soll unter Berücksichtigung seiner Zielgruppe – den Benutzern des Verfahrens im Fachbereich – in Aufbau, Inhalt und Sprache gestaltet werden. Das Benutzerhandbuch kann z. B. nachfolgende Punkte enthalten:

- Einführung in das Verfahren, seine fachliche Zielsetzung und die einzelnen Verfahrensteile,
- Überblick zu den Funktionen und dem Informationsfluß mit Erläuterungen,
- Anleitung zur Vorbereitung der Arbeit mit dem Verfahren mit Beispielen, z. B.
  - o Anmeldung,
  - o Programmstart,
- Anleitung zur Arbeit mit dem Verfahren anhand von Beispielen, z. B.
  - o Auswahl von Funktionen,
  - o Bildfolgen und Bildschirmmasken mit Ausfüllanweisung je Funktion,
  - o erzeugte Listen mit Aufbau und Bedeutung je Funktion,
  - o manuelle Vor- und Nachbereitung durch den Fachbereich je Funktion,
- maschinelle und manuelle Kontrollen und Abstimmungen im Verfahren,
- Hinweis- und Fehlermeldungen mit Angaben zu Ursache und eventuell erforderlichen Korrekturmaßnahmen,
- Kontaktstelle für Rückfragen,
- Datenbank- und Dateiübersicht sowie

- Verzeichnis der gültigen Schlüssel- und Datenfeldwerte.

Das Benutzerhandbuch und die Produktionsunterlagen sollten so rechtzeitig vor dem Wirksamwerden der Änderungen fertiggestellt sein, daß sich die Mitarbeiter mit dem Verfahren vertraut machen können und der Verfahrensbetrieb vorbereitet werden kann. Andernfalls ist unter Umständen mit einer langen Anlaufphase zu rechnen, bis das Verfahren sicher angewendet werden kann.

Die Informationen des Benutzerhandbuches sollten bei Dialogverfahren möglichst auch als Hilfefunktion maschinell zur Verfügung stehen. Empfehlungswert ist eine gezielte Auswahlmöglichkeit bestimmter Informationen und die Berücksichtigung des Dialogzustandes bei Aufruf der Hilfefunktion (kontextabhängige Hilfe), wie sie bei vielen APC-Standardprogrammen vorhanden ist.

Der erforderliche Schulungsaufwand wird häufig unterschätzt. Auch bei Verfahren, die auf vernetzten oder unernetzten APC betrieben werden, werden oft die Schwierigkeiten für den Benutzer nicht erkannt. APC stellen zwar viele Funktionen im Grunde leicht bedienbar bereit. Unbeschadet dessen werden die Fähigkeiten der Benutzer oft überschätzt, die IT-Systeme sachgerecht einzusetzen. Daher kommt auch in diesem Bereich einer angemessenen Information und Schulung der Benutzer große Bedeutung zu. Die Hinweise zum Benutzerhandbuch gelten entsprechend.

Hinweise für eine sachgerechte Planung der Schulung enthalten die Rahmenrichtlinien<sup>6</sup> für die Aus- und Fortbildung im Bereich Informationstechnik (IT) des Kooperationsausschusses ADV Bund/Länder/Kommunaler Bereich.

Eine fortlaufende Betreuung kann auch durch Ansprechpersonen in den fachlich zuständigen Bereichen gewährleistet werden (Nr. 3.4.6.3).

---

<sup>6</sup> Bundesminister des Innern [Hrsg.]: Rahmenrichtlinien für die Aus- und Fortbildung im Bereich Informationstechnik (IT) in der öffentlichen Verwaltung des Kooperationsausschusses ADV Bund / Länder / Kommunaler Bereich (KoopA ADV) -IT-Aus- und Fortbildungsrichtlinien- (Schriftenreihe der KBSI; Band 23)

### 3.5 Verfahrenspflege und -änderungen

- 3.5.1 *Bei der Verfahrenspflege sollen der ordnungsgemäße Einsatz des Verfahrens sowie seine Anpassung an veränderte Anforderungen gewährleistet werden. Soweit wesentliche Änderungen erforderlich werden, ist wie bei einem neuen IT-Vorhaben vorzugehen. Für andere Änderungen sind entsprechende Regelungen zu treffen. Für jede Verfahrensänderung sind grundsätzlich ein erneuter Ab- schlußtest und in jedem Fall eine Freigabe durchzuführen.*
- 3.5.2 *Für abweichende Vorgehensweisen zur schnellen Behebung von Fehlern sind besondere schriftliche Regelungen zu treffen und die Beteiligung der zuständi- gen Fachbereiche sicherzustellen.*
- 3.5.3 *Änderungen der Hardware und der nicht verfahrensspezifischen Software, sind im Rahmen einer geordneten Vorgehensweise vorzunehmen. Dabei ist sicherzu- stellen, daß zusammengehörige Änderungen vollständig durchgeführt und Stö- rungen sowie Unterbrechungen des Verfahrensbetriebes durch Folgeänderun- gen verhindert werden. Die bei der Durchführung eines IT-Vorhabens zu Test und Freigabe beschriebenen Grundsätze sollen sinngemäß angewendet werden. Alle Maßnahmen im Rahmen von Änderungen sind zu dokumentieren.*

Wirtschaftliche Pflege und Änderung der Verfahrenssoftware kann durch

- eine geordnete Vorgehensweise,
- den Einsatz von geeigneten Methoden und Werkzeugen und
- eine vollständige, nachvollziehbare Dokumentation

bereits bei der Verfahrensentwicklung erleichtert werden. Mit der Modularisierung der Verfahrenssoftware kann erreicht werden, daß nur einzelne Module von Änderungen im Rahmen einer Pflegemaßnahme betroffen sind und bei Erweiterungen viele Module weiterverwendet werden können.

Die im Verfahren verwendeten Datenstrukturen sollen durch eine wiederholungsfreie Darstellung änderungs- und erweiterungsfreundlich gehalten werden (siehe auch Nr. 4.6).

Die Programme sollten durch eine entsprechende Gestaltung der Datenzugriffe, z. B. über festgelegte Schnittstellen und Zugriffsmodule, weitgehend unabhängig von Ände- rungen der Datenstrukturen gehalten werden (siehe auch Nr. 3.4.4).

Grundsätzlich ist auch bei Pflege und Änderung von IT-Verfahren größeren Umfangs die Vorgehensweise eines Projektes vorzusehen. Insbesondere müssen die im Laufe der Ver- fahrensentwicklung erarbeiteten Ergebnisse für die Pflege herangezogen und aktualisiert werden. Die Gewichtung der einzelnen Projektschritte und Tätigkeiten kann an den Um- fang der jeweiligen Änderung angepaßt werden, ggf. können einzelne Projektschritte und Tätigkeiten entfallen.

Die Verfahrenspflege soll einem Versionenkonzept auf Modulebene folgen, bei dem die einzelnen verbesserten Versionen planvoll, geordnet, zeitlich abgestimmt und ange-

kündigt freigegeben werden. Dabei ist sicherzustellen, daß jedes Modul eine separate Versionsnummer erhält, die – wenn möglich – maschinell gepflegt wird. Bei jeder Änderung eines Moduls ist auch eine neue Versionsnummer zu vergeben. Für jede Verfahrensänderung soll ein erneuter Verfahrenstest und eine komplette Freigabe durchgeführt werden (siehe Nr. 3.4.5).

Die Vollständigkeit sowie die fachliche und technische Richtigkeit von Änderungen haben die jeweils zuständigen Bereiche entsprechend dem Vorgehen bei Test und Freigabe (Nr. 3.4.5) sicherzustellen. Die Übernahme von Änderungen muß der festgelegten Vorgehensweise folgen. Besondere Probleme können entstehen, wenn durch den IT-Bereich ohne Beteiligung der fachlich Zuständigen kurzfristig Fehler beseitigt werden müssen. Dann sollte durch eine nachgängige Prüfung die Korrektheit der durchgeführten Maßnahmen nachvollzogen werden. Für derartige Fälle sollten entsprechende Regelungen getroffen werden (Nr. 3.5.2).

Schwierigkeiten können auch wesentliche Änderungen des für die Produktion eingesetzten IT-Basisystems (Hardware und Betriebssystem) bereiten, da diese Auswirkungen auf sämtliche IT-Verfahren haben können (Nr. 3.5.3). Häufig ist erheblicher Umstellungsaufwand erforderlich. Daher sollte die Produktionsumgebung möglichst wenig geändert werden.

Änderungen der IT-Produktionsumgebung können sich z. B. auf die

- Anpassung des Funktionsumfangs der Verfahren,
- Korrektur fehlerhafter Funktionen, z. B. der Hardware, Systemsoftware oder Verfahrenssoftware, und
- Optimierung der Produktionsumgebung

beziehen. Um die Funktionsfähigkeit zu sichern und die Möglichkeit zu erhalten, IT-Systeme im Wettbewerb zu beschaffen, kann langfristig auch ein Systemwechsel, z. B. zu einem herstellerunabhängigen Betriebssystem wie UNIX, vorteilhaft sein.

Die im Abschnitt "Test und Freigabe" (Nr. 3.4.5) bezüglich der Verfahrenssoftware beschriebenen Grundsätze sollten auch auf die Änderung der übrigen Ressourcen – z. B. der Hardware und Systemsoftware – übertragen werden. Dazu sind die eingesetzte Hardware und Software und deren Änderungen nachvollziehbar aufzuzeichnen (Konfigurationsmanagement).

Jede Änderung muß im Rahmen einer geordneten Vorgehensweise geschehen, um die Risiken einer

- fehlerhaften Planung oder Ausführung von Änderungen,
- unvollständigen Übernahme zusammengehöriger Änderungen,
- Störung oder Unterbrechung der Produktion und
- Instabilität der Produktionsumgebung durch notwendig werdende häufige Folgeänderungen

zu minimieren. Deshalb sollten die geplanten Änderungen an der Produktionsumgebung frühzeitig mit Termin, Inhalt und Umfang bekanntgegeben und in einer Änderungsplanung zusammengefaßt werden. Ziele der Änderungsplanung sollen sein:

- die Vermeidung von Änderungshäufungen zu einem Termin (ggf. mit dem erhöhten Risiko der Instabilität des IT-Basissystems),
- die Verringerung der Änderungshäufigkeit durch zweckmäßige Kombination verschiedener Änderungen,
- die Berücksichtigung von Produktionsspitzenzeiten sowie
- die wirksame Terminverfolgung erforderlicher Änderungen.

Die regulären Änderungstermine sollten möglichst auf wenige bestimmte Tage innerhalb einer Woche oder eines Monats beschränkt werden. Die Änderungsplanung für die Produktion soll mit den Planungen für Verfahreneinführungen und -änderungen abgestimmt sein.

Die für die Durchführung und den Test der Änderung erforderlichen Maßnahmen sind zwischen den beteiligten Bereichen unter besonderer Berücksichtigung der Abhängigkeiten der IT-Verfahren untereinander abzustimmen. Die sich daraus ergebenden Aufgaben sind mit Terminsetzung verbindlich zwischen den beteiligten Bereichen zu verteilen. Abhängigkeiten können dabei durch eine Staffelung der Termine berücksichtigt werden. Die Termine sind von einer verantwortlichen Stelle – in der Regel durch den für den zentralen Verfahrensbetrieb zuständige Bereich – zu verfolgen und abzustimmen. Die Änderungsplanung sollte einschließlich der Termine laufend fortgeschrieben werden. Eine maschinelle Unterstützung bei Verfahrensänderungen – insbesondere bei der Terminverfolgung, beim Konfigurationsmanagement und bei der Versionsverwaltung – ist empfehlenswert.

Mängel bei der Verfahrenspflege und -änderung führen häufig dazu, daß die Qualität der Programme schlechter wird. Hierzu tragen z. B. die im Lauf der Zeit entstehenden Personalveränderungen bei. Die Verfahren sind dann beispielsweise nicht mehr optimal auf das IT-System abgestimmt, oder die Dokumentation stimmt nicht mehr mit den tatsächlichen Gegebenheiten überein. Die Verfahren gelten als "überpflegt". Änderungen sind dann häufig nur noch mit großem Aufwand durchzuführen und führen häufig zu Folgefehlern.

## 4 Betrieb von IT-Verfahren

### 4.1 Grundsätzliches

4.1.1 *Der Verfahrensbetrieb umfaßt die administrative und technische Abwicklung freigegebener Verfahren.*

4.1.2 *Die vollständige und richtige*

- Ermittlung, Erfassung und Eingabe der Daten,*
- Speicherung und Verarbeitung der Daten sowie*
- Ausgabe von Daten*

*müssen nachvollziehbar und kontrollierbar sein.*

4.1.3 *Die Vollständigkeit und Richtigkeit ist durch organisatorische Maßnahmen und programmierte Kontrollen zu gewährleisten. Es ist stets sicherzustellen, daß in den Arbeitsablauf nicht unbefugt eingegriffen und Daten nicht unkontrolliert verändert und vernichtet werden können. Der Verfahrensbetrieb ist ständig insbesondere im Hinblick auf die Aufrechterhaltung eines störungsfreien Einsatzes der Verfahren sowie die durchgängige Beachtung von festgelegten Vorgehensweisen und Arbeitstechniken zu überwachen.*

Der Verfahrensbetrieb ist so zu gestalten, daß die technischen und administrativen Voraussetzungen für die zeitnahe Erledigung der Aufgaben unter Berücksichtigung der übergreifenden Zielsetzung der IT (siehe Nr. 1.3) gegeben sind (Nr. 4.1.1). Dazu ist der Verfahrensbetrieb im Rahmen der Gesamtplanung vorausschauend (über mehrere Jahre) zu planen. Die Planung ist jährlich fortzuschreiben. Der Planungshorizont soll sich auf den Zeitraum der mittelfristigen Finanzplanung erstrecken (siehe auch Nr. 2.1). Dabei sollten möglichst konkrete Vorgaben für die Qualität des Verfahrensbetriebes getroffen werden, die ihre Grundlagen in den Benutzeranforderungen finden. Dazu sind geeignete Kriterien festzulegen, die sich an meßbaren Leistungsgrößen orientieren. Beispiele für derartige Kriterien sind:

- die tägliche Zeit der Verfügbarkeit der Verfahren,*
- die maximalen Antwortzeiten,*
- die maximalen Ausfallzeiten (je Tag, Woche oder Monat),*
- die Zeit zwischen Auftragseingang und Ergebnisauslieferung,*
- die täglichen Auslieferungszeiten der Ergebnisse,*
- die Qualität der Ergebnisse beim Druck oder*
- die maximal zulässige Fehlerrate beim automatischen Erfassen von Belegen.*

Damit läßt sich die Art des IT-Systems, dessen Kapazität, und der Umfang der Peripherie und somit der Mittelbedarf festlegen.



Die Planung des Verfahrensbetriebs umfaßt auch die Verfügbarkeit von Verbrauchsmaterial und des sonstigen Inventars. Beim Verbrauchsmaterial, z. B. Magnetbändern, Disketten, Druckerpapier, sollte überschlägig die je Zeiteinheit benötigte Menge ermittelt werden, um entsprechende Haushaltsmittel vorsehen zu können.

Die Planung soll auch den Bedarf für die Verfahrensentwicklung berücksichtigen. Werden Ressourcen sowohl in der Verfahrensentwicklung als auch im Verfahrensbetrieb eingesetzt, sollte der Verfahrensbetrieb Priorität bei der Zuteilung von Kapazitäten haben, da es in der Regel leichter gelingt, Kapazitätsengpässe bei der Verfahrensentwicklung, z. B. durch organisatorische Maßnahmen, auszugleichen.

Voraussetzung für die Nachvollziehbarkeit und Kontrollierbarkeit des Verfahrensbetriebes (Nr. 4.1.2) ist eine aussagekräftige Dokumentation. Insbesondere ist die organisatorische und technische Umgebung, in welcher der Verfahrensbetrieb durchgeführt wird, zu dokumentieren. Zur Dokumentation der Produktionsumgebung soll eine Übersicht der einzelnen Bestandteile der Produktionsumgebung und die dazu von Hardware- oder Systemsoftwareherstellern gelieferte Dokumentation gehören. Die Ausprägung der jeweiligen Konfigurationen, z. B. die gewählten Systemparameter, und alle individuellen Erweiterungen sind detailliert zu beschreiben (siehe auch Nr. 3.5.3). Die Dokumentation der Produktionsumgebung sollte auch Arbeitsanweisungen für die geordnete Aufnahme, Aufrechterhaltung und Beendigung des Betriebes enthalten und die Einbindung von Verfahren in die Produktionsumgebung beschreiben.

Die koordinierte Abwicklung des Betriebes mehrerer über Datenaustausch oder gemeinsame Ressourcennutzung gekoppelter Verfahren kann durch eine verfahrenübergreifende Dokumentation unterstützt werden. Diese gibt dem für den Verfahrensbetrieb zuständigen Personal einen Überblick über die produktiv einzusetzenden Verfahren und ihre fachliche und technische Verknüpfung. Die Verfahrenübersicht kann aus der Dokumentation der Verfahrensentwicklung abgeleitet werden und beschreibt

- die fachliche Zielsetzung,
- den Auslöser oder Turnus der Verarbeitung,
- die Berührungspunkte zu anderen Verfahren und

verweist auf die zugehörigen, detaillierten Produktionsunterlagen.

Demgegenüber liefert die verfahrensspezifische Dokumentation je Verfahren die zur ordnungsgemäßen, sicheren und wirtschaftlichen Abwicklung der Produktion erforderlichen Informationen. Die verfahrensspezifische Dokumentation soll aus

- den im Rahmen der Verfahrensentwicklung erstellten Produktionsunterlagen ergänzt um
  - o die Darstellung der produktiven Abläufe (Jobs) und
  - o die tatsächliche Speicherzuordnung der Dateien und Datenbanken
- und der Dokumentation der Änderungen

bestehen.

Die verfahrenübergreifende und -spezifische Dokumentation bildet die Voraussetzung für die Nachvollziehbarkeit und Kontrollierbarkeit (Nr. 4.1.2, Nr. 4.1.3).

Zur Überwachung der Produktion ist die vollständige und ordnungsgemäße Abwicklung der Verarbeitung – möglichst maschinell – zu protokollieren. Die statistische Auswertung der Verarbeitungsdaten, z. B. nach Häufigkeiten und Art aufgetretener Fehler, kann Hinweise auf Schwachstellen und Störungsquellen des IT-Betriebes sowie der Verfahren liefern. Die Schwachstellen sollen untersucht und ggf. beseitigt werden. Eine maschinelle Erstellung und Verwaltung der Verarbeitungsdaten ist empfehlenswert.

Neben der vollständigen und richtigen Verarbeitung soll der Verfahrensbetrieb als weiteres Ziel die Ergebnisse zeitgerecht bereitstellen und eine günstige Auslastung der Ressourcen gewährleisten. Auch dazu kann eine Auswertung der Verarbeitungsdaten beitragen.

Alle Änderungen des Betriebs, z. B. Änderungen der Plattenbelegungen, Geräteaus-tausch, sollten frühzeitig und im voraus in einem Änderungsplan für die Produktion mit Termin, Inhalt und Umfang festgelegt werden (siehe auch Nr. 3.5). Dieser Plan soll auch weiterführende Hinweise, etwa das Protokoll der Aufgabenverteilung zur Durchführung der Änderung, enthalten. Der Änderungsplan soll zusammen mit der weiterführenden Dokumentation eine Arbeitsanweisung für das betroffene Personal darstellen. Die Änderungen sind in einem Änderungsnachweis beispielsweise in Form einer Stichpunktliste (Checkliste) zu dokumentieren. Dadurch werden Änderungen der Produktionsumgebung nachvollziehbar belegt und die Datenverarbeitung möglichst wenig beeinträchtigt (siehe auch Nr. 3.5).

Die Produktionsumgebung sollte sowohl bezüglich der Daten als auch bezüglich der Ressourcennutzung von der Entwicklungs- und Testumgebung getrennt sein, um entsprechend den IT-Mindestanforderungen unbefugte Eingriffe vermeiden und den störungsfreien Betrieb leichter gewährleisten zu können. Die gemeinsame Nutzung von Ressourcen ist nur dann möglich, wenn Ordnungsmäßigkeit und Sicherheit gewährleistet sind.

Die IT-Mindestanforderungen enthalten zur Sicherheit weitere Ausführungen (siehe Nr. 7), bei deren Beachtung die unter Nr. 4.1.3 enthaltenen Forderungen, insbesondere die nach der Verhinderung von unbefugten Eingriffen in den Arbeitsablauf und von unkontrollierten Veränderungen von Daten, erfüllt werden können.

## 4.2 Funktionentrennung und Verantwortlichkeiten

- 4.2.1 *Unabhängig von unterschiedlichen Verarbeitungsformen beim Einsatz der IT müssen*
- *Fachverantwortung und*
  - *Betriebsverantwortung*
- eindeutig festgelegt werden.*
- 4.2.2 *Insbesondere sollen die Verantwortlichkeiten für folgende Funktionen unterschieden werden:*
- *Datenermittlung*
  - *Datenerfassung und -eingabe*
  - *Arbeitsplanung und -vorbereitung*
  - *Datenverarbeitung*
  - *Nachbearbeitung von Datenausgaben*
  - *Datenträgerverwaltung*
  - *Überwachung des Verfahrensbetriebes.*
- 4.2.3 *Die Abgrenzung und Zuweisung der Funktionen und Verantwortungsbereiche ist im einzelnen schriftlich festzulegen. Kontrollfunktionen sollen von Ausführungsfunktionen getrennt sein.*
- 4.2.4 *Soweit eine Trennung von Funktionen und damit von Verantwortungsbereichen nicht möglich oder nicht zweckmäßig ist, sind geeignete Sicherheits- und Kontrollmaßnahmen vorzuschreiben. Auch in diesen Fällen muß die Zuordnung der Funktionen im einzelnen geregelt sein.*

Die Trennung der Funktionen (Nr. 4.2.1, Nr. 4.2.2) erleichtert das Nachvollziehen und die Kontrolle (siehe Nr. 4.1) des Betriebs von IT-Verfahren.

Im Rahmen der aufgeführten Funktionen bezieht sich die Fachverantwortung meist auf

- die Vorgabe der fachlichen Anforderungen an Verfahren (Nr. 3.3),
- die Bestätigung im Rahmen der Freigabe, daß die fachlichen Anforderungen erfüllt sind (Nr. 3.4.5),
- die Vorgaben für die terminliche Abwicklung der Verfahren (Nr. 3.4.6),
- die termingerechte Lieferung der richtigen und vollständigen Eingabeinformationen (Nr. 4.3),
- bei Dialogverfahren und dezentralen Verfahren die dezentrale Datenerfassung und -eingabe und

- das Überwachen des Verfahrensbetriebes mit Terminverfolgung sowie Abnahme, Endkontrolle und fachliche Nachbearbeitung der Ausgabeinformationen (Nr. 4.1 und Nr. 4.3).

Die Betriebsverantwortung im Rahmen der in Nr. 4.2.2 aufgeführten Funktionen umfaßt insbesondere

- das Sicherstellen des vorschriftsgemäßen Einsatzes ausschließlichen von freigegebenen Verfahren (Nr. 4.1.3),
- das Sicherstellen der anforderungsgerechten Verarbeitungsbereitschaft durch die entsprechende Gestaltung des IT-Basissystems aus Hardware und Systemsoftware (Nr. 4.1.3),
- das Gewährleisten der Sicherheitserfordernisse der Verfahren (Nr. 4.1.3 und Nr. 7),
- das termingerechte Abwickeln der Verfahren (Nr. 4.3.3.4),
- die vollständige Übernahme, Umsetzung und Verarbeitung der Eingabeinformationen – ggf. einschließlich der Erfassung – (Nr. 4.3.1.1 und Nr. 4.3.3.2),
- das Durchführen der vorgeschriebenen Kontrollen und Abstimmungen (Nr. 4.1.3, Nr. 4.3.1 und Nr. 4.3.3.2) sowie
- das richtige und vollständige technische Weiterbearbeiten und Weiterleiten der Ausgabeinformationen als Verfahrensergebnisse (Nr. 4.3.3.2).

Fach- und Betriebsverantwortung können teilweise zusammengefaßt werden (siehe Nr. 4.4), wenn die Verfahren dezentral, z. B. mit APC, betrieben werden.

Zentraler und dezentraler Verfahrensbetrieb bieten unterschiedliche Möglichkeiten, eine Funktionentrennung zu verwirklichen. Allgemein läßt sich eine Funktionentrennung bei zentralem Betrieb leichter herstellen. Daher sollte ein Verfahren zentral betrieben werden, wenn

- große Datenbestände von mehreren Fachbereichen gepflegt werden,
- erhöhte Anforderungen an die Sicherheit des Verfahrens gestellt werden oder
- die Nutzung von gemeinsam verwalteten Ressourcen durch mehrere Verfahren die Wirtschaftlichkeit fördert.

Ein Verfahren soll dezentral betrieben werden, wenn

- das Verfahren eine begrenzte Aufgabenstellung löst,
- ein entsprechendes zentrales Verfahren nicht wirtschaftlicher entwickelt oder betrieben werden kann,
- Sicherheit und Ordnungsmäßigkeit nicht beeinträchtigt werden,
- die dezentrale Lösung nicht im Widerspruch mit dem Verfahrenssoftware-, Hardware- oder Systemsoftwarekonzept steht und
- ggf. zentrale Datenbestände gelesen, zusammengefaßt und ausgewertet, nicht aber verändert werden.

Unabhängig von der Betriebsart sind die Häufung von Kontroll- und Durchführungsaufgaben bei einer Person und eine Personenabhängigkeit zu vermeiden (Nr. 4.2.3).

Daher sollte neben einem hauptverantwortlichen Mitarbeiter zumindest ein weiterer Mitarbeiter in der Lage sein, die Funktion in angemessener Zeit zu übernehmen. Bei einer Vertretungsregelung ist die Funktionentrennung ebenfalls zu berücksichtigen. Hinweise zum Betrieb von IT-Verfahren bei eingeschränkter Funktionentrennung enthält Nr. 4.4.

Bei kleineren Stellen und ungünstigen organisatorischen Gegebenheiten, z. B. Verteilung des Personals über mehrere Orte oder weit auseinanderliegende Räumlichkeiten sowie bei dezentralen Verfahren, die teilweise oder vollständig in der Verantwortung der Fachbereiche betrieben werden, kann es unumgänglich sein, daß mehrere der in Nr. 4.2.2 aufgeführten Funktionen von denselben Personen wahrgenommen werden. In diesen Fällen kann die Ordnungsmäßigkeit der Verarbeitung durch (maschinelle) Protokollierung und Prüfung wichtiger Verarbeitungsschritte gewährleistet werden. Daher ist aber, z. B. bei Dialogverfahren, bei denen Dateneingabe und -verarbeitung im Fachbereich angesiedelt sind, regelmäßig mit zusätzlichem Entwicklungsaufwand für Protokollierungsfunktionen und Plausibilitätsprüfungen zu rechnen.

## 4.3 *Verfahrensbetrieb bei Funktionentrennung*

### 4.3.1 *Datenerfassung und -eingabe*

4.3.1.1 *Die vollständige und richtige Erfassung und Eingabe sind zu kontrollieren. Hierfür sollen möglichst programmierte Kontrollen eingerichtet werden. Die Durchführung der Kontrollen und ihre Ergebnisse sind zu bescheinigen bzw. maschinell zu protokollieren.*

4.3.1.2 *Einzelheiten einschließlich des Verfahrens zur Fehlerbereinigung sind in Regelungen festzulegen.*

Bei Verfahren, die Massendaten verarbeiten, spielt die Datenerfassung eine große Rolle. Für die Richtigkeit und Vollständigkeit der angelieferten Daten soll die datenliefernde Stelle – in der Regel der fachlich zuständige Bereich – verantwortlich sein (siehe auch Nr. 4.2). Die Kontrolle der vollständigen und richtigen Erfassung und Eingabe obliegt überwiegend den für die IT zuständigen Bereichen.

Bei Dialogverarbeitung kommt den programmierten Eingabekontrollen besondere Bedeutung zu, da die Daten in aller Regel unmittelbar nach der Dateneingabe verarbeitet werden und häufig keine oder nur stichprobenweise weitere Prüfungen vorgesehen sind (siehe Nr. 4.4). Bei kassenwirksamen Verfahren ist zudem eine Protokollierung der Eingabe, einschließlich der Angaben zum Bearbeiter und zum Zeitpunkt der Eingabe, unerlässlich.

Fehler, die, z. B. bei Plausibilitätsprüfungen, von den für die IT zuständigen Bereichen erkannt werden, werden häufig auch von diesen bereinigt. Damit wird aber die Verantwortung für die fachliche Richtigkeit der Daten verwischt. In jedem Fall sollten daher die fachlich zuständigen Bereiche – ggf. nachgängig – die Korrektheit der Fehlerbehebung bestätigen.

### 4.3.2 *Arbeitsplanung und -vorbereitung*

*Die technische Handhabung des Verfahrens ist unter Berücksichtigung der vorhandenen Kapazitäten zu planen und vorzubereiten. Dazu hat der Bereich Arbeitsplanung und -vorbereitung Unterlagen und Anweisungen zu liefern für*

- die Steuerung der Datenverarbeitung,*
- die Überwachung des Verfahrensbetriebes sowie*
- die Arbeitsnachbereitung.*

Aspekte der Arbeitsplanung sind aus fachlicher Sicht die termingerechte Bereitstellung der Verfahren sowie ihrer Ergebnisse und aus technischer Sicht die optimale Auslastung

der Ressourcen. Abhängigkeiten und – insbesondere bei knappen Ressourcen – Prioritäten müssen bei der Planung berücksichtigt werden.

Die tägliche Belegung der Produktionsumgebung mit abzuwickelnden Verfahren ist zweckmäßigerweise im voraus in einem Produktionsplan niederzulegen. Zusammen mit den verfahrensspezifischen Produktionsunterlagen wird er zur konkreten Arbeitsanweisung für das Personal im Bereich Verfahrensbetrieb.

Die vorbereitenden Maßnahmen für die Datenverarbeitung müssen in Produktionsunterlagen beschrieben sein (siehe auch Nr. 3.4.4.4 und Nr. 3.4.6.2). Diese können sich für den Ersteinsatz und die Folgeeinsätze des Verfahrens unterscheiden. Vorbereitende Maßnahmen können z. B. sein:

- beim Ersteinsatz eines IT-Verfahrens:
  - o das Erstellen der produktiven Job-Abläufe,
  - o die Anlage der Dateien und Datenbanken in der Produktionsumgebung,
  - o die Installation von Komponenten des Basissystems, z. B. Datenbank- und Dialogsystem,
- bei Folgeeinsätzen des IT-Verfahrens:
  - o das Starten von Komponenten des Basissystems,
  - o das Anfordern von Datenträgern aus dem Archiv, z. B. Magnetbänder, Kassetten,
  - o das Anfordern von Formularen,
  - o das Prüfen der vollständigen Erfüllung aller Voraussetzungen für die Verfahrensabwicklung und
  - o das Durchführen von Folgearbeiten, z. B. Aufbereiten und Versand erzeugter Druckausgaben, Archivieren oder Versand erzeugter Datenträger, Freigabe nicht mehr benötigter Zwischenspeicherbereiche im Haupt- und Hintergrundspeicher sowie das Abschalten oder Anhalten nicht mehr benötigter Komponenten des IT-Basissystems, z. B. der Datenbank- und Dialogsysteme.

Soll auf geänderte Anforderungen rasch und unter Beibehaltung der Betriebssicherheit reagiert werden können, muß es möglich sein, kurzfristig durchzuführende Einmal-, Sonder- oder Wiederholungsläufe von Verfahren oder Verfahrensteilen im Rahmen der Arbeitsplanung in die Produktion einzubringen.

Da die Arbeitsplanung große Auswirkungen auf die Ordnungsmäßigkeit und Sicherheit der Verarbeitung hat, sollten Anträge zur Aufnahme von Verfahren oder Verfahrensteilen in die Arbeitsplanung schriftlich gestellt und nur bei Freigabe des Verfahrens bzw. des Verfahrensteils berücksichtigt werden (Nr. 3.4.5).

Ein maschinelles Unterstützen der Arbeitsplanung und -vorbereitung, z. B. bei der Erstellung, dem Test und der Dokumentation von Job-Abläufen, ist insbesondere bei komplexen Verfahren aus wirtschaftlicher Sicht und zur Verbesserung der Ablaufsicherheit geboten.

Im Rahmen der Arbeitsplanung ist auch die ausreichende Verfügbarkeit des Verbrauchsmaterials, z. B. Formulare, Listenpapier, Magnetbänder, Disketten, für die Datenverarbeitung sicherzustellen.

### 4.3.3 Datenverarbeitung

*4.3.3.1 Die Steuerung der Datenverarbeitung soll möglichst automatisiert erfolgen. Manuelle Eingriffe sollen sich auf Ausnahmesituationen beschränken. Alle manuellen Eingriffe in die Verfahrensabwicklung, insbesondere bei Ausnahmesituationen, sind zu protokollieren und, soweit vorhersehbar, detailliert durch Arbeitsanweisungen zu regeln.*

*4.3.3.2 Bei der Datenverarbeitung sind insbesondere zu gewährleisten:*

- die vollständige und richtige Übernahme der Daten zur Verarbeitung,*
- die vollständige und richtige Verarbeitung, Speicherung und Ausgabe der Daten im Rahmen der freigegebenen und gültigen Verfahren,*
- die vollständige Durchführung der vorzunehmenden Kontrollen,*
- die Sicherung der Daten und der Programme,*
- die vollständige und richtige Weiterleitung der Arbeitsergebnisse.*

*4.3.3.3 Die vollständige und ordnungsgemäße Abwicklung der Datenverarbeitung ist zu kontrollieren und zu bescheinigen. Rekonstruktionen von Datenträgern durch das Personal der Datenverarbeitungsstelle sind zu protokollieren.*

*4.3.3.4 Die Übernahme und die Abgabe von Datenträgern und von Arbeitsergebnissen sind durch Arbeitsablaufbelege zu sichern und zu bescheinigen.*

*4.3.3.5 Beim Auftreten von Ausnahmesituationen ist deren korrekte Behandlung zu überwachen. Ausnahmesituationen, die sich nicht im Rahmen einer festgelegten Arbeitsanweisung in kurzer Zeit beheben lassen, sind im Rahmen einer speziellen Problembehandlung zu bearbeiten. Die betroffenen Bereiche sind unverzüglich zu informieren. Alle getroffenen Maßnahmen sind zu dokumentieren.*

Wenn die Erfordernisse des Verfahrensbetriebes bereits beim Entwurf eines IT-Verfahrens berücksichtigt worden sind und der Verfahrensbetrieb sachgerecht vorbereitet ist, kann die Datenverarbeitung weitgehend automatisiert ablaufen. Damit können auch die in Nr. 4.3.3 geforderten Protokolle maschinell erzeugt werden (Nr. 4.3.3.1 bis Nr. 4.3.3.3).

Die Maßnahmen zur Überwachung der Datenverarbeitung, z. B. die manuellen Kontrollen und Abstimmungen zur Überwachung der Richtigkeit der Ergebnisse, sollten zweckmäßigerweise in Produktionsunterlagen beschrieben sein.

Um Schwachstellen der IT-Verfahren zu erkennen, hat es sich als nützlich erwiesen, aus den Verarbeitungsergebnissen regelmäßig Zufallsstichproben zur detaillierten fachlichen



Nachkontrolle zu ziehen. Art, Umfang und Häufigkeit der Stichproben sind entsprechend den möglichen Folgen von Fehlfunktionen festzulegen.

Auch bereits freigegebene Programme sollten bei bedeutsamen IT-Verfahren dahingehend kontrolliert werden, ob sie z. B. durch Softwareviren manipuliert wurden. Als Hilfsmittel zur Erkennung solcher Manipulationen können Prüfsummen dienen, die vor jedem Aufruf der Programme neu ermittelt und verglichen werden (siehe auch Nr. 7).

Bei Änderungen an der Produktionsumgebung sollte das Überwachen der Datenverarbeitung für einen begrenzten Zeitraum intensiviert werden. Ziel dieser Änderungsüberwachung ist es festzustellen, ob die Änderungen richtig und vollständig im Sinne der fachlichen Aufgabenerfüllung sowie technisch optimal im Sinne der Ressourcenausnutzung durchgeführt wurden (siehe auch Nr. 3.5).

Die vollständige und ordnungsgemäße Abwicklung der Produktion wird üblicherweise über einen Produktionsnachweis dokumentiert. Dieser soll für jeden in den Produktionsunterlagen vorgeschriebenen Arbeitsschritt – insbesondere für die Arbeitsschritte zur Kontrolle und Abstimmung – oder Sondersituationen, wie die Rekonstruktion von Datenträgern, Erledigungsvermerke enthalten.

Ein Produktionsnachweis kann auch Daten für eine Leistungsverrechnung und die Optimierung der Ressourcen enthalten. Dazu können z. B. zählen:

- Programmlaufzeiten,
- Haupt- und Hintergrundspeicherbelegung,
- Magnetband- oder -kassettenanforderungen,
- erzeugte Druckseiten.

Um Schwachstellen frühzeitig zu erkennen und Planungsdaten zu gewinnen ist eine, möglichst maschinelle Auswertung des Produktionsnachweises, z. B. nach Fehlerhäufigkeiten, durchschnittlichen Programmlaufzeiten oder durchschnittlicher Ressourcenauslastung, empfehlenswert.

Die Bereinigung von Ausnahmesituationen sollte stets – ggf. nachgängig – unter Beteiligung aller zuständigen Bereiche untersucht und dokumentiert werden. Bei einer Häufung von Fehlern bei der Datenverarbeitung, z. B. in der Einführungsphase eines Verfahrens, neigen die fachlich zuständigen Bereiche dazu, die Fehlerbereinigung den für die IT Zuständigen zu überlassen. Eine wirksame Kontrolle der Datenverarbeitung ist in diesen Fällen nicht mehr gegeben, die Funktionentrennung ist faktisch aufgehoben.

## 4.4 Verfahrensbetrieb bei eingeschränkter Funktionentrennung

4.4.1 Wenn keine oder nur eine teilweise Trennung von Funktionen möglich ist, z. B. beim Einsatz von Arbeitsplatzrechnern (APC), arbeitsplatznahen Mehrplatzsystemen und dialogorientierter Verarbeitung, sind besondere organisatorische und technische Sicherungs- und Kontrollmaßnahmen vorzusehen. Es sind Regelungen zu treffen, die sich insbesondere auf die Sicherheit des Verfahrensbetriebes und die Nachvollziehbarkeit einzelner Tätigkeiten beziehen. Der Betrieb der IT-Einrichtungen, die Sicherung von Daten sowie die Verwaltung, Benutzung und Verwahrung von Datenträgern sind entsprechend zu kontrollieren.

4.4.2 Sicherheitsmaßnahmen haben hierbei besondere Bedeutung und sich im Einzelfall am Schutzbedürfnis des betreffenden Verfahrens zu orientieren. Dabei sind Hard- und Software sowie bautechnische und organisatorische Vorkehrungen unter Beachtung der Wirtschaftlichkeit so aufeinander abzustimmen, daß Daten und Programme vor unberechtigter Kenntnisnahme und Nutzung, vor Verfälschung und vor Verlust geschützt sind.

Maßnahmen zur Gewährleistung der Sicherheit können unter anderem sein:

- Zugangsbeschränkung für Räume, in denen IT-Einrichtungen installiert sind,
- Einsatz von Sicherheitssoftware,
- nicht umgehbare Zugriffsberechtigungen,
- Sperrung der Betriebssystemebene,
- Abschließbarkeit der Geräte,
- Sperrung der Laufwerke für bewegliche Datenträger (z. B. für Disketten oder Magnetbandkassetten) gegen unbefugten Zugriff,
- sichere Aufbewahrung von Datenträgern und
- regelmäßige Datensicherung.

4.4.3 Beim Betrieb von APC und Mehrplatzsystemen ist insbesondere sicherzustellen, daß nur ordnungsgemäß erworbene Software eingesetzt wird. Über die eingesetzte Software ist für jedes Gerät ein Verzeichnis zu führen. Der ungenehmigte Einsatz privater Software und privater IT-Einrichtungen ist nicht zulässig. Ebenso dürfen dienstliche IT-Einrichtungen nicht ohne Genehmigung privat genutzt werden. Für selbstzuerstellende Software sind die Regelungen für die Durchführung von IT-Vorhaben entsprechend der Bedeutung der Software für die Aufgabenerledigung anzuwenden.

4.4.4 Bei tragbaren APC sind zusätzlich die Risiken zu berücksichtigen, die sich durch eine standortunabhängige Verwendung des Gerätes ergeben.

*4.4.5 Kann die erforderliche Sicherheit nicht gewährleistet werden, so ist auf den Einsatz arbeitsplatznaher IT zu verzichten.*

Für APC und arbeitsplatznah eingesetzte Mehrplatzsysteme ist eine Funktionentrennung nur selten durchführbar; so werden z. B. häufig die Daten am Arbeitsplatz gesichert und die Datenträger dort aufbewahrt. Auch bei Dialogverfahren ist – je nach Ausgestaltung des Verfahrens – die Funktionentrennung mehr oder weniger eingeschränkt, da die Verantwortung für die Verarbeitung der Daten teilweise bei den fachlich zuständigen Bereichen liegt. In diesen Fällen gelten die IT-Mindestanforderungen entsprechend. Der häufig niedrige Preis von APC und arbeitsplatznah eingesetzten Mehrplatzsystemen und die in der Regel leichtere Bedienbarkeit der Geräte darf nicht zu einem sorglosen Einsatz führen. Geringere Anforderungen an die Ordnungsmäßigkeit und Sicherheit des Betriebes könnten allenfalls aus dem Einsatzbereich der IT-Systeme, z. B. für weniger sensible Anwendungen, hergeleitet werden. Diese Anforderungen sind über die Abwägung von Sicherheits- und Wirtschaftlichkeitsaspekten zu begründen und müssen sich aus einer Risikoanalyse und einem Sicherheitskonzept (siehe Nr. 7.2) ergeben (Nr. 4.4.2).

Je nach Bedeutung des IT-Verfahrens können ggf. erhebliche Kosten entstehen, um die Ordnungsmäßigkeit und Sicherheit zu gewährleisten:

- So sind APC und arbeitsplatznah eingesetzte Mehrplatzsysteme unter Beachtung der Wirtschaftlichkeit ggf. durch Hardware und Software so zu erweitern, daß Schwachstellen – insbesondere bezüglich des Schutzes der Daten vor unberechtigter Kenntnisnahme, vor Verfälschung und Verlust – behoben werden (Nr. 4.4.2).
- Dialogorientierte Verarbeitung am Sachbearbeiterplatz kann gegenüber einer zentralen Belegerfassung Vorteile bringen. Insbesondere kann die Handhabung für den Benutzer einfacher sein. Der Rücklauf fehlerhafter, nicht verarbeiteter Vorgänge zur Korrektur sowie eine separate, ggf. fehleranfällige Datenerfassung einschließlich des organisatorisch häufig aufwendigen Datenträgerlaufes kann weitgehend fortfallen. Dem sind jedoch erhöhter Entwicklungsaufwand, zusätzlich benötigte Hardware und Systemsoftware, z. B. Steuereinheiten, Terminals, Dialog-Monitore, zusätzliche Kapazitäten wegen der ungleichmäßigen Lastverteilung (Belastungsspitzen zu den Hauptnutzungszeiten) sowie höhere Anforderungen an die Stabilität der Verfahren, um Arbeitsunterbrechungen zu verhindern, gegenüberzustellen.

Die durch diese Maßnahmen anfallenden Kosten müssen bei einer Wirtschaftlichkeitsbetrachtung berücksichtigt werden.

Im Hinblick auf die Sicherheit ist auch die Vertrauenswürdigkeit von Fremdsoftware zu prüfen. So sollten bei jeder Softwarelieferung Datenträger mit Schreibe- und Leseschutz in einer versiegelten Verpackung angefordert werden.

Auf dienstlich genutzten Geräten dürfen ausschließlich freigegebene oder für die Nutzung zugelassene IT-Verfahren betrieben werden. Die Einhaltung dieser Anforderung soll stichprobenmäßig kontrolliert werden. Dabei kann auch das nach den IT-Mindest-

anforderungen zu führende Bestandsverzeichnis herangezogen werden (Nr. 4.4.3, siehe auch Nr. 2.1.1).

Bei vernetzten IT-Systemen (siehe Nr. 4.5), die ggf. den Zugriff auf zentrale Datenbestände gestatten, z. B. über File-Transfer, und Zugang zu öffentlichen Netzen haben, ist die Sicherheit des gesamten Netzwerks an seinem schwächsten Glied – häufig einem APC – zu beurteilen. Ist das zu erreichende Sicherheitsniveau für ein Verfahren oder die im Zugriff befindlichen Daten nicht ausreichend, muß auf eine Vernetzung von APC mit den genannten Zugriffsmöglichkeiten verzichtet werden.

Der Beratung der Benutzer beim Einsatz dezentraler IT-Systeme, insbesondere APC, kommt große Bedeutung zu. Die Fähigkeit der Benutzer wird häufig überschätzt. Wegen der scheinbar leichten Bedienbarkeit vieler Standardprogramme werden die Anforderungen an die Benutzer der IT-Systeme vielfach unterschätzt. Daher sollte die regelmäßige Betreuung der Benutzer sichergestellt werden. Personen ohne spezielle IT-Kenntnisse mit Fachverantwortung, ggf. auch mit Entwicklungsverantwortung, sind aufgabengerecht zu schulen (siehe auch Nr. 3.4.6.3).

## 4.5 Einsatz von Netzwerken

4.5.1 Eine Vernetzung von IT-Geräten ist nur dann vorzusehen, wenn IT-Verfahren durch

- Datenübertragung,
- gemeinsame Nutzung von Hard- und Software,
- gemeinsamen Zugriff auf zentral oder dezentral gespeicherte Informationen

sicherer und wirtschaftlicher abgewickelt werden können. Die Erfüllung dieser Voraussetzungen ist im Rahmen der Vor- und Hauptuntersuchung nachvollziehbar zu dokumentieren.

4.5.2 Die Verwaltung und Steuerung des Netzwerkes soll durch geeignete Hard- und Software unterstützt werden. Entsprechend dem Umfang der Vernetzung sollen Netzwerkverwaltung und -steuerung als besondere Funktion vorgesehen werden, zu der insbesondere gehören:

- Verwaltung und Verteilung von Ressourcen, Informationen und Funktionen auf die Komponenten im Netzwerk,
- Sicherung der Daten,
- Verwaltung und Kontrolle der Zugriffsberechtigungen für das gesamte Netzwerk,
- Koordination, Überwachung und Durchführung der Netzwerkfunktionen so wie
- Erkennung, Eingrenzung und – soweit möglich – selbständige Behebung von Fehlern und Schwachstellen.

4.5.3 Kann die erforderliche Sicherheit im Netzwerkbetrieb nicht gewährleistet werden, so ist auf eine Vernetzung zu verzichten.

Unter einem Netzwerk soll hier die Verbindung von räumlich getrennten Systemen aus Hardware und Systemsoftware zum direkten Datenaustausch miteinander verstanden werden. Einfache Systeme in diesem Sinne sind z. B. Bildschirmarbeitsplätze mit Verbindung zu einem zentralen IT-System; komplexere Systeme sind z. B. miteinander verbundene Rechenzentren. Bei der Beschaffung der zu verbindenden Systeme sind die in der Gesamtplanung (Nr. 2.1) festgelegten Normen, Standards und Konventionen zu beachten (siehe auch Nr. 3.4.2). Sofern die Aufgabengerechtigkeit hierdurch gefördert wird – z. B. bei der Bürokommunikation oder bei der Vernetzung von Systemen über Grundstücksgrenzen hinweg – können Netze mit Zugängen zu allgemeinen Kommunikationsdiensten (z. B. DATEX-L, DATEX-P, TELETEX, BTX, TELEFAX, ISDN) ausgestattet werden.

Die durch die Vernetzung entstehenden Kosten müssen durch den zusätzlichen Nutzen gerechtfertigt sein (Nr. 4.5.1). Zu diesen Kosten trägt auch der Aufwand für die Ver-

waltung des Netzwerkes bei (Nr. 4.5.2). Wegen der für diese Aufgabe notwendigen Spezialkenntnisse sollte für die Netzwerkverwaltung und -steuerung eine besondere Funktion vorgesehen werden.

Die Vernetzung von Systemen birgt – insbesondere bei Netzen mit Zugängen über allgemeine Kommunikationsdienste und bei Netzen mit installierten Laufwerken zur Erzeugung transportabler, maschinenlesbarer Datenträger (z. B. Diskettenstationen in APC) – zusätzliche Sicherheitsrisiken. Die zur Aufrechterhaltung der Sicherheit geeigneten Maßnahmen sind aus der Risikoanalyse und dem Sicherheitskonzept (Nr. 7.2) abzuleiten und dem Umfang der Vernetzung, der Vertraulichkeit der Daten und der Anfälligkeit der Ressourcen anzupassen. Eine Maßnahme soll zumindest die restriktive, aktuelle, nicht umgehbare Vergabe von Zugriffsberechtigungen auf Ressourcen, Informationen und Funktionen des Netzes sein.

Zusätzlich sollte bei der Übertragung sensibler Daten über offene Netze eine Kryptierung erwogen werden. In jedem Fall sollte der Empfänger der Daten die Verbindung aufbauen, um den Netzzugang von unbekanntem Anschlüssen aus zu erschweren. Dazu können Rückrufsysteme (Call-Back-Units) eingesetzt werden, die die über das Datennetz anfragenden Benutzer nicht an das System durchschalten, sondern diese nach der Identifizierung unter deren eigener Nummer zurückrufen.

## 4.6 Einsatz von Datenbanksystemen

- 4.6.1 *Datenbanksysteme sollen so eingerichtet sein, daß die Strukturierung, Ablage, Verwaltung, Wiedergewinnung und Sicherung von Daten unabhängig von spezifischer Verfahrenssoftware ermöglicht wird.*
- 4.6.2 *Beim Einsatz von Datenbanksystemen sind insbesondere Maßnahmen zu treffen, die die Richtigkeit der Daten (Datenintegrität) und ihre Widerspruchsfreiheit (Datenkonsistenz) gewährleisten. Die im Verfahren verwendeten Datenstrukturen sollen durch eine wiederholungsfreie Darstellung änderungs- und erweiterungsfreundlich gehalten werden. Es ist sicherzustellen, daß Datenspeicherung und -wiedergewinnung nicht unkontrolliert erfolgen können. Dazu sind Regelungen zu treffen, die insbesondere Plausibilitätsbedingungen für Datenfelder und die Verarbeitungsschritte umfassen.*
- 4.6.3 *Die Verfahrenssoftware soll grundsätzlich unabhängig von der Datenstruktur sein. Dazu soll ggf. die Kommunikation zwischen Verfahrenssoftware und Datenbanksystem über eine standardisierte Schnittstelle erfolgen.*
- 4.6.4 *Das Datenbanksystem soll in das Zugriffsschutzsystem integriert sein, wobei der Zugriffsschutz nicht umgehbar sein darf.*
- 4.6.5 *Die Datenbestände sind regelmäßig hinsichtlich ihrer Aktualität und Gültigkeit zu überprüfen.*

Häufig werden Datenbanken im Rahmen mehrerer IT-Verfahren von verschiedenen Fachbereichen genutzt, die die Speicherung und Wiedergewinnung der Daten mit unterschiedlicher Zielrichtung durchführen. Änderungen der Datenstruktur sind daher nicht auszuschließen. Zudem führt der Wandel fachlicher Anforderungen zu Änderungen der Datenstrukturen.

Um derartige Änderungen möglichst wirtschaftlich durchführen zu können, sollten die Datenstrukturen entsprechend gestaltet (Nr. 4.6.2) und die Verfahrenssoftware unabhängig von der Datenstruktur der Datenbank sein (Nr. 4.6.3).

Dies kann durch die Verwendung einer standardisierten Datenbanksprache, z. B. SQL, und von Datenbankzugriffmodulen in den IT-Verfahren, die unabhängig von den übrigen Programmteilen sind, unterstützt werden. Datenbankmanagementsysteme, mit denen eine Datenbank verwaltet wird, sollten eine möglichst bedienerfreundliche Benutzeroberfläche haben. Wenn Möglichkeiten für Ad-hoc-Abfragen und -Änderungen bestehen, sind Maßnahmen zu ergreifen, damit diese nicht zum Unterlaufen der Datenintegrität und -konsistenz mißbraucht werden können. Der Zugriffsschutz darf, auch auf systemnaher Ebene, nicht umgehbar sein (Nr. 4.6.4).

Ein Datenbanksystem soll die Datenintegrität und -konsistenz gemäß den verfahrensspezifisch oder datenspezifisch vorgegebenen Regeln, – z. B. Plausibilitätsbedingungen für Datenfelder, Bildung von zusammengehörenden Arbeitsschritten (Transaktionslogik) mit Zurücksetzen von unvollständigen Änderungen bei fehlerhafter Verarbeitung, –

möglichst automatisch sicherstellen können, z. B. durch entsprechende Festlegungen im Rahmen der Definition der Datenstrukturen oder durch Prozeduren der Datenbanksprache (Nr. 4.6.2). Derartige Festlegungen erfordern erfahrungsgemäß einen hohen Abstimmungs- und Entwicklungsaufwand, der bei der Vorhabenplanung zu berücksichtigen ist.

Die Aktualität und Gültigkeit der Daten ist sowohl eine Fach- als auch eine IT-Aufgabe. Die für IT zuständigen Bereiche haben durch Kontroll- und Hilfsprogramme, durch technische Reorganisation der Datenbanken sowie Auslagerung und Archivierung nicht mehr benötigter Daten die Fachseite dabei zu unterstützen, die Daten aktuell und konsistent zu halten.

Bei umfangreichen Datenbanken oder vielfältigen, sich häufig ändernden fachlichen Anforderungen kann es wirtschaftlich sein, für die Verwaltung der Datenbanken einschließlich der Dokumentation und Festlegung der Bedeutung der Daten sowie der Integritäts- und Konsistenzregeln (Nr. 4.6.2) eine gesonderte Funktion vorzusehen (Datenbankadministration).



## 5 Erfolgskontrolle

- 5.1 *Die zuständige Stelle hat nach der Einführung eines IT-Verfahrens zu prüfen, ob der angestrebte Erfolg eingetreten ist und ob die veranschlagten Kosten eingehalten worden sind.*
- 5.2 *Die Ergebnisse der Überprüfung sind zu dokumentieren und evtl. erforderliche Maßnahmen zu ergreifen.*

Für den Begriff Erfolgskontrolle gibt es eine Vielfalt an Bezeichnungen und Definitionen sowie inhaltliche Überschneidungen und Unstimmigkeiten. Einen einheitlichen Begriff gibt es nicht. So werden neben dem Wort "Erfolgskontrolle" weitere Bezeichnungen mit unterschiedlichem, ähnlichem, gleichen oder teilweise identischem Begriffsinhalt verwendet: "Ergebniskontrolle", "Ergebnisbewertung", "Evaluation", "Effektivitätskontrolle", "Nachschaurechnung", "Nachkalkulation", (interne/externe) "Effizienzkontrolle", "Wirtschaftlichkeitskontrolle". Die Erfolgskontrolle läßt sich als Verfahren kennzeichnen, das dazu dient, festzustellen, bis zu welchem Grad die angestrebten Ziele erreicht worden sind.

Durch Schwächen bei Entwurf und Ausführung eines IT-Verfahrens, durch zwischenzeitlich andere fachliche Anforderungen und neue externe Vorgaben, z. B. durch gesetzliche Bestimmungen, durch andere technische Möglichkeiten, durch Änderungen des Benutzerumfeldes oder durch zwischenzeitlich aufgetretenen Einschränkungen, wie Kürzung der erforderlichen Haushaltsmittel, kann es dazu kommen, daß der Erfolg eines IT-Verfahrens nicht im vorgesehenen Umfang eintritt. Durch eine Erfolgskontrolle können Verfahrensschwachstellen oder im nachhinein unrealistische, nicht umsetzbare Zielsetzungen erkannt werden. Die Ergebnisse der Erfolgskontrolle können beispielsweise für die Organisation der Behörde und die Planung künftiger Vorhaben sowie die Anpassung des eingeführten Verfahrens genutzt werden.

Die Erfolgskontrolle ist grundsätzlich Aufgabe der Verwaltung. Im IT-Rahmenkonzept sind für jedes Verfahren Angaben zur Erfolgskontrolle erforderlich<sup>7</sup>. Die Stelle, die die Erfolgskontrolle durchführt, sollte möglichst außerhalb der Stellen für IT angesiedelt sein.

Bei Prüfungen sollte vor allem darauf hingewirkt werden, daß Erfolgskontrollen wie vorgesehen durchgeführt werden ("Erfolgskontrolle der Erfolgskontrolle").

Die Erfolgskontrolle bezieht sich auf den Zeitraum, in dem die zu untersuchende Maßnahme bereits wirksam war. Gleichwohl bedeutet dies nicht erst eine Untersuchung nach Abschluß aller mit der Einführung eines IT-Verfahrens zusammengehörenden Maßnahmen. Vielmehr sollte die Erfolgskontrolle so zeitnah wie möglich, ggf. auch bereits bei Teilmaßnahmen, deren Ergebnis schon beurteilt werden kann, und unter Beachtung der Grundsätze Ordnungsmäßigkeit, Sicherheit und Wirtschaftlichkeit erfolgen.

---

<sup>7</sup> siehe Bundesministerium des Innern [Hrsg.]: Gliederung der IT-Rahmenkonzepte mit Hinweisen und Erläuterungen zu ihrer Erstellung und Fortschreibung Stand 31. Mai 1990 (Schriftenreihe der KBSt; Band 18); dort Nr. 2.8

Als Grundlage von Kontrollen sollten den ursprünglich ermittelten Kosten und Aufwendungen (z. B. Personal) sowie dem angestrebten Nutzen die tatsächlich entstandenen Ausgaben (Investitionen, Betriebskosten und sonstige Aufwendungen) und der erzielte Nutzen gegenübergestellt werden. Die Erfolgskontrolle kann somit als ein Anwendungsfall einer Nutzen-Kosten-Untersuchungen angesehen werden (siehe auch Anhang 4 Hinweise zu Wirtschaftlichkeitbetrachtungen) und ist jedenfalls mehr als ein bloßer Erfolgsbericht.

Über einen Vergleich der tatsächlichen mit den geplanten Kosten können die Bewertung der Wirtschaftlichkeit des Verfahrens erleichtert und Hinweise zur Neu- oder Weiterentwicklung der Verfahren sowie zur Umgestaltung der übrigen Ressourcen, z. B. zur Anpassung von Rechnerkapazitäten, gewonnen werden.

Wichtigste Voraussetzung einer wirksamen Erfolgskontrolle sind operationale Zielkriterien, die möglichst alle Ziele erfassen, damit die den Erfolg beeinflussenden Größen auch kontrollierbar sind. Das ist dann am einfachsten, wenn die Zielsetzung (siehe Nr. 2.1 und Nr. 3.3) in quantifizierbaren Größen oder Kennzahlen ausgedrückt ist. Derartige Kennzahlen können beispielsweise die Zeit für die Bearbeitung eines Vorgangs, die Kosten je Dialogschritt oder die Kosten je Ausgabedokument sein.

Empfehlenswert ist der regelmäßige Vergleich der Kosten und des Nutzens der eigenen IT mit denen vergleichbarer Institutionen, um die Ursachen negativer Abweichungen zu ermitteln und ggf. Gegenmaßnahmen abzuleiten.

Der Bundesbeauftragte für Wirtschaftlichkeit in der Verwaltung gibt im Band 2 seiner Schriftenreihe Hinweise zur Erfolgskontrolle<sup>8</sup>.

---

<sup>8</sup> Der Präsident des Bundesrechnungshofes als Bundesbeauftragter für Wirtschaftlichkeit in der Verwaltung [Hrsg.]: Erfolgskontrolle finanzwirksamer Maßnahmen in der öffentlichen Verwaltung: Gutachten des Präsidenten des Bundesrechnungshofes als Bundesbeauftragter für Wirtschaftlichkeit in der Verwaltung, abgeschlossen im Juni 1989 (Schriftenreihe des Bundesbeauftragten für Wirtschaftlichkeit in der Verwaltung; Band 2) – Stuttgart; Berlin; Köln: Kohlhammer, 1989

## 6 Qualitätssicherung

- 6.1 *Die Verfahrensentwicklung und der -betrieb sind laufend im Hinblick auf die durchgängige Beachtung der festgelegten Vorgehensweisen und Arbeitstechniken (Methoden und Werkzeugen) zu überprüfen und zu bewerten. Die Prüfung und Bewertung soll anhand von im voraus festgelegten Qualitätsnormen erfolgen. Bei Abweichungen sind entsprechende Maßnahmen zu treffen.*
- 6.2 *In angemessenen Zeitabständen ist zu überprüfen, ob Verfahren ordnungsgemäß angewandt werden und evtl. Schwachstellen zu beseitigen sind. Das Ergebnis der Prüfung und die eingeleiteten Maßnahmen sind zu dokumentieren.*

Zwischen- und Endergebnisse können bereits im Verlauf eines Vorhabens frühzeitig geprüft werden, um deren Qualität zu sichern und so den darauf aufbauenden Tätigkeiten eine korrekte, verwertbare, Folgefehler vermeidende Grundlage für die weitere Arbeit zu bieten.

Methoden für die Qualitätssicherung sind z. B.

- die (maschinelle oder manuelle) Inspektion,
- das schrittweise Nachvollziehen von Arbeitsschritten (Walk Through) und
- die Abstimmungssitzung.

Die Prüfung formaler Qualitätsnormen, z. B. die Verwendung oder Vermeidung bestimmter Befehle in Programmen oder das Erreichen eines bestimmten Antwortzeitverhaltens beim Betrieb der Verfahren, aber auch die Einhaltung bestimmter Vorgehensweisen, z. B. die Vollständigkeit der Ergebnisse eines Vorhabensabschnittes, kann maschinell unterstützt werden.

Die Funktionen Entwicklung und Pflege von Verfahren auf der einen und Qualitätssicherung auf der anderen Seite sollten nicht von demselben Mitarbeiterkreis wahrgenommen werden.

Bei der Verfahrensentwicklung soll die interne Qualitätssicherung laufend vorgenommen werden. Zusätzlich sollten die fachlich zuständigen Stellen eine Qualitätssicherung jeweils nach dem Abschluß eines Vorhabensabschnittes auf der Grundlage der bis dahin erstellten Ergebnisse durchführen. Bei der Festlegung der Vorgehensweise zur Vorhabensdurchführung soll die Qualitätssicherung berücksichtigt werden (siehe Nr. 3.2).

# 7 Sicherheit beim Einsatz der IT

## 7.1 Allgemeines

*Den Risiken beim Einsatz der Informationstechnik ist durch organisatorische, personelle und technische Maßnahmen zur Sicherheit der IT Rechnung zu tragen. Insbesondere muß die Informationstechnik vor Risiken geschützt werden, die zu*

- unberechtigter Kenntnisnahme (Verlust der Vertraulichkeit),*
  - unberechtigter Veränderung oder Verfälschung (Verlust der Integrität) und*
  - Beeinträchtigung oder Verlust der Verfügbarkeit (Verlust der Funktionalität)*
- von Daten und Programmen führen. Verantwortlichkeiten sind in Dienstweisungen festzulegen.*

Risiken können grob klassifiziert werden

nach der Auswirkung in

- Verlust der Vertraulichkeit,
- Verlust der Integrität und
- Verlust der Verfügbarkeit

oder nach der Ursache in

- höhere Gewalt (technisches Versagen, Katastrophen),
- fahrlässiges Handeln (menschliches Versagen) und
- vorsätzliches Handeln (Manipulation, Spionage, Sabotage).

Sicherheitsmaßnahmen sollen

- die Eintrittswahrscheinlichkeit der Risiken verringern,
- den Eintritt des Risikofalles zuverlässig erkennbar machen und
- den möglichen Schaden gering halten.

(Siehe auch die Hinweise auf Risiken beim Einsatz der IT und wiederkehrende Mängel bei der Sicherheit der IT im Band 3 der Schriftenreihe<sup>9</sup> des Bundesbeauftragten für Wirtschaftlichkeit in der Verwaltung).

Je nach der Art des eingesetzten Verfahrens können die Maßnahmen unterschiedliche Ausprägung haben. So liegt bei kassenwirksamen Verfahren der Schwerpunkt der Sicherheitsmaßnahmen auf

---

<sup>9</sup>Der Präsident des Bundesrechnungshofes als Bundesbeauftragter für Wirtschaftlichkeit in der Verwaltung [Hrsg.]: Datenverarbeitung in der Bundesverwaltung: Feststellungen und Hinweise des Präsidenten des Bundesrechnungshofes als Bundesbeauftragter für Wirtschaftlichkeit in der Verwaltung zu Mängeln und Risiken beim Einsatz der Informationstechnik (Schriftenreihe des Bundesbeauftragten für Wirtschaftlichkeit in der Verwaltung; Band 3) – Stuttgart, Berlin, Köln: Kohlhammer, 2. Auflage 1993

- dem Schutz der Daten und Programme vor Verfälschung und Verlust der Verfügbarkeit,
- der Verhinderung des manipulierten Betriebes der Verfahren,
- der nachträglichen Erkennbarkeit von Manipulationen sowie
- der Nachvollziehbarkeit der Verarbeitung.

Die Sicherheitsmaßnahmen müssen die Fehlleitung von Zahlungen, z. B. zur persönlichen Bereicherung, weitestgehend ausschließen und die Beleg- und Kontenfunktion im Sinne der Speicherbuchführung für die Dauer der gesetzlichen Aufbewahrungsfristen zuverlässig sicherstellen. Im Hinblick auf die Nachvollziehbarkeit des Verfahrens ist die Dokumentation bei einem automatisierten Verfahren als Bestandteil des Haushalts-, Kassen- und Rechnungswesens anzusehen und unterliegt somit den gesetzlichen Aufbewahrungsfristen. Zur Dokumentation zählen in diesem Zusammenhang sowohl die Entwicklungsdokumentation – z. B. Programm- und Moduldokumentation einschließlich der Umwandlungslisten – als auch die Betriebsdokumentation – z. B. Produktions- und Änderungsnachweise, Zugriffsprotokolle. Voraussetzung für die Nachvollziehbarkeit eines Verfahrens ist ein ordnungsgemäßes Freigabeverfahren mit einem Versionenkonzept.

Spezifische Anforderungen an kassenwirksame Verfahren finden sich in den Bestimmungen<sup>10</sup> über den Einsatz von automatisierten Verfahren im Haushalts-, Kassen- und Rechnungswesen (HKR-ADV-Best (B)).

Bei Verfahren mit besonderen Anforderungen an die Vertraulichkeit der Daten, z. B. im Verteidigungs- und Sicherheitsbereich steht der Schutz der Daten und Programme vor unberechtigter Kenntnisnahme und Verfälschung im Vordergrund. Spezifische Anforderungen finden sich in den Richtlinien<sup>11</sup> für den Schutz von Verschlusssachen in der automatisierten Datenverarbeitung.

Bei technischen Verfahren zur Steuerung von kritischen Prozessen liegt der Schwerpunkt der Sicherheitsmaßnahmen auf der Funktionssicherheit. Maßnahmen in diesem Zusammenhang sind z. B.

- die ausreichende Kapazität und Stabilität der Hardware, der Systemsoftware und der Verfahren,
- die ausreichende bauliche Sicherung und
- die aufgabengerechte Notorganisation mit einer hinreichend kurzen Wiederanlaufzeit oder einer gesicherten Weiterführung oder Beendigung des Verarbeitungsprozesses.

Für alle Verfahren ist die ordnungsgemäße und sichere Verfahrensentwicklung mit geordneter Vorgehensweise (siehe Nr. 3.1, 3.2, 3.3, 3.4.4), Risikoanalyse, Sicherheitskonzept (Nr. 7.2) und umfangreichen Tests sowie der ordnungsgemäße und sichere Verfahrensbetrieb mit dem ausschließlichen Einsatz von getesteten, dokumentierten und

<sup>10</sup> siehe Nr. 1.1 (Fußnote auf Seite 10)

<sup>11</sup> Der Bundesminister des Innern: Richtlinien für den Schutz von Verschlusssachen in der automatisierten Datenverarbeitung (Richtlinien für Daten-VS) – Schreiben an die Obersten Bundesbehörden vom 13. Januar 1981, Az. IS 4 - 608 090/1 VS-NfD

freigegebenen Verfahren sicherzustellen (Nr. 3.4.5, 3.4.6, 3.5 und Nr. 4). In die Verfahren sind im Rahmen des technisch Möglichen maschinelle Kontrollen und Abstimmungen zu integrieren.

## 7.2 Risikoanalyse und Sicherheitskonzept

7.2.1 *Die zur Aufrechterhaltung der Sicherheit geeigneten Maßnahmen sind aus einer Risikoanalyse abzuleiten und in einem Sicherheitskonzept darzustellen. Im Rahmen der Risikoanalyse sollen mindestens folgende Punkte behandelt werden:*

- *Feststellung der Bedeutung der IT und einzelner Verfahren für die Aufgabenerfüllung,*
- *Erfassung erkennbarer Bedrohungen im Zusammenhang mit dem Einsatz der IT,*
- *Abschätzung der Eintrittswahrscheinlichkeit der Bedrohung,*
- *Quantitative oder qualitative Abschätzung der möglichen Schäden durch die Bedrohung unter Berücksichtigung ihrer Eintrittswahrscheinlichkeit sowie*
- *Ermittlung geeigneter Maßnahmen zur Gewährleistung eines ausreichenden Sicherheitsstandards einschließlich ihrer Kosten.*

*Die Ergebnisse der Risikoanalyse sind vor dem Hintergrund der Grundsätze der Ordnungsmäßigkeit und Wirtschaftlichkeit sowie eines hinnehmbaren Restrisikos abzuwägen.*

7.2.2 *Aufbauend auf der Risikoanalyse und dem Sicherheitskonzept sind im erforderlichen Umfang technische und organisatorische Sicherheitsmaßnahmen festzulegen, die aufeinander abzustimmen sind.*

7.2.3 *Die Maßnahmen zur Datensicherung müssen den Erfordernissen der Aktualität, Sicherheit und Wiederherstellbarkeit Rechnung tragen, z. B. durch angemessen häufige Sicherungen, eine geeignete Sicherungstechnik und Aufbewahrung der Datenträger.*

7.2.4 *Gegen Fehlbedienungen und unbeabsichtigte Änderungen von Daten sind geeignete Maßnahmen zu treffen.*

7.2.5 *Räumlichkeiten, die der Unterbringung von IT-Einrichtungen und Datenträgern dienen (insbesondere Rechenzentren), sind dem Risiko angemessen baulich zu sichern.*

7.2.6 *Die Wirksamkeit der Sicherungsmaßnahmen ist in regelmäßigen Abständen zu überprüfen.*

Für die optimale Auswahl der zu ergreifenden Maßnahmen und ihre Abstimmung aufeinander ist eine geordnete, methodisch begründete Vorgehensweise – die Risikoanalyse – vorzusehen (Nr. 7.2.1). Darauf aufbauend sind die zu ergreifenden Maßnahmen zusammenzustellen und im Sicherheitskonzept derart aufeinander abzustimmen, daß sie technisch und organisatorisch lückenlos zusammenwirken (Nr. 7.2.2). Hinweise auf Maßnahmen im einzelnen finden sich in den Erläuterungen zu Nr. 7.3.

Grundlage für die Erstellung eines umfassenden Sicherheitskonzeptes ist eine verfahrensbezogene Risikoanalyse. Dabei sind die Bedrohungen und die daraus resultierenden möglichen Schadenshöhen beim Eintreten des Risikofalles zu bewerten. Um die Bewertung sachgemäß durchführen zu können, ist es unverzichtbar, den Träger des Verfahrens in die Analyse einzubeziehen. Erst solche Analysen können Aufschluß darüber geben, welcher finanzielle, organisatorische und personelle **Sicherheitsaufwand** gegenüber den möglichen Bedrohungen und Risiken **wirtschaftlich angemessen** ist und welche Risiken als **tolerable Restrisiken** hingenommen werden können.

Bei der Erstellung der Risikoanalyse sollten folgende Punkte beachtet werden:

- Die möglichen Risiken sind für jedes IT-Verfahren aufzuzeigen und in einer Übersicht zusammenzufassen.
- Die Auswirkungen einzelner Risiken und mögliche verfahrensspezifische Schäden sind kurz zu beschreiben und ggf. zu quantifizieren (Schätzwerte). Dabei ist die Bedeutung des Verfahrens für die Verwaltung anzugeben, hinnehmbare Ausfallzeiten sind abzuschätzen, z. B. Verfahren muß immer verfügbar sein, Verfahren kann maximal zwei Tage ausfallen. Die Schätzung der hinnehmbaren Ausfallzeiten ist nachvollziehbar zu begründen.
- Die möglichen Schadenswerte sind, falls möglich, mit der Wahrscheinlichkeit ihres Eintreffens grob zu gewichten, z. B. unwahrscheinlich – wenig wahrscheinlich – wahrscheinlich.

Ziel dieser Analyse ist es, ein möglichst vollständiges Bild der Risiken, Abhängigkeiten und möglichen Schäden der IT-Verfahren in der Verwaltung zu erhalten.

Basierend auf den festgestellten und bewerteten Risiken sind Vorbeuge- und Gegenmaßnahmen auf ihre Eignung zu prüfen und deren Kosten überschlägig zu ermitteln. Die Maßnahmen können

- bauliche,
- organisatorische (einschließlich personelle),
- gerätetechnische oder
- programmtechnische

Aspekte betreffen. Sie müssen so beschaffen sein, daß sie gegenüber den aufgezeigten Risiken schadensverhindernd, zumindest aber schadensbegrenzend wirken. Da die Sicherheitsmaßnahmen in der Regel mit

- Kosten,
- zusätzlichem Personalaufwand,
- geringerem Datendurchsatz bei der Verarbeitung und
- Komplizierung des Verwaltungshandelns

verbunden sind, müssen sie entsprechend den möglichen Schäden, die ohne Vorkehrungen eintreten können, unter wirtschaftlichen Gesichtspunkten gewählt werden.

Die Risiken, die nach wirtschaftlicher Abwägung der möglichen Schäden und der Kosten der dagegen gerichteten Sicherheitsmaßnahmen nicht abgedeckt werden, bilden das



zu **tolerierende Restrisiko**. Dieses ist den Verfahrensverantwortlichen bekanntzumachen.

Würden keine Risikoanalysen erstellt, so könnte nicht festgestellt werden, ob die zu treffenden Sicherheitsmaßnahmen dem Schutzbedürfnis der IT-Anwendung angemessen sind und wirtschaftlich gestaltet werden.

Nachdem in der Risikoanalyse festgelegt wurde, welche Sicherheitsteilmaßnahmen für die IT-Verfahren bei Inkaufnahme des tolerablen Restrisikos durchgeführt werden sollen, ist im nächsten Schritt das Sicherheitskonzept zu erstellen. Es soll insbesondere Aussagen

- zur Aufgabenverteilung und zu den Zuständigkeiten für IT-Sicherheit,
- zum IT-Basissystem und seiner Konzeption,
- zur Verfahrenssoftware und ihrer Konzeption,
- zu dezentralen Systemen,
- zu Netzwerken,
- zur Funktionentrennung und Personenunabhängigkeit,
- zur Zugriffsberechtigung,
- zur Zutrittsberechtigung,
- zum Verursacher- und Verwendungsnachweis,
- zur Datensicherung,
- zum Datentransport,
- zur Datenvernichtung,
- zur baulichen Sicherung,
- zur Produktion,
- zur Änderung der Produktionsumgebung und
- zur Notorganisation

beinhalten und die erforderlichen Maßnahmen beschreiben.

Da sich die Gesamtsicherheit von IT-Verfahren erst aus dem Zusammenspiel aller Teilmaßnahmen ergibt, ist im Sicherheitskonzept auch darzulegen, wie die einzelnen Teilmaßnahmen technisch und organisatorisch zusammenwirken sollen, um einen möglichst großen Schutz zu gewährleisten.

Eine unverzichtbare Voraussetzung für die Gewährleistung von Sicherheit ist die laufende Kontrolle der Wirksamkeit aller im Sicherheitskonzept aufgeführten technischen und personellen Maßnahmen. Auf welche Weise diese Kontrollen durchgeführt werden, ist ebenfalls im Sicherheitskonzept darzustellen.

Das Sicherheitskonzept bedarf der laufenden Aktualisierung, um

- die Sicherheitsmaßnahmen den sich ändernden IT-Verfahren anzupassen,
- neue technische Möglichkeiten zu berücksichtigen und
- den Veränderungen der Bedrohung entsprechen

zu können.

Für viele IT-Anwendungen gelten ähnliche Sicherheitsaspekte. Die Anwendungen können deshalb zur Vereinfachung in Gruppen zusammengefaßt werden, z. B. Verfahren der Bürokommunikation, kassenwirksame Verfahren usw. Für diese **Gruppen von Anwendungen mit ähnlichen Randbedingungen** lassen sich die Risiken und möglichen Schäden **zusammenfassend in der Risikoanalyse darstellen**, um eine aufwendige Einzeldarstellung mit laufenden Wiederholungen zu vermeiden.

Durch ein Paket von Grundsicherheitsmaßnahmen, die jeweils dem derzeitigen Stand der Technik und allgemein anerkannten Sicherheitsstandards entsprechen müssen, kann im allgemeinen bereits ein Großteil der üblicherweise bestehenden Risiken abgedeckt werden. Diese **Grundsicherheitsmaßnahmen** können **ebenfalls summarisch** im Sicherheitskonzept dargestellt werden.

**Detailliert darzustellen** sind in der Risikoanalyse diejenigen Verfahren, die im Hinblick auf Gefährdung und Schadensmöglichkeiten **Besonderheiten** aufweisen und zu deren Absicherung Sicherheitsmaßnahmen notwendig sind, die von den Standardmaßnahmen abweichen oder besonders kostenträchtig sind.

Besonderes Augenmerk ist hierbei den Bereichen Datensicherung und Backup zu widmen, die je nach Notwendigkeit der Verfügbarkeit

- einfache Datenträgersicherung,
- Ausweichrechenzentrum oder
- Parallelbetrieb

erforderlich machen können. Wegen möglicher hoher Kosten sind Maßnahmen dieser Art besonders sorgfältig zu erläutern.

Für die Angabe bzw. die Abschätzung möglicher Schadenshöhen und Kosten einzelner Sicherheitsmaßnahmen können Erfahrungswerte aus vergangenen Zeiträumen herangezogen werden.

Bei Neuentwicklungen muß die Risikoanalyse Bestandteil der Vorgehensweise zur Verfahrensentwicklung sein, das Sicherheitskonzept ist bei Entwicklung und Betrieb zu berücksichtigen. Für bestehende Verfahren, für die noch kein Sicherheitskonzept vorliegt, soll eine Risikoanalyse im Rahmen der Pflege nachgeholt und das entstehende Sicherheitskonzept angemessen umgesetzt werden (siehe auch Nr. 3.5).

Risikoanalyse und Sicherheitskonzept sind zu dokumentieren (siehe auch IT-Richtlinien, Nr. 4 und Nr. 10).

Das vorhandene oder auszuwählende IT-Basissystem bestimmt wesentlich, welche Sicherheitsmaßnahmen eingerichtet werden können. Dementsprechend sind die erforderlichen Sicherheitsmaßnahmen bereits bei der Beschaffung zu berücksichtigen (Nr. 3.4.2). Insbesondere muß das IT-Basissystem eine hinreichende Stabilität gegen Störungen aufweisen. Bei Betrieb mehrerer IT-Verfahren auf dem gleichen IT-Basissystem, ist die Stabilität am Bedarf des Verfahrens mit den höchsten Ansprüchen an die Zuverlässigkeit zu orientieren. Den Störungen wie

- fahrlässige oder vorsätzliche Fehlbedienung,
- Ausfall der Stromversorgung,
- Ausfall oder Fehlfunktion einzelner Systembestandteile

können folgende Maßnahmen zur Förderung der Stabilität entgegenwirken:

- die konzeptionelle Berücksichtigung der Sicherheitsanforderungen bei Planung des IT-Basissystems,
- eine unterbrechungsfreie Notstromversorgung,
- eine regelmäßige, vorbeugende Wartung,
- die Ausbildung von Personal zur Vornahme von Reparaturen mit Lagerhaltung häufig benötigter Ersatzteile,
- die Schulung und Betreuung der Benutzer sowie
- eine geordnete Vorgehensweise bei der Änderung des IT-Basissystems mit hinreichenden Tests.

Für alle, insbesondere aber für personenbezogene Daten dürfen nur berechtigte Zugriffe sowohl zum Lesen als auch zur Veränderung oder Löschung zugelassen werden. Die Maßnahmen zur Zugriffsberechtigung sind durch geeignete Maßnahmen zur Zutrittsberechtigung zu ergänzen, um den unberechtigten Zugriff auf Hardware und Datenträger zu verhindern oder zumindest nachträglich erkennbar machen. Wichtige Maßnahmen zur Zugriffsberechtigung sind insbesondere

- die restriktive, aktuelle, personen- und aufgabenbezogene Vergabe und ständige maschinelle Kontrolle von Zugriffsvollmachten und
- das Protokollieren der Zugriffe und des Zeitpunkts mit Angabe des eindeutig, z. B. über ein Kennwort, identifizierten verantwortlichen Mitarbeiters.

Im Hinblick auf die Datensicherheit sind Maßnahmen gegen den Verlust von Daten und die Wiederherstellung eines konsistenten Datenzustandes nach einer Störung in angemessener Zeit zu ergreifen (Nr. 7.2.3). Zu den Maßnahmen zählen insbesondere

- die konzeptionelle Berücksichtigung der Datensicherung in der Verfahrensentwicklung,
- die Datensicherung,
- die katastrophensichere Aufbewahrung der Sicherungsmedien sowie
- die detaillierte Festlegung des Vorgehens zum Wiederanlauf der Verfahren mit dem Schwerpunkt auf der Beschreibung der Wiederherstellung eines konsistenten Datenzustandes.

Dabei ist zu beachten, daß die Wiederherstellung eines Datenbestandes nur in wenigen Fällen lediglich mit standardmäßig vorhandenen Funktionen der betriebssystemnahen Software gelingt. Vielmehr sind die Erfordernisse der Wiederherstellung eines Datenbestandes und des Wiederanlaufs auch in der Anwendungssoftware zu berücksichtigen und vor der Einführung eines Verfahrens entsprechend zu erproben.

Die Datenintegrität, d. h. die Eintragung gültiger und nicht manipulierter Werte in die Datenfelder, und die Datenkonsistenz, d. h. die ggf. datei- bzw. datenbankübergreifende

Widerspruchsfreiheit der Werte aller Datenfelder, ist über Kontrollen (z. B. Plausibilitätsprüfungen) und Abstimmungen (z. B. Abstimmsummen) sicherzustellen. Die Wahrung der Datenkonsistenz kann durch eine geeignete Gestaltung der Datenstrukturen – z. B. durch die Widerspruchsfreiheit und die Verträglichkeit von Feldtypen und -längen – erleichtert werden (siehe auch Nr. 4.6).

Fehlerträchtige Funktionen können durch zusätzliche Kontrollen – z. B. nach dem Vier-Augen-Prinzip – besonders abgesichert werden.

In vielen Fällen reichen die Sicherheitsmechanismen des IT-Basissystems oder der Standardsoftware, z. B. der Datenbanksysteme, nicht aus, um die Datenkonsistenz aufrecht zu erhalten (siehe auch Nr. 4.6). In diesen Fällen müssen Sicherheitsmaßnahmen der Verfahrenssoftware auf der einen und des IT-Basissystems mit Hardware und Systemsoftware auf der anderen Seite so aufeinander abgestimmt werden, daß ein vorsätzliches oder fahrlässiges Umgehen der Maßnahmen wirksam verhindert oder nachweisbar wird.

Die Verfahrenssoftware muß eine dem Verfahren angemessene Stabilität gegen Störungen aufweisen. Störungen können beispielsweise sein:

- vorsätzliche oder fahrlässige Fehlbedienung,
- Datenfehler,
- Programmfehler und
- Ausfall der Hardware oder der Systemsoftware.

Die Verfahrenssoftware muß Störungen wie die beiden erstgenannten

- erkennen und aufzeichnen,
- wenn möglich maschinell beheben oder zur manuellen Behebung auffordern und
- die Bearbeitung geordnet fortsetzen oder beenden.

In jedem Fall müssen Störungen nachträglich erkennbar und die Fehlerursache ermittelbar sein. Durch ein festgelegtes Vorgehen für den Wiederanlauf mit der Wiederherstellung eines konsistenten Datenbestandes müssen Störungen nach den Anforderungen der Verfahren in angemessener Zeit behoben werden können.

Besondere Bedeutung kommt der Stabilität bei der Dialog- und Prozeßbearbeitung zu, da diese direkt an die Arbeitsabwicklung gekoppelt ist und eine Störung direkte Auswirkungen auf den Arbeitsfortschritt im Fachbereich bzw. auf die Sicherheit und die Ergebnisqualität des Prozesses hat (siehe auch Nr. 4.4 und Nr. 4.5).

Zielsetzung der baulichen Sicherung (Nr. 7.2.5) ist der Schutz von Ressourcen der IT vor den Risiken der Zerstörung durch äußere Gewalteinwirkung (Feuer, Explosion, Wasser usw.), Sabotage und Einstrahlung. Räumlichkeiten, die der Unterbringung von Datenträgern und Datenverarbeitungsanlagen dienen, z. B. Rechenzentren, sind dem Risiko entsprechend angemessen baulich zu sichern. Die erforderlichen baulichen Maßnahmen sollen bestimmt sein durch die Kosten für deren Umsetzung und die dadurch erreichte Begrenzung des möglichen Schadens.

Organisatorische Sicherungsmaßnahmen, z. B. Zutrittskontrollen durch Pförtner, sollen sich mit baulichen Vorkehrungen ergänzen. In Abwägung des jeweiligen Risikos können die Räumlichkeiten zur Unterbringung von Datenträgern und Datenverarbeitungsanlagen beispielsweise verfügen über

- nur einen Zugang, um den Zutritt in bestmöglicher Weise überwachen zu können (weitere Ausgänge sollen nur dann vorhanden sein, wenn diese als Notausgänge eingerichtet sind und eine unkontrollierte Benutzung verhindert wird, z. B. durch Alarmverriegelungen),
- Alarmanlagen (optisch und akustisch), um Pförtner und Polizei auf Störungen aufmerksam zu machen,
- Monitore, um schwer einsehbare Gebäudeteile und Flächen überwachen zu können,
- Außenglas, das einem Anschlag widerstehen kann und zusätzlich durch Splitterglasfolien gesichert ist,
- Rauchmelder, um die Entstehung eines Feuers zum frühestmöglichen Zeitpunkt entdecken zu können,
- Brandschutzwände sowie Brandschutztüren mit Selbstschließvorrichtung, um das Übergreifen eines Feuers zu verhindern,
- Rauchabschottung, um bei einem Feuer das Verrauchen weiterer Gebäudeteile zu vermeiden,
- Decken, Trennwände und Verkleidungen, die aus nicht-brennbarem Material bestehen,
- Wasserschutz an Wänden und Decken, um das Eindringen von Wasser – z. B. bei einem Löschvorgang – zu verhindern und
- Wasserabflußmöglichkeiten, Rücklaufventile und zusätzliche Abdichtungen, um einen Wasserschaden durch Leckagen an Leitungen, Rückstau in Abwasserkanälen und Überflutung bei starkem Regen zu verhindern. (Insbesondere sollen Räumlichkeiten vorgesehen werden, die oberhalb eines Gefährdungsniveaus durch Hochwasser liegen.)

Die genannten Sicherungsmaßnahmen sind auf die Umgebung der zu schützenden Räumlichkeiten zur Unterbringung von Datenträgern und Datenverarbeitungsanlagen auszudehnen, wenn die Wirksamkeit der Sicherungsmaßnahmen dadurch begünstigt wird.

Die Funktionsfähigkeit der baulichen Sicherungsmaßnahmen ist – wie die übrigen Sicherungsmaßnahmen auch – in angemessenen Abständen zu prüfen.

### 7.3 Regelungen zur Sicherheit der IT

*Übergreifende Maßnahmen zur Sicherheit der IT müssen in speziellen Regelungen verbindlich festgelegt werden. Insbesondere sollen Aussagen über Zugangsberechtigungen, Zutrittsberechtigungen, Zugriffsberechtigungen, Datensicherung sowie Weitergabe, Verwendung und Transport von Daten getroffen werden.*

Der Inhalt der Regeln im einzelnen hat sich an den Schutzbedürfnissen der Daten und Anwendungen zu orientieren. Der im folgenden beispielhaft dargestellte Regelungsumfang muß daher entsprechend dem Sicherheitskonzept an den Einzelfall angepaßt werden.

Über Regelungen zur Zutrittsberechtigung ist sicherzustellen, daß nur entsprechend bevollmächtigte Personen Zutritt zu Räumen erhalten, in denen sich Hardwareeinrichtungen oder Datenträger befinden. Die Berechtigung ist mitarbeiterbezogen und aufgabengerecht zu staffeln und zeitnah zu vergeben. Der Zutritt soll weitgehend durch technische Maßnahmen geprüft werden. Wird nicht-autorisierten Personen der Zutritt gewährt, sollen sie von autorisiertem Personal begleitet werden. Informationen, für die der Besucher keine Berechtigung hat, dürfen ihm nicht auf dem Wege des direkten Zugangs bekannt werden. Die Mitnahme von Gegenständen, insbesondere von Datenträgern, ist durch geeignete Maßnahmen – z. B. durch Verbot der Mitnahme von Taschen in das Rechenzentrum oder durch Datenträgerbegleitpapiere – zu verhindern. Zutritt und Verlassen der Räume sind im Hinblick auf die spätere Nachvollziehbarkeit zu protokollieren.

Über eine Regelung zur Zugriffsberechtigung ist sicherzustellen, daß nur entsprechend bevollmächtigte Personen Zugriff auf maschinelle Funktionen und maschinell gespeicherte Informationen erhalten. Die Zugriffsberechtigung ist mitarbeiterbezogen und aufgabengerecht zu staffeln. Dabei soll sowohl die Lese- als auch die Schreibberechtigung restriktiv und zeitnah vergeben werden. Bei personenbezogenen Daten ist der Datenschutzbeauftragte an der Vergabe der Zugriffsberechtigungen zu beteiligen. Die vergebenen Zugriffsberechtigungen sollen maschinell bei jeder Zugriffsanforderung geprüft werden. Das maschinelle Identifizierungsverfahren für Mitarbeiter soll unberechtigte Zugriffe durch entsprechende Maßnahmen verhindern, z. B. Kennworte mit regelmäßigem, maschinell erzwungenem Wechsel mit vorgeschriebener Mindestlänge, verdeckte Eingabe, automatische Abmeldung bei Überschreitung einer bestimmten Zeit der Nicht-Aktivität. Die Mitarbeiter sind zu verpflichten, die Kennworte streng vertraulich zu behandeln. Die zu ergreifenden Maßnahmen bei dem Verdacht oder der Gewißheit des Bekanntwerdens (z. B. durch Beobachtung bei der Eingabe oder durch Bekanntgabe für Wartungszwecke) sind im voraus festzulegen. Zumindest sollte dazu das Kennwort gewechselt werden.

Kennworte sollen nur durch den jeweiligen Mitarbeiter änderbar sein. Die Stelle zur Vergabe der Zugriffsberechtigung soll keinen Einblick in die benutzten Kennworte haben und nur in der Lage sein, die Kennworte einzelner Mitarbeiter auf einen Ausgangswert zurückzusetzen, der vom Mitarbeiter unverzüglich, maschinell kontrolliert zu

ändern ist. Unberechtigte Zugriffsversuche sollen im Hinblick auf die spätere Nachvollziehbarkeit protokolliert werden.

Über eine Regelung zur Datensicherung ist sicherzustellen, daß alle im Rahmen der IT zu speichernden Daten durch zuverlässige Sicherungs- und Wiederherstellungsverfahren im Falle ihres Verlustes auf dem Verarbeitungsdaträger (Originaldatenträger) von einem oder mehreren Sicherungsdaträgern unmittelbar oder mittelbar rekonstruiert werden können (siehe Nr. 7.2.3). Daten im Sinne der Datensicherung sind dabei nicht nur die zu verarbeitenden Ein- und Ausgabedaten der Verfahren, sondern auch die maschinell gespeicherten Bestandteile der Verfahren, z. B. Programme, Abläufe und Dokumentation. Unter Verarbeitungsdaträgern sind die Massenspeicher – in der Regel Festplatten – zu verstehen, auf denen die Daten für den Betrieb gespeichert und zur Verarbeitung bereitgehalten werden. Sicherungsdaträger sind die Datenträger – in der Regel Magnetbänder, Magnetbandkassetten oder Disketten –, auf die die Verarbeitungsdaten (Originaldaten) kopiert wurden. Die Sicherungsdaträger dürfen nur für Rekonstruktionszwecke genutzt und keinesfalls unabhängig von den Verarbeitungsdaträgern verändert werden. Sie sind räumlich getrennt von den Verarbeitungsdaträgern katastrophensicher unter Berücksichtigung des Zugriffs- und Zutrittsschutzes zu lagern (siehe Nr. 7.2.5). Es sollen mehrere Generationen mit eindeutiger Identifizierbarkeit der Generationsfolge für die Rekonstruktion auf getrennten Sicherungsdaträgern gehalten werden. Auch die Generationen sind möglichst räumlich getrennt voneinander zu lagern. Bei der Lagerung sind die physikalischen Eigenschaften – insbesondere die mögliche Speicherdauer – der benutzten Datenträger zu berücksichtigen. Sicherungsverfahren dienen zur Übertragung von Daten von den Verarbeitungs- auf die Sicherungsdaträger, Wiederherstellungsverfahren der Übertragung von den Sicherungs- auf die Verarbeitungsdaträger. Die Datenübertragung zwischen Verarbeitungs- und Sicherungsdaträger darf nur mit Hilfe dieser festgelegten Verfahren erfolgen. Komplettsicherungen und Teilsicherungen – z. B. nur von geänderten Daten eines Tages – können zur Förderung der Wirtschaftlichkeit und Aufgabengerechtigkeit unter Beibehaltung der Sicherheit miteinander kombiniert werden. Die Auswirkungen des gewählten Sicherungsverfahrens auf das Wiederherstellungsverfahren und die Dauer der Rekonstruktion sind dabei zu beachten.

Die Datensicherung ist in der Verfahrensentwicklung konzeptionell zu berücksichtigen. Die zur Datensicherung vorhandenen Bestandteile des IT-Systems sollen in die Konzeption einbezogen werden, soweit sie die Sicherheitsanforderungen erfüllen. Die nicht vom System sicherzustellenden Datensicherungsfunktionen sind im Verfahren anderweitig zu realisieren (siehe auch 7.2). Im Rahmen des Verfahrensbetriebes sollen die Datensicherung und die Verwaltung der Datensicherungsträger möglichst automatisiert geschehen. Andernfalls sind sie zumindest organisatorisch zu regeln. Die Automatisierung soll auch die Rekonstruktion umfassen. Insbesondere soll die Auswahl der richtigen Generation zur Wiederherstellung maschinell unterstützt und kontrolliert werden. Die notwendigen manuellen Arbeitsabläufe zur Rekonstruktion sind detailliert zu beschreiben und regelmäßig vom zuständigen Personal zu üben. Jede durchgeführte Rekonstruktion ist zu protokollieren.

Über eine Regelung zur Weitergabe und Verwendung ist sicherzustellen, daß Herkunft, Änderung und Verbleib von wesentlichen Informationen mit Angabe von Termin und verantwortlichem Mitarbeiter vollständig nachvollzogen werden können. Dies gilt sowohl für die Verarbeitung im eigenen Hause als auch für den Datenaustausch. Insbesondere ist eine zeitnahe Auswertung im Hinblick auf Fehler und versuchten oder vollendeten Mißbrauch vorzusehen. Maßnahmen können z. B. sein:

- Nutzung von Datenträgerbegleitpapieren,
- Zutritts- und Abgangsprotokolle für Räume, in denen sich Hardware oder Datenträger befinden,
- Zugriffsprotokolle für Programme, Dateien und Datenbanken und
- Datenerfassungsprotokolle im Rahmen von Batch- und Dialogverfahren.

Maschinelle Aufzeichnungen, insbesondere Zugriffsprotokolle, können nur im Zusammenhang mit dem eindeutigen, nicht umgeharen Identifizierungsverfahren der Zugriffskontrolle und der Ankündigung einer entsprechenden Auswertung gegenüber den betroffenen Personen vor Beginn der Aufzeichnung Beweiskraft erlangen. Weitergabe- und Verwendungsnachweise sind als Bestandteil der Dokumentation des Verfahrensbetriebes – insbesondere bei kassenwirksamen Verfahren – im Rahmen der entsprechenden Fristen aufzubewahren.

Einen Sonderfall der Datenverwendung stellt die Datenvernichtung dar. Über eine Regelung zur Datenvernichtung ist die Aufrechterhaltung des Schutzes der Daten vor unberechtigter Kenntnisnahme bei nicht mehr benötigten Daten durch ihre Vernichtung bzw. unwiederherstellbare Löschung sicherzustellen. Die Regelung soll sich dabei sowohl auf ausgedruckte als auch auf gespeicherte Daten beziehen. Die Entsorgung von Listen, Formularen und anderen Druckerzeugnissen der IT – auch mikroverfilmten – in geschlossenen, vor unberechtigtem Zugang geschützten Behältern und ihre ordnungsgemäße Vernichtung ist zu gewährleisten. Daten, die nicht mehr benutzt werden, sind für den Zugriff zu sperren und nach dem Ablauf der Aufbewahrungsfristen unter Beachtung der Ordnungsmäßigkeit und Sicherheit unwiederherstellbar zu löschen. In der Regelung ist zu beschreiben, welche Daten betroffen und welche Aufbewahrungsfristen einzuhalten sind.

Bei Speichereinrichtungen, die zur Reparatur oder Entsorgung das Haus verlassen, sind die Daten unwiederherstellbar zu löschen oder die Datenträger zu vernichten. Ist ein Löschen oder Vernichten technisch nicht möglich, muß über geeignete organisatorische Maßnahmen sichergestellt werden, daß die Daten nicht in unberechtigten Zugriff gelangen.

Über eine Regelung zum Datentransport ist die Aufrechterhaltung des Schutzes der Daten vor unberechtigter Kenntnisnahme, vor Verfälschung und Verlust beim Transport mit Hilfe von beweglichen Datenträgern, z. B.

- Magnetbändern,
- Magnetbandkassetten,
- Disketten und
- Listen,



oder von Leitungen zwischen Geräten der Hardware im Netzwerk, z. B. Kabel im Hause, Kabel außer Haus oder Richtfunk, sicherzustellen. Datenträger – insbesondere unmittelbar lesbare Listen – sind bei entsprechenden Sicherheitsanforderungen auch innerhalb des Hauses in einem geschlossenen Behälter zu transportieren. Die folgenden Begleitinformationen sollen jedem Transport (bei Transport über Leitung entsprechend) beigelegt werden, z. B. in Form von Datenträgerbegleitpapieren:

- die Beschreibung der Datenträger, z. B. deren Aufzeichnungsformat, Code, Inhalt,
- die Angabe des Datenträgerlaufes mit Absender, Versandform, Transporteur, Empfänger und Soll-Terminen,
- die Empfangsbestätigung des Transporteurs mit Ist-Termin,
- die Empfangsbestätigung des Empfängers mit Ist-Termin sowie
- eventuelle Abstimmungen, z. B. Seiten- oder Datensatzanzahl, Prüf- oder Kontrollsummen.

Der Datenträgerlauf darf nicht eigenmächtig verändert werden. Die Datenträgerbegleitpapiere sollen zur Kontrolle an den Absender zurückgesandt werden. Werden Datenträger zurückgesandt, deren Inhalt nicht mehr benötigt wird, sollen diese zuvor unwiederherstellbar gelöscht werden. Ggf. sind Leitungen und Geräte gegen unberechtigte Abhörangriffe mit oder ohne direkten Kontakt zur Leitung oder zum Gerät – z. B. durch Auswertung der entstehenden elektromagnetischen Felder – abzuschirmen. Bei vertraulichen oder gegen Verfälschung empfindlichen Daten ist vor dem Transport eine Verschlüsselung vorzusehen. Der Verschlüsselungscode muß ebenfalls vertraulich sein und soll nur dem Absender und dem Empfänger, nicht aber einem eventuellen Transporteur bekannt sein. Verfälschungen an transportierten Daten sollen über geeignete Kontrollen erkannt werden können. Daten dürfen nur an zum Zugriff befugte Empfänger geliefert werden.

Beim Transport über Wählleitungen soll der Empfänger grundsätzlich die Verbindung aufbauen und die Übertragung aktiv kontrollieren. Es ist sicherzustellen, daß die transportierten Daten vom Absender zumindest bis zur Bestätigung des fehlerfreien Empfangs wiederhergestellt und erneut versandt werden können, um das Verlustrisiko der Daten zu minimieren.

## 7.4 Notfallplanung und Notorganisation

7.4.1 *Die im Falle langandauernder Störung des Verfahrensbetriebes und des Verlustes der Daten zu ergreifenden Maßnahmen sind entsprechend der Bedeutung der Verfahren in einem Notfallplan festzulegen. Eine Notorganisation soll sicherstellen, daß die wesentlichen Verfahren einschließlich der Daten nach angemessen kurzer Zeit zuverlässig wieder zur Verfügung stehen.*

7.4.2 *Die Wirksamkeit der Notfallmaßnahmen ist in regelmäßigen Abständen zu überprüfen. Die Notfallplanung ist fortzuentwickeln und dem Stand der Technik anzupassen.*

Die Notorganisation soll als Teil des Sicherheitskonzeptes im Falle einer Katastrophe sicherstellen, daß die wesentlichen Verfahren der Verwaltung nach angemessener Zeit entsprechend den fachlichen Anforderungen – in der Regel zwischen wenigen Stunden und wenigen Tagen – zuverlässig wieder zur Verfügung stehen. Eine Katastrophe kann entstehen durch die Zerstörung oder die langandauernde Störung der Hardware oder der Software im Zusammenhang mit

- äußerer Gewalteinwirkung, z. B. Feuer, Wasser, Explosion,
- technischem oder menschlichem Versagen oder
- Sabotage.

Wesentliche Verfahren im Sinne der Notfallorganisation sind solche, deren langzeitiger Ausfall aus Gründen der Ordnungsmäßigkeit, Sicherheit oder Wirtschaftlichkeit nicht vertretbar ist. In diesem Sinne nicht wesentliche Verfahren sollen grundsätzlich nicht in die Notorganisation einbezogen werden. Die Kosten der Notorganisation sind in die Wirtschaftlichkeitsbetrachtungen einzubeziehen.

Die im Falle einer Katastrophe zu ergreifenden Maßnahmen sind im Rahmen einer Notfallplanung festzulegen. Die Notfallplanung muß sich an der Wahrscheinlichkeit für den Eintritt einer Katastrophe, an dem möglichen Schaden durch eine Katastrophe und ihrer Ursachen orientieren. Sie muß mit der baulichen Sicherung der Ressourcen abgestimmt werden, die Katastrophen verhindern oder ihren Schaden begrenzen soll. Die in der Notfallplanung zu berücksichtigenden wesentlichen Verfahren sind in Abstimmung mit den Fachbereichen festzulegen. Dabei ist auch zu ermitteln, ob mit ergänzenden organisatorischen Maßnahmen ein längerer Verzicht der Fachbereiche auf die IT-Verfahren möglich ist. In diesem Zusammenhang ist auch die Reihenfolge der Bereitstellung der Verfahren nach einer Katastrophe abzustimmen. Für jedes Verfahren ist der Wiederanlauf, insbesondere im Hinblick auf den Datenzustand, detailliert zu beschreiben. Die Datensicherung muß die Erfordernisse dieses Wiederanlaufes in Bezug auf Aktualität, Vollständigkeit und Funktionsfähigkeit durch entsprechend häufige Sicherungen bzw. eine geeignete Sicherungstechnik (siehe Nr. 7.2.3) und die katastrophensichere Lagerung der Datensicherungsträger (siehe Nr. 7.2.5) – z. B. in einem feuerfesten Tresor oder einem separaten Gebäude – gewährleisten. Die Wiederherstellung von Daten, die sich nicht maschinell aus Sicherungen ableiten lassen, ist soweit erforderlich durch geeignete Maßnahmen – z. B. die Protokollierung von Eingaben oder die Aufbewahrung

von Eingabebelegen – sicherzustellen. Wenn nötig muß auch die Datenerfassung für den Zeitraum zwischen Eintritt der Katastrophe und dem erfolgreich beendeten Wiederanlauf mit der Übernahme der Daten in das Verfahren in die Planung einbezogen werden. Voraussetzung für die Notorganisation ist die schnelle Bereitstellung von mit der System- und Verfahrenssoftware verträglicher Ersatzhardware, z. B. durch

- Vorhalten eigener, räumlich getrennter, im täglichen Betrieb nicht vollständig ausgelasteter Hardware mit der Möglichkeit, die freien Kapazitäten für eine Optimierung einzusetzen,
- gegenseitige Hilfestellung verschiedener Stellen oder
- ggf. Beauftragung eines auf Notorganisation spezialisierten Serviceunternehmens.

Zusätzlich ist für Netzwerkkapazität, z. B. Standleitungen zum Ersatzrechenzentrum, und die benötigte Infrastruktur, z. B. Transportkapazitäten für Personal und Datenträger, vorzusorgen. Eine Abstimmung mit externen Stellen – z. B. der Deutsche Bundespost oder der Feuerwehr – kann erforderlich sein. Für die geplante Ersatzhardware ist die Produktionsumgebung mit entsprechend konfigurierter System- und Verfahrenssoftware und den Abläufen (Jobs) für die wesentlichen Verfahren ständig auf Datensicherungsträgern katastrophengeschützt bereitzuhalten. Insbesondere bei Änderungen der Produktionsumgebung ist die entsprechende Sicherung zu berücksichtigen (Nr. 3.5.3).

Die Notfallplanung muß schließlich die organisatorischen Maßnahmen in einem Katastrophenfall beschreiben.

Die Notfallplanung ist durch Notfallübungen auf Funktionsfähigkeit zu prüfen. Es kann empfehlenswert sein, die Übung oder Teilmaßnahmen davon unregelmäßig und unangekündigt durchzuführen. Schwachstellen sind unverzüglich zu beheben. Die Fachbereiche müssen beurteilen, ob sie mit der zeitlichen, qualitativen und quantitativen Wiederherstellung der Produktion in einer wirklichen Katastrophe ihre Aufgaben ordnungsgemäß fortführen könnten.

Die im Falle einer Katastrophe zu ergreifenden Maßnahmen sind im voraus detailliert in einem Notfallplan zu dokumentieren, der für den Notfall sicher aufzubewahren ist. Der Notfallplan umfaßt z. B.:

- den Alarmierungsplan für die in jedem Fall betroffenen Stellen,
- die Regelung der Zuständigkeiten und Vollmachten mit Benennung der entsprechenden Personen und ihrer Stellvertreter,
- das Verzeichnis der möglicherweise zusätzlich betroffenen Stellen, Lieferanten und Serviceunternehmen mit Nennung der Ansprechpartner,
- ggf. die Regelung zur Aufrechterhaltung eines manuellen Notbetriebes,
- die Vorgehensweise zur Beschaffung und Installation der Ersatzhardware,
- die Vorgehensweise zur Übertragung der Produktionsumgebung auf die Ersatzhardware,
- die Reihenfolge des Wiederanlaufes der wesentlichen Verfahren und
- je Verfahren die Vorgehensweise für den Wiederanlauf unter besonderer Beachtung der Wiederherstellung eines gültigen Datenbestandes.

Bei allen Angaben sind Adressen und Telefonnummern, auch private, für einen reibungslosen Kommunikationsaufbau anzugeben und aktuell zu halten.

Der Notfallplan soll im Falle einer Katastrophe eine konkrete Arbeitsanweisung für das betroffene Personal darstellen. Die ordnungsgemäße Ausführung des Notfallplanes ist im Produktionsnachweis zu dokumentieren.

## Verarbeitungsarten in der IT

Im Zuge der Entwicklung der Datenverarbeitung haben sich drei typische Verarbeitungsarten herausgebildet:

Stapelverarbeitung (Batch),  
Dialogverarbeitung und  
Prozeßdatenverarbeitung,

deren Merkmale im folgenden erläutert sind. Zu beachten bleibt, daß bei einzelnen IT-Verfahren diese Verarbeitungsarten nebeneinander auftreten können und sich nicht gegenseitig ausschließen.

### 1 Stapelverarbeitung (Batch)

In der Regel sind bei der Stapelverarbeitung folgende Merkmale vorzufinden:

- die Eingabe erfolgt über eine separate Datenerfassung für mehrere gleichartige Vorgänge,
- mehrere gleichartige Vorgänge werden in einem Programmlauf verarbeitet,
- für mehrere gleichartige Vorgänge werden die Daten über Listen, sonstige Druckbelege und maschinenlesbare Datenträger, z. B. Magnetbänder, Disketten, ausgegeben,
- die Zeitspanne zwischen der Dateneingabe und der Datenverarbeitung mit Datenausgabe liegt in der Größenordnung von Stunden oder Tagen,
- der Benutzer kann die Verarbeitungsschritte, die im voraus festgelegt sind, nicht beeinflussen.

Die Stapelverarbeitung wird typischerweise eingesetzt, wenn

- eine große Anzahl von gleichartigen Vorgänge zu bearbeiten sind,
- die Erfordernisse an die Aktualität der Datenbestände nicht beeinträchtigt werden,
- die Datenausgabe erst zu einem festgelegten Termin am Ende eines Dateneingabezeitraums, z. B. am Monatsende, vorliegen soll,
- die Dateneingabe mit Hilfe von z. B. Formularen oder maschinell lesbaren Datenträgern, mit wenigen Fehlern und ohne die Notwendigkeit anschließender manueller Korrekturen erfolgen kann.

### 2 Dialogverarbeitung

Die Dialogverarbeitung ist in der Regel durch folgende Merkmale gekennzeichnet:

- die Eingabe erfolgt über Bildschirmarbeitsplätze im Fachbereich jeweils für einen zu bearbeitenden Vorgang,
- die Verarbeitung eines Vorgangs geschieht in einem Verarbeitungsschritt, wobei mehrere Dialogschritte, z. B. die Ausgabe an den Benutzer oder Eingaben des Benutzers, für einen Verarbeitungsschritt notwendig sein können,
- die Ausgabe erfolgt über Bildschirmarbeitsplätze und Drucker im Fachbereich je Vorgang,
- die Verarbeitungszeit beträgt typischerweise zwischen Sekunden und Minuten,
- der Benutzer hat Einwirkungsmöglichkeiten auf den Ablauf der Verarbeitung und die einzelnen Dialogschritte, z. B. über Auswahlmenüs und Funktionstasten.

Die Dialogverarbeitung wird überwiegend eingesetzt, wenn

- ein einzelvorgangsbezogener Arbeitsablauf angestrebt wird,
- die Datenbestände, z. B. für Auskunftszwecke, ständig aktuell sein sollen,
- die Datenverarbeitungsergebnisse zeitnah vorliegen sollen,
- die Dateneingabe umfangreichen maschinellen Kontrollen mit anschließenden manuellen Korrekturen unterzogen wird,
- der Benutzer durch die Funktionen des IT-Systems beim Arbeitsablauf geführt und direkt unterstützt werden soll,
- der Benutzer die Möglichkeit haben soll, den Arbeitsablauf während der Bearbeitung zu beeinflussen.

### 3 Prozeßdatenverarbeitung

Hierbei sind typischerweise folgende Merkmale anzutreffen:

- die Prozeßdatenverarbeitung dient der maschinellen Steuerung und Überwachung von technischen Prozessen,
- die Daten – in diesem Fall mit Informationen über Ereignisse des zu steuernden Prozesses – werden über Sensoren eingegeben,
- die Datenverarbeitung geschieht in einem Verarbeitungsschritt,
- die Datenausgabe führt zur Einwirkung auf Stell- und Regeleinrichtungen für Kenngrößen des Prozesses,
- die Verarbeitung geschieht in Sekundenbruchteilen,
- die Verarbeitung wird durch Ereignisse im Prozeß beeinflusst.

Die Prozeßverarbeitung wird eingesetzt, wenn technische Prozesse maschinell zu steuern und zu überwachen sind.

## IT-Funktionen und ihre Aufgaben

Typischerweise ist folgende Aufgabenverteilung vorzufinden:

Verfahrensentwicklung,  
Verfahrensbetrieb,  
Beratung, Schulung und Koordination,  
Datenorganisation,  
Systemtechnik,  
Administration,  
Sicherheit und Datenschutz.

### 1 Verfahrensentwicklung

mit der Zuständigkeit für

- **Entwicklung und Pflege von Verfahren:**
  - o Entwicklung neuer Verfahren
  - o Weiterentwicklung bestehender Verfahren durch wesentliche fachliche Änderung dieser Verfahren
  - o Pflege bestehender Verfahren durch Beseitigung von Fehlern und Optimierung ohne wesentliche fachliche Änderung dieser Verfahren
- **Methoden und Werkzeuge zur Entwicklung und Pflege von IT-Verfahren:**
  - o Auswahl, Vorbereitung, Einführung und Pflege von Methoden und Werkzeugen
  - o Entwicklung und Fortschreibung von Regelungen
  - o Gestaltung der Projektorganisation
  - o Beratung und Schulung des an der Verfahrensentwicklung beteiligten Personals aus allen Bereichen – z. B. dem Teilbereich zentrale Verfahrensentwicklung oder dem Fachbereich – in den Fragen der Verfahrenstechnik
- **Qualitätssicherung:**
  - o formale Kontrolle der Einhaltung von Regelungen
  - o inhaltliche Kontrolle der Ergebnisse.

Die **Entwicklungsverantwortung** soll dabei insbesondere umfassen:

- die Ableitung der technischen Anforderungen an Verfahren aus den fachlichen Vorgaben,

- die vollständige und richtige Umsetzung der fachlichen Anforderungen in Verfahren – insbesondere in Verfahrenssoftware, Datenstrukturen sowie maschinelle und manuelle Abläufe,
- die Beseitigung von Fehlern in den Verfahren und
- die technische Unterstützung bei der Freigabe der Verfahren im Rahmen der Fachverantwortung.

Die Verfahrensentwicklung soll bei zentral betriebenen Verfahren organisatorisch als abgegrenzter Teilbereich im Bereich IT angesiedelt sein. Eine hierarchische Unterordnung der Verfahrensentwicklung unter den Verfahrensbetrieb ist in der Regel ungünstig.

Bei dezentral betriebenen Verfahren kann die Verfahrensentwicklung organisatorisch entweder dezentral dem für den Betrieb verantwortlichen Fachbereich oder, wie oben beschrieben, zentral dem Bereich IT zugeordnet werden. Grundsätzlich soll die Verfahrensentwicklung auch bei dezentral betriebenen Verfahren zentral zugeordnet werden, wenn

- das Verfahren mehrfach dezentral betrieben wird,
- das Verfahren einen (für den Fachbereich zu) hohen informationstechnischen Schwierigkeitsgrad aufweist,
- erhöhte Anforderungen an den Schutz der Daten vor unberechtigter Kenntnisnahme, Verfälschung und Verlust zu stellen sind,
- erhöhte Anforderungen an die Funktionssicherheit des Verfahrens zu stellen sind oder
- Ergebnisse des dezentralen Verfahrens zur Fortschreibung zentraler Datenbestände genutzt werden.

Ist keine der oben genannten Voraussetzungen erfüllt, ist bei dezentral betriebenen Verfahren die Zuordnung der Verfahrensentwicklung zu dem das Verfahren betreibenden Fachbereich empfehlenswert, um die zentrale Verfahrensentwicklung zu entlasten.

Die Gliederung der Stellen bei der Verfahrensentwicklung soll verfahrensorientiert vorgenommen werden. Die Ausnahme hiervon bilden nebengeordnete allgemeine Dienstleistungs- und Kontrollfunktionen; bei diesen sollen die Stellen funktionsorientiert gegliedert sein.

## 2 Verfahrensbetrieb

mit der Zuständigkeit für

- **Datenerfassung** (für Stapelverarbeitung):
  - o Verarbeitungsgerechte, vollständige und richtige Erfassung der auf Erfassungsbelegen vom Fachbereich vorgegebenen Daten
  - o Bereitstellung der erfaßten Daten
- **Produktionsvorbereitung:**
  - o Auftragsentwurf (Job Design)



- o Auftragsstrom-Zusammenstellung
- o Zusammenstellung von Auftragsnetzen
- o Reservieren von Betriebsressourcen
- o Freigabe nicht mehr benötigter Betriebsressourcen
- **Produktionssteuerung:**
  - o Konsol-Bedienung
  - o Peripherie-Bedienung
  - o Wiederherstellung und Wiederanlauf
  - o Produktionsnachbereitung
- **Datenträgerverwaltung/Archiv:**
  - o Bereitstellung, Versand und Entgegennahme von Datenträgern
  - o Verwaltung der Datenträger
  - o Archivierung der Datenträger
- **Datensicherung:**
  - o Sicherung der Datenbestände
  - o Bereitstellung von Sicherungsbeständen für Notfälle
- **Produktionsüberwachung:**
  - o Abnahme/Übernahme von Verfahrens- und Systemsoftware
  - o Terminüberwachung
  - o Feststellung und Beseitigung von Störungen
  - o Durchsatzkontrolle und -optimierung
  - o Qualitätskontrolle/Endkontrolle der Produktionsergebnisse
  - o Netzwerküberwachung

### 3 Beratung, Schulung und Koordination

(kann organisatorisch eingeordnet sein in Verfahrensentwicklung oder Verfahrensbetrieb)

### 4 Datenorganisation

mit der Zuständigkeit für:

- Konzeption und Abstimmung der verfahrensbezogenen und verfahrenübergreifenden Datenstrukturen (insoweit Mitarbeit bei der Verfahrensentwicklung)
- Vorbereitung, Einführung und Pflege der Datenstrukturen (insoweit Mitarbeit beim Verfahrensbetrieb)
- Konzeption der Datensicherung und -wiederherstellung
- Beratung und Schulung in Fragen der Datenorganisation

(Erster Punkt der Strichaufzählung kann organisatorisch eingeordnet sein in Verfahrensentwicklung, zweiter in Verfahrensbetrieb, dritter und vierter in Verfahrensentwicklung oder -betrieb)

## 5 Systemtechnik

mit der Zuständigkeit für:

- Vorbereitung, Einführung und Pflege der Hardware und Systemsoftware
- Beratung und Schulung in Fragen der Systemtechnik (kann eingeordnet sein in Verfahrensbetrieb)

## 6 Administration

mit der Zuständigkeit für:

- mittel- und langfristige Planung
- Beschaffung der Ressourcen
- Verwaltung
- Leistungsverrechnung

(erster und zweiter Strich können für den jeweiligen Anteil auf Verfahrensentwicklung und -betrieb aufgeteilt werden, dritter und vierter kann in Verfahrensbetrieb eingeordnet werden)

## 7 Sicherheit und Datenschutz

mit der Zuständigkeit für:

- Mitarbeit, Koordination und Qualitätssicherung bei Risikoanalysen und der Erstellung von Sicherheitskonzepten
- Ständige und zeitnahe Kontrolle der Maßnahmen zur Gewährleistung der Vertraulichkeit, Verfügbarkeit und Integrität der Daten, Verfahren und Ressourcen der IT
- Gewährleistung der Beachtung des Datenschutzgesetzes bei der Verarbeitung personenbezogener Daten

## Methoden und Werkzeuge

- 1 Allgemeine Werkzeuge bei IT-Vorhaben
- 2 Systementwurf und Programmierung
  - 2.1 Entwurfsmethoden
  - 2.2 Werkzeuge für den fachlichen und technischen Entwurf
  - 2.3 Werkzeuge für die Programmierung
- 3 Test und Abnahme
  - 3.1 Methoden für den Test
  - 3.2 Werkzeuge zur Testunterstützung

### 1 Allgemeine Werkzeuge bei IT-Vorhaben

Zu den allgemeinen Werkzeugen bei IT-Vorhaben zählen z. B.:

- ein Werkzeug zur maschinellen Abbildung und Anwendung des Vorgehensmodells (Vorgehensmodell-Treiber):

Dieses Werkzeug soll die Bearbeitung aller Tätigkeiten und Ergebnisse des Vorgehensmodells über alle Projektabschnitte im Dialog unterstützen, sämtliche übrigen Werkzeuge unter seiner Benutzeroberfläche zusammenfassen und alle im Projektverlauf entstehenden Ergebnisse verwalten.
- ein Konfigurationsmanagementsystem:

Ein Konfigurationsmanagementsystem zur Verwaltung von Programmen, Prozeduren und Datenelementen soll

  - o die Trennung von Verfahrensentwicklung und -produktion sicherstellen,
  - o den Übergang von Verfahrensteilen aus der Verfahrensentwicklung in die Produktion technisch sichern, kontrollieren und protokollieren,
  - o verschiedene Entwicklungszustände bei der Verfahrensentwicklung – z. B. geplant, in Arbeit, fertiggestellt, getestet, abgenommen – verwalten,
  - o verschiedene Versionen im Verfahrensbetrieb verwalten, die Zugehörigkeit zu einzelnen Verfahren dokumentieren,
  - o Zugriffsberechtigungen berücksichtigen und
  - o Langbezeichnungen zu den technischen Kurzbezeichnungen der Verfahrensteile verwalten.
- ein leistungsfähiger, bildschirmorientierter Texteditor
- ein Werkzeug zur Textaufbereitung:

Ein Werkzeug zur Textaufbereitung soll die Möglichkeiten bieten

- o Textbausteine aus einzelnen Ergebnissen zu einem Bericht zusammenzustellen,
- o vordefinierte Kopf- und Fußzeilen sowie Seitenformate zu verwenden,
- o die Seiten maschinell zu numerieren sowie
- o Inhalts-, Abbildungs- und Stichwortverzeichnisse maschinell zu generieren.

## 2 Systementwurf und Programmierung

### 2.1 Entwurfsmethoden

Methoden für den Entwurf sollen

- die Funktionen und den Informationsfluß des zukünftigen Verfahrens unter Beteiligung der Fachbereiche in einem fachlichen Modell zusammenführen und
- aus dem fachlichen ein technisches Modell mit der Zuordnung von Funktionen zu Programmen oder Modulen und Informationen zu Dateien, Datenbanken, Bildschirmmasken, Listen usw. ableiten.

Ein methodisches Vorgehen beim fachlichen Entwurf soll

- die Verständlichkeit, Vollständigkeit, Widerspruchsfreiheit und Wiederholungsfreiheit des fachlichen Modells sicherstellen,
- Berührungspunkte zu anderen Verfahren aufzeigen und
- eine Grundlage schaffen für den technischen Entwurf.

Die Methoden für den technischen Entwurf sollen sicherstellen, daß alle Funktionen, Informationen und Beziehungen des fachlichen Modells vollständig in das technische Modell übernommen werden. Ein methodisches Vorgehen beim technischen Entwurf soll zusätzlich

- die Bewertung und Verbesserung des technischen Verhaltens ohne fachliche Änderung erlauben,
- die Grundlagen für die Software-Qualitätsmerkmale, wie Aufgabengerechtigkeit, Stabilität, Kapazität, Änderbarkeit, Erweiterbarkeit und Übertragbarkeit legen,
- die Voraussetzungen für die Anwendung strukturierter Methoden der Softwareentwicklung schaffen und
- die Wiederverwendbarkeit von Modulen begünstigen.

Grundsätzlich geeignet sind alle Methoden oder Methodenkombinationen, welche

- die Gliederung der Funktionen und ihre wiederholungs- und widerspruchsfreie Darstellung,
- die Gliederung der Informationen und ihre wiederholungs- und widerspruchsfreie Zusammenfassung zu Objekten und
- die Verknüpfung von Funktionen und Informationen (Ein-/Ausgabebeziehungen)

unterstützen. Es ist empfehlenswert, eine zentrale Stelle zu beteiligen, die die Abstimmung mit anderen Projekten in diesem Zusammenhang sicherstellt (siehe auch Nr. 3.1 und Nr. 2.2 der IT-Prüfungshinweise).

## 2.2 Werkzeuge für den fachlichen und technischen Entwurf

Als Werkzeuge für den fachlichen und technischen Entwurf können z. B. eingesetzt werden:

- Data Dictionary (Datenwörterbuch), eventuell mit angeschlossenem Grafiksystem:  
Ein Data Dictionary soll die Eigenschaften von Funktionen und Informationen des fachlichen und des technischen Entwurfs, insbesondere Programme, Module, Dateien, Datenbanken, Bildschirmmasken, Listen, Datenfelder, und deren Beziehungen untereinander verwalten. Diese Beziehungen sollen mit Hilfe eines angeschlossenen Grafiksystems dargestellt werden können.
- Datenmodellierungswerkzeug:  
Ein Datenmodellierungswerkzeug soll den Entwurf der Datenstrukturen unterstützen und die Grundlagen für den Aufbau der Dateien und Datenbanken liefern.
- Pseudocode-Generator:  
Ein Pseudocode-Generator soll Strukturelemente zur eindeutigen, genauen Beschreibung von Abläufen zur Verfügung stellen und die Einhaltung der Strukturregeln prüfen. So können Programme und Module mit Hilfe des Pseudocode-Generators beschrieben werden.
- Entscheidungstabellen-Generator:  
Eine Entscheidungstabelle verknüpft Bedingungen und daraus abzuleitende Aktionen. Ein Entscheidungstabellen-Generator erleichtert das Erstellen von Entscheidungstabellen und deren Prüfung auf Vollständigkeit, Widerspruchsfreiheit und Wiederholungsfreiheit. Mit Entscheidungstabellen lassen sich z. B. Programmfunktionen beschreiben.
- Listen- und Bildschirmmasken-Generator:  
Ein Listen- und Bildschirmmasken-Generator erlaubt die Gestaltung der Benutzeroberfläche eines Verfahrens im Dialog. Dabei können Listen und Bildschirmmasken auch in ihrer logischen Folge frühzeitig in der Form dargestellt werden, wie sie sich später im Verfahren wiederfinden werden (Prototyping). Die so festgelegten Formate stehen für die Programmierung ohne zusätzlichen Aufwand zur Verfügung.  
Beim fachlichen Entwurf kann ein grober Entwurf der Formate im Zuge des Prototyping vorgenommen werden.  
Beim technischen Entwurf können mit Hilfe des Listen- und Bildschirmmasken-Generators detailliert die entsprechenden Formate festgelegt werden.
- Generator für die Verfahrensarchitektur:  
Ein Generator für die Verfahrensarchitektur kann aufbauend auf den strukturierten Beschreibungen über den Aufbau von Listen und Bildschirmmasken und der

vorgegebenen Reihenfolge der Funktionen ein Gerüst für das Programmsystem eines Verfahrens mit Einstiegspunkten, z. B. für Ein-/Ausgabevorgänge oder die Verarbeitung einzelner Funktionen, erzeugen.

- Generator für Programmrahmen:

Ein Programmrahmen-Generator kann für einzelne Programmtypen – z. B. Dialogprogramm mit und ohne Benutzerdialog, Batch-Programm – die Steuerungslogik erzeugen.

Die **Dokumentation des fachlichen Entwurfes** eines Verfahrens kann über die in Nr. 3.3.4 der IT-Prüfungshinweise genannten Elemente hinaus je nach den eingesetzten Werkzeugen enthalten:

- eine grafische Darstellung des Informationsflusses mit der Verknüpfung von benötigten und erzeugten Informationen mit den durchzuführenden Funktionen
- Ein-/Ausgabebeziehungen für jede einzelne Funktion und das gesamte Verfahren
- Reihenfolge der Funktionen
- Beschreibung der fachlichen Informationen
  - o Herkunft
  - o gültige Werte
  - o Abhängigkeiten
  - o Schlüsselverzeichnisse
  - o Zugriffsberechtigungen
  - o Aufbewahrungsfristen
  - o ggf. Verweis auf verfahrenübergreifende Dokumentation
- Beschreibung der fachlichen Funktionen
  - o Verarbeitungsregeln
  - o Rechenformeln
  - o automatisch erzeugte Verarbeitungsschritte
  - o technische und organisatorische Kontrollen und Abstimmungen
  - o Zugriffsberechtigungen
  - o Behandlung fachlicher Fehler mit Angabe der Fehlermeldungen und der erforderlichen Maßnahmen
  - o eventuell Verweis auf verfahrenübergreifende Dokumentation
  - o Aufstellung der fachlichen Mengengerüste und
  - o Anleitung zur fallweisen Prüfung des Verfahrens.

Die **Dokumentation des technischen Entwurfes** kann über die in Nr. 3.3.4 der IT-Prüfungshinweise genannten Elemente hinaus je nach den eingesetzten Werkzeugen enthalten:

- Beschreibung der Dateien und Datenbanken bis auf Datenfeldebene
  - o Aufbau der Dateien und Datenbanken (Datensatzstruktur bis auf Datenfeldebene und Organisationsform)
  - o Zuordnung der fachlichen Informationen zu Datenfeldern

- o Ergänzung der fachlichen Beschreibung der Informationen mit technischen Angaben
- o Angaben zum Schutz der Daten
- o Angaben zur Archivierung und zu den Aufbewahrungsfristen
- Verzeichnis der Programme und Module
  - o Zuordnung der fachlichen Funktionen zu Programmen bzw. Modulen mit Verweis auf die entsprechende Dokumentation
- Beschreibung der Bildschirmmasken, Listen und sonstigen Formulare
  - o Zuordnung von Datenfeldern
  - o Anweisungen zum Ausfüllen und zur Weiterverarbeitung und -verteilung
- Darstellung des detaillierten Ablauf- und Datenflußplanes
- Aufstellung der technischen Mengengerüste
- Darstellung der Einbindung in das technische Umfeld und der technischen Berührungspunkte zu anderen Verfahren
- Beschreibung der Überleitung in andere technische Umgebungen.

## 2.3 Werkzeuge für die Programmierung

Werkzeuge für die Programmierung sind z. B.

- Übersetzungsprogramme (Assembler, Compiler) für Quelltexte einer bestimmten Programmiersprache (COBOL, PL/1, C usw.)
- Programmgeneratoren
 

Programmgeneratoren sollen aus strukturierten Vorgaben, z. B. Pseudocode, Entscheidungstabellen, Listen- oder Bildschirmmaskenformaten, möglichst vollständig, ggf. zu ergänzenden Quelltext einer bestimmten Programmiersprache erzeugen.
- VHLL (Very High Level Languages): VHLL sind Programmiersprachen mit leistungsfähigen integrierten Befehlen zur Datenabfrage, Datenänderung, Dialogsteuerung und Berichterstellung.
 

Sie können zu einer erheblichen Steigerung der Produktivität in der Programmierung führen. Bei ihrem Einsatz sind mögliche Auswirkungen auf das Durchsatzverhalten und die Systembelastung der mit VHLL entwickelten Verfahren zu berücksichtigen. Die Anforderungen zur Verfahrensentwicklung sind auch bei Anwendung von VHLL uneingeschränkt zu beachten.

## 3 Test und Abnahme

### 3.1 Methoden für den Test

Methoden für den Test sind z.B.

- Schrittweise Zusammenführung der einzelnen Verfahrensbestandteile vom Feinen zum Groben mit Test bei jedem Schritt (inkrementelle Modulintegration, Bottom-Up),
- Test mit Betrachtung des inneren Aufbaus und Ablaufes einzelner Verfahrensbestandteile (White-Box-Test),
- Test ohne Betrachtung des inneren Aufbaus und Ablaufes einzelner Verfahrensbestandteile (Black-Box-Test),
- Test mit Betrachtung der erfahrungsgemäß meist genutzten Daten- und Funktionskombinationen (Normalpfad-Test),
- Test mit Betrachtung fehlerhafter Daten- und Funktionskombinationen und deren korrekter Behandlung (Fehlerpfad-Test),
- Test mit Betrachtung erfahrungsgemäß in Entwurf und Ausführung fehleranfälliger Daten- und Funktionskombinationen (Fehlererwartungs-Test),
- Bildung von Klassen fachlich gleich- oder ähnlichbedeutender Wertebereiche der Daten mit Test von Daten aus der Mitte und vom Rand dieser Klassen und der Annahme der Allgemeingültigkeit des Testergebnisses (Äquivalenzklassen-Test mit Grenzwertanalyse),
- Testdeckungsgrad-Ermittlung mit dem Nachweis der hinreichenden Vollständigkeit der Testfälle in Bezug auf den fachlichen und technischen Funktionsumfang des Verfahrens.

### 3.2 Werkzeuge zur Testunterstützung

Werkzeuge zur Testunterstützung können z. B. sein:

- Werkzeug zur Programmaufbau-Untersuchung (statische Analyse)
 

Ein Werkzeug zur Untersuchung des Programmaufbaus soll ohne die Ausführung oder die Nachbildung der Ausführung des Programms mögliche formale Fehler finden. Fehlerarten, die auf diese Weise gefunden werden können, sind

  - o Benutzung eines Datenfeldes, das noch nicht mit einem Wert belegt ist,
  - o Nichtbenutzung von Datenfeldern,
  - o Nichtbenutzung von Programmteilen,
  - o formal widersprüchliche Beschreibung von Übergabebereichen zwischen Programmteilen.
- Werkzeug zur Programmablauf-Untersuchung (dynamische Analyse)
 

Ein Werkzeug zur Untersuchung des Programmablaufes soll bei der Ausführung oder der Nachbildung der Ausführung eines Programms mögliche Fehler finden bzw. den Testenden durch die Gewährung des Einblickes in den Ablaufpfad der dabei ausgeführten Anweisungen und die benutzten Daten des Programms bei der Fehlersuche unterstützen. Zusätzlich soll es die Aufrufumgebung für ein zu testendes Modul nachbilden können und Unterstützung bei der Ermittlung des Testdeckungsgrades durch Zählung der Häufigkeiten einzelner Ablaufpfade bieten.



Es ist sicherzustellen, daß beim Einsatz eines solchen Werkzeuges die geordnete Vorgehensweise zur Fehlerbehebung eingehalten und nicht durch die Methode "Versuch und Irrtum" ersetzt wird.

- Testdaten-Generator  
Ein Testdaten-Generator soll bei der Erstellung und Verwaltung von möglichst wiederverwendbaren, den fachlichen und technischen Funktionsumfang des Verfahrens vollständig abdeckenden Testfällen Unterstützung bieten.
- Hauptspeicherauszug-Lesehilfen (Dump-Lesehilfen).

## Hinweise zu Wirtschaftlichkeitsbetrachtungen

- 1 Vorschriften und Regelungen
- 2 Aufstellen von Wirtschaftlichkeitsbetrachtungen
- 3 Berechnungsmethoden
- 4 Kostenarten und Kostensätze
- 5 Berücksichtigung von Preisänderungen und Unsicherheiten
- 6 Nutzwertanalysen, Nutzen-Kosten-Analysen

### 1 Vorschriften und Regelungen

Im Bundesbereich gibt es einige für alle Ressorts geltende Regelungen für die Durchführung von Wirtschaftlichkeitsbetrachtungen, so in den vorläufigen Verwaltungsvorschriften zu § 7 BHO, im Handbuch für Organisationsplanung und in den Empfehlungen der KBSt.

#### 1.1 Bundshaushaltsordnung

Das Gebot zur Wirtschaftlichkeit und Sparsamkeit bei Aufstellung und Ausführung des Haushaltsplans ergibt sich aus § 7 BHO. Die vorläufigen Verwaltungsvorschriften zur BHO (Vorl. VV-BHO) unterscheiden zwei Arten von Wirtschaftlichkeitsbetrachtungen:

- Zur Ausgestaltung des Grundsatzes der Wirtschaftlichkeit und Sparsamkeit (§7 Absatz 1 BHO) verlangen die Vorl. VV-BHO grundsätzlich (Nr. 1.2 zu § 7) für alle Vorhaben die Untersuchung
  - der Ziele,
  - der alternativen Lösungsmöglichkeiten,
  - der Kosten einschließlich der Folgekosten,
  - des Nutzens,und dabei insbesondere
  - der Auswirkungen auf den Haushalt des Bundes
  - der Dringlichkeit und
  - des Zeitplans der Verwirklichung.
- Darüber hinaus werden in Absatz 2 des § 7 BHO für geeignete Maßnahmen von erheblicher finanzieller Bedeutung (gesamtwirtschaftliche) Nutzen-Kosten-Untersuchungen gefordert. Hierfür enthalten die Vorl. VV-BHO ausführliche Erläuterungen zu einem 11-stufigen Verfahrensmuster einer Nutzen-Kosten-Untersuchung (Nr. 2 zu § 7).

Unabhängig von diesen Wirtschaftlichkeitsbetrachtungen ist vor Abschluß von Verträgen immer zu prüfen, welche Vertragsart (Kauf, Miete, Leasing, Mietkauf oder ähnliches) für den Bund am wirtschaftlichsten ist (Nr. 1.6 zu § 7).

Die Vorl. VV-BHO werden zur Zeit unter Federführung des Bundesministeriums der Finanzen überarbeitet. Am Prinzip der Erfordernis von Wirtschaftlichkeitsbetrachtungen wird dabei festgehalten werden.

## **1.2 Handbuch für Organisationsplanung**

Das vom Bundesministerium des Innern herausgegebene Handbuch<sup>12</sup> für Organisationsplanung enthält im Teil 3 Hinweise zum methodischen Vorgehen beim Einsatz der Informationstechnik, dort in Nr. 4.3.2.5 Anregungen für den Organisator zur Durchführung von Wirtschaftlichkeitsbetrachtungen.

## **1.3 Gliederung von IT-Rahmenkonzepten**

In der als Band 18 der Schriftenreihe der KBSt herausgegebenen Empfehlung<sup>13</sup> zur "Gliederung der IT-Rahmenkonzepte mit Hinweisen und Erläuterungen zu ihrer Erstellung und Fortschreibung" heißt es im Zusammenhang mit geplanten Vorhaben:

"Für Wirtschaftlichkeitsbetrachtungen zu IT-Vorhaben sind als wesentliche Größen Bedarf (Ziele), Nutzen und Kosten zu behandeln. Um den Bedarf schlüssig herzuleiten, kann auf vorhandene Vor- und Hauptuntersuchungen verwiesen werden. Alternativen – wie z. B. die bisherige Lösung der Fachaufgabe – sind zu diskutieren. Falls Zahlen vorliegen, z. B. hinsichtlich des Mengengerüsts, sollen sie in die Argumentation einbezogen werden. Der Nutzen eines Vorhabens muß in jedem Fall nachgewiesen werden, auch wenn eine Quantifizierung nicht möglich ist. Der Aufwand zum Nachweis des Nutzens hängt zudem vom Umfang und der Bedeutung des Vorhabens ab. Die Darstellung sollte sich an § 7 BHO und den Verwaltungsvorschriften zum § 7 BHO orientieren. Eine vollständige und überzeugende Darstellung der Kosten (Hardware, Software, Beratung/Erstellung und Ausbildung) ist unverzichtbar, sie sollte auch eine Abschätzung des eigenen Arbeitsaufwandes einschließen. Über eine jährliche Fortschreibung kann durch eine solche Abschätzung auch die Dynamik eines IT-Vorhabens erkennbar werden. Aus den Wirtschaftlichkeitsbetrachtungen sollen sich auch die Haushaltsansätze ergeben. Um weitgehende Vollständigkeit zu erreichen, sind hier auch die für das Verfahren relevanten Beträge zu berücksichtigen, die nicht unter der Titelgruppe Datenverarbeitung eingestellt sind, wie z. B. Kosten der Schulung oder Arbeitsplatzausstattung."

<sup>12</sup> Bundesminister des Innern [Hrsg.]: Handbuch für Organisationsplanung; Az. O 12 - 131024 -2/0 vom Oktober 1988 – darin als Teil 3: Hinweise zum methodischen Vorgehen beim Einsatz der Informationstechnik in der Bundesverwaltung –IT-Org.-Hinweise–; Az. O 12 - 131 120/13 vom November 1990

<sup>13</sup> siehe auch Nr. 1.3 der IT-Prüfungshinweise (Fußnote auf Seite 17)

#### 1.4 Empfehlung der KBSt zu Wirtschaftlichkeitsbetrachtungen

Die KBSt hat im Jahre 1992 eine Empfehlung<sup>14</sup> zur Durchführung von Wirtschaftlichkeitsbetrachtungen beim Einsatz der IT herausgegeben. Die Empfehlungen berücksichtigen sowohl monetär bewertbare als auch nicht monetär bewertbare Kriterien. Diese können arbeitsplatzbezogen, arbeitsplatzübergreifend, gesamtorganisationsbezogen sowie im Hinblick auf externe Wirtschaftlichkeitseffekte bedeutsam sein. Die Empfehlung geht von folgenden Kriterien für eine Wirtschaftlichkeitsbetrachtung aus:

- Einmalige Kosten- und monetäre Nutzen-Kriterien
  - o Einmalige Kosten für das neue IT-Verfahren (Planungs- und Entwicklungskosten, Systemkosten, Kosten der Systemeinführung)
  - o Einmaliger monetärer Nutzen (einmalige Kosteneinsparungen aus Vermeidung von Erhaltungskosten und/oder Erweiterungskosten des Altsystems, einmalige Erlöse aus der Verwertung des Altsystems)
- Laufende Kosten- und monetäre Nutzen-Kriterien
  - o Laufende Sachkosten/Sachkosteneinsparungen (Leitungskosten/Postgebühren, anteilige CPU-Kosten, Verbrauchsmaterial, Datenträger, Energie- und Raumkosten)
  - o Laufende Personalkosten/Personaleinsparungen (Personalkosten aus Systembenutzung, Kosten/Nutzen aus Dienstposten-Umstufung, Einsatzbetreuung und Systemadministration, Schulung/Fortbildung)
  - o Laufende Kosten/Einsparungen bei Wartung/Systempflege (Hardware, Software)
  - o Sonstige laufende Kosten und Einsparungen (Datenschutz/-sicherungskosten, Kosten externer Beratung, Versicherungen, sonstige laufende Kosten)
- Dringlichkeitskriterien
  - o Ablösedringlichkeit Altsystem (Unterstützungskontinuität, Stabilität, Flexibilität)
  - o Einhaltung von Verwaltungsvorschriften und Gesetzen
- Qualitativ-strategische Kriterien
  - o Priorität des IT-Vorhabens
  - o Qualitätszuwachs bei der Erledigung von Fachaufgaben (Leistungssteigerung bei der Aufgabenabwicklung, Beschleunigung von Arbeitsabläufen)
  - o Informationssteuerung der administrativ-politischen Ebene (besserer Informationsstand der Entscheidungsträger, Erhöhung der Entscheidungskompetenz und des Entscheidungsspielraums)
  - o Mitarbeiterbezogene Effekte (Attraktivität der Arbeitsbedingungen, Qualifikationssicherung/-erweiterung)

<sup>14</sup> Bundesministerium des Innern [Hrsg.]: Empfehlung zur Durchführung von Wirtschaftlichkeitsbetrachtungen beim Einsatz der IT in der Bundesverwaltung (Empfehlung IT-WiBe) Version 1 - Juli 1992 (Schriftenreihe der KBSt; Band 26)

- o Effekte hinsichtlich Bürgernähe (Einheitliches Verwaltungshandeln und höhere Rechtssicherheit, Erhöhung der Verständlichkeit und Transparenz des Verwaltungshandelns, extern wirksame Beschleunigung von Verwaltungsentscheidungen, Imageverbesserung)

Die Empfehlung gibt eine Methode an, die monetär bewertbare und nicht monetär bewertbare Kriterien zusammenführt.

### **1.5 Regelungen einzelner Verwaltungen**

Detailliertere Regelungen und Arbeitshilfen finden sich in den Richtlinien einzelner Ressorts und Behörden, z. B. den Richtlinien für Wirtschaftlichkeits- und Nutzenuntersuchungen bei der Deutschen Bundespost (Richtl WNU, KNr 651 240 000-7) aus dem Jahre 1987 oder den Richtlinien für Wirtschaftlichkeitsuntersuchungen – Investitionsmaßnahmen – (RWU 2 – DS 213/2) der Deutschen Bundesbahn vom 1. Juli 1983.

## **2 Aufstellen von Wirtschaftlichkeitsbetrachtungen**

Wirtschaftlichkeitsbetrachtungen werden in der Bundesverwaltung überwiegend im Zusammenhang mit der Planung von IT-Vorhaben und der Erstellung und jährlichen Fortschreibung von behörden- und vorhabenbezogenen IT-Rahmenkonzepten durchgeführt.

Soweit Berechnungen durchgeführt werden, sind sie in der Regel auf den Beginn eines Vorhabens oder den Betrachtungszeitpunkt zu beziehen. Der Betrachtungszeitraum der Berechnungen ist vom jeweiligen Vorhaben abhängig. Er sollte in jedem Fall über den Zeitpunkt des Einsatzes oder der Einführung hinausreichen, um z. B. Betriebskosten mitzuberücksichtigen. Insbesondere bei größeren Vorhaben geht dieser Zeitraum weit über den Rahmen der mittelfristigen Finanzplanung hinaus.

Bei Ersatzbeschaffungen oder geringem Investitionsvolumen kann auf Wirtschaftlichkeitsbetrachtungen verzichtet werden. Hierbei ist jedoch zu bedenken, daß auch Vorhaben mit geringem Investitionsvolumen und Ersatzbeschaffungen weitreichende Auswirkungen auf die Organisation haben und mit hohen Folgekosten verbunden sein können. Auch können Sicherheitsanforderungen eine Rolle spielen, durch die weitere ausgabenwirksame Maßnahmen notwendig werden. In jedem Fall sollten Alternativen erwogen und ein Vergleich der Kosten dieser Alternativen durchgeführt werden.

## **3 Berechnungsmethoden**

Es werden im Rahmen von Wirtschaftlichkeitsbetrachtungen sowohl statische als auch dynamische Berechnungsverfahren angewandt – bei statischen Verfahren in der Regel Kostenvergleichsrechnungen, bei dynamischen Verfahren hat sich die Kapitalwertmethode durchgesetzt.

Kostenvergleichsrechnungen eignen sich für den Vergleich qualitativ gleicher Alternativen, typischerweise Beschaffungsmaßnahmen mit geringerem Umfang. Da sich in der IT in der Regel das Ausgabevolumen über mehrere Jahre hinweg verteilt, ist die Kapitalwertmethode grundsätzlich vorzuziehen.

Als Kalkulationszinsfuß ist nach dem Handbuch für Organisationsplanung "der übliche Kapitalmarktzins für Kredite vergleichbarer Laufzeit" anzusetzen, "dabei ist in der Regel von dem Realzins öffentlicher Anleihen auszugehen (= durchschnittliche Emissionsrendite der Anleihen der öffentlichen Hand abzüglich der Änderungen des Preisindex für das Bruttosozialprodukt)". In den vergangenen 30 Jahren lag dieser Zinssatz um oder unter 6 v. H., so daß für die Festlegung des Zinssatzes kein grundsätzliches Problem besteht.

Soweit alternative Lösungen untersucht werden, wird zweckmäßigerweise darauf verzichtet, die in beiden Fällen gleichen Kosten in die Berechnung einzubeziehen.

Restwerte und Zeitwerte sollten nur dann berücksichtigt werden, wenn entsprechende Einnahmen auch tatsächlich erzielt werden können. Eine Vorhersage dazu ist in der IT wegen des raschen Wechsels der Gerätegenerationen schwierig. Soweit bekannt sind auch die Kosten für die Entsorgung von Geräten zu berücksichtigen.

#### 4 Kostenarten und Kostensätze

Im Gegensatz zu Kostenvergleichen bei anstehenden Vertragsabschlüssen (nach Nr. 1.6 der Vorl. VV zu § 7 BHO ) sind bei der Planung von IT-Vorhaben die für die Anwendung von Berechnungen wichtigen Eingangsgrößen in der Praxis häufig nur schwer zu ermitteln. So sind, insbesondere bei umfangreichen Entwicklungen in der IT, mitunter Wirtschaftlichkeitsbetrachtungen bereits zu einem Zeitpunkt erforderlich, wenn der eigene Personalaufwand, der Umstellungsaufwand, die Nutzungsdauer, die Restwerte oder die Ausgaben für Externe noch nicht hinreichend bekannt sind (siehe Nr. 5).

Grundsätzlich sollte eine Vollkostenbetrachtung angestrebt werden, d. h. es werden auch die kalkulatorischen Kosten (und Nutzen) berücksichtigt, die nicht unmittelbar bei den IT-Ausgaben haushaltswirksam sind, z. B. die Kosten des eigenen Personals.

#### 5 Berücksichtigung von Preisänderungen und Unsicherheiten

Wenn in einer Wirtschaftlichkeitsbetrachtung Zukunftsdaten einfließen, die mit Unsicherheiten behaftet sind, weil zum Zeitpunkt der Betrachtung keine genauen Aussagen möglich sind, z. B. hinsichtlich Nutzungsdauer, Preisentwicklung, Änderungen des Geschäftsanfalls, Änderungen des Personalbedarfs durch Arbeitszeitverkürzung, sind weitergehende Überlegungen notwendig.

Hilfreich können insbesondere Empfindlichkeitsanalysen (Sensitivitätsanalysen) sein. Dabei werden ungenau zu bestimmende Eingangsgrößen hinsichtlich ihrer Auswirkung

auf das Ergebnis der Wirtschaftlichkeitsbetrachtung untersucht. Sensitivitätsanalysen können große Unterschiede bei der Berechnung der zu erwartenden Einsparungen aufzeigen, z.B. durch unterschiedliche Annahmen über den Abschluß einer Maßnahme.

## 6 Nutzwertanalysen, Nutzen-Kosten-Analysen

Wenn mehrere unterschiedliche Ziele zu berücksichtigen sind, eine Entscheidung aufgrund von Nutzendarlegungen oder eine reine Bewertung nach Kosten nicht möglich ist, können Nutzwertanalysen angewandt werden, bei denen Sachverhalte subjektiv, etwa durch Punktevergaben, bewertet werden. In der Regel werden Nutzwertanalysen zusammen mit Kostenrechnungen durchgeführt.

Die Entscheidungsfindung ist dann einfach, wenn die Ergebnisse der Wirtschaftlichkeitsrechnung und der Nutzwertanalyse für die gleiche Lösungsalternative sprechen. In allen anderen Fällen besteht eine Möglichkeit darin, beide Betrachtungen in einer Nutzen-Kosten-Analyse zu verknüpfen. Dazu kann beispielsweise für das Kostenergebnis der Wirtschaftlichkeitsberechnung eine entsprechende Umrechnung in die Punktbewertung der Nutzwertanalyse erfolgen. Man kann z. B. der wirtschaftlichsten Alternative (mit dem kleinsten Kapitalwert oder den geringsten Ausgaben) die maximale Punktzahl geben. Ein Maß der Abweichung kann die prozentuale Abweichung des Kapitalwertes vom günstigsten Wert sein. Diese Abweichung kann dann mit einer entsprechenden Punktzahl bewertet werden.

Unabhängig von der Methode im einzelnen bringen Nutzwertanalysen oder Nutzen-Kosten-Analysen die Beteiligten dazu, die relevanten Kriterien auszuwählen und die entsprechenden Bewertungen einzubringen. In diesem Sinne fördern Nutzwertanalysen oder Nutzen-Kosten-Analysen den Konsens der Beteiligten.

Je nach Art und Umfang des Vorhabens wird im Einzelfall zu entscheiden sein, welche Methode am zweckmäßigsten ist.

## Beispiele für Prüfungsansätze

### Inhaltsverzeichnis

	Seite
<b>Vorbemerkung zu den Beispielen.....</b>	<b>116</b>
<b>Beispiel 1: Informationstechnik einer Behörde.....</b>	<b>118</b>
1 IT-Organisation .....	119
2 Rechenzentrum.....	120
3 Datenfernübertragung.....	122
4 Arbeitsplatzcomputer .....	123
5 Beschaffung und Wartung von Hardware .....	124
6 IT-Verfahren .....	125
7 Datenbanken.....	126
8 Softwareentwicklung und -pflege.....	127
<b>Beispiel 2: IT-Vorhaben .....</b>	<b>130</b>
1 Allgemeines.....	130
2 Voruntersuchung .....	131
3 Hauptuntersuchung .....	132
4 Ausführung.....	132
5 Einführung .....	133
<b>Beispiel 3: IT-Verfahren.....</b>	<b>135</b>
1 Organisation .....	135
2 Verfahrenspflege .....	135
3 Betrieb.....	138
4 Datensicherheit/Datenschutz .....	140
<b>Beispiel 4: Beschaffung von Arbeitsplatzcomputern.....</b>	<b>141</b>
1 Vergabe .....	141
2 Vertragsabwicklung.....	142



<b>Beispiel 5: Einsatz lokaler Netze.....</b>	<b>144</b>
1 Planungsziele/Konzeption.....	144
2 Ist-Aufnahme .....	145
3 Durchführung.....	145
4 Kosten .....	147
5 Nutzung.....	147
<b>Beispiel 6: Notfallplanung.....</b>	<b>148</b>
1 Anforderungen an die Notfallplanung.....	148
2 Ermittlung des Kapazitätsbedarfs.....	149
3 Bereitstellung von Ersatzrechensystemen .....	151
4 Sicherungskonzept und Wiederanlaufmaßnahmen.....	152
5 Wiederanlaufkonzept .....	154
6 Notfallorganisation.....	155
7 Tests und Übungen .....	156
<b>Beispiel 7: Beschaffung von Hardware.....</b>	<b>157</b>
1 Organisation.....	157
2 Durchführung.....	157
3 Kontrolle .....	158

## Vorbemerkung zu den Beispielen

Die IT-Prüfungshinweise sollen dem Prüfer Anregungen für die Prüfung von Maßnahmen der Verwaltung im Bereich der Informationstechnik geben. Voraussetzung für eine wirtschaftliche und wirksame Prüfungstätigkeit ist deren gründliche Vorbereitung. Der Prüfungsleitfaden<sup>15</sup> des Bundesrechnungshofes empfiehlt eine strukturierte Vorgehensweise bei der Prüfungsvorbereitung:

- 1 - Erläuternde Angaben zum Prüfungsvorhaben  
Beschreibung des Prüfungsfeldes mit Abgrenzung des Prüfungsvorhabens; Anlaß der Prüfungstätigkeit; Darstellung der mit der Prüfung verfolgten Zielvorstellung  
**wer** und/oder **was**, **warum** soll geprüft werden?  
**was** soll damit bezweckt werden?
- 2 - Beschaffung und Auswertung der für die Prüfung erforderlichen Materialien  
Informationssammlung anhand prüfungsbezogener Unterlagen, Auswertung früherer Prüfungserkenntnisse; Verfahren und Grundsätze für die Beschaffung  
**was** wird zur Vorbereitung benötigt?
- 3 - Festlegung des geplanten Erhebungsablaufs
  - Auswahl der zu prüfenden Stellen
  - Bestimmung des zeitlichen Rahmens
  - Festlegung der Vorgehensweise
    - = Bestimmung von Prüfungsbreite und -tiefe
    - = Festlegung von Prüfungsschwerpunkten
    - = Beschreibung der vorgesehenen Prüfungstechnik**wo** ) soll  
**wann** ) geprüft  
**wie** ) werden
- 4 - Zusammenarbeit mit weiteren Stellen
  - Beteiligung zuständiger Prüfungsgebiete
  - Unterstützung durch Vorprüfstellen
  - Hinzuziehung von Sachverständigen
  - Zusammenarbeit mit anderen externen Prüfungseinrichtungen (Landesrechnungshöfe, internationale Rechnungshöfe)**wer** ist zu beteiligen?

Das dabei erarbeitete Prüfungskonzept soll als Richtschnur für den Prüfungsverlauf dienen. Es wird zumeist mit einem Fragen- oder Stichwortkatalog die Prüfungsschwerpunkte beschreiben und vertiefen.

<sup>15</sup> Der Präsident des Bundesrechnungshofes [Hrsg.]: Prüfungsleitfaden –Arbeitshilfe für die Prüfer des Bundesrechnungshofes – Frankfurt am Main, 2., überarbeitete und erweiterte Auflage 1992

Die Umsetzung der IT-Prüfungshinweise in ein für den Einzelfall einer Prüfung geeignetes spezielles Prüfungskonzept mit zugehörigem Fragenkatalog kann sinnvoll nur für den einzelnen Prüfauftrag geschehen. Der Prüfer hat daher aus der Vielzahl von möglichen Einzelthemen die für seine Prüfung geeigneten Themen und Fragestellungen selbst zusammenzustellen. Er muß dabei z.B. neben den beabsichtigten Prüfungsschwerpunkten auch den einsetzbaren Zeit- und Personalaufwand für die Prüfung und die der Prüfung angemessenen Arbeitsweisen und Prüfungstechniken beachten. Die Nutzbarkeit von Fragensammlungen ist daher grundsätzlich insoweit begrenzt, als die Besonderheiten des Einzelfalles nicht berücksichtigt werden können und die Fragen bezogen auf einen Einzelfall nicht vollständig sein können.

Ungeachtet dessen sind in diesem Anhang beispielhaft einige Themen- und Fragenkataloge aufgenommen, wie sie bei der Vorbereitung von Prüfungen des Bundesrechnungshofes und der Vorprüfstellen des Bundes entstehen können. Um die Beispiele für einen allgemeinen Leserkreis verständlicher zu machen, wurden keine speziellen Fragen zu den Besonderheiten einzelner Verfahren, Anlagen oder Organisationen aufgeführt. Auch wurde die Wiederholung von inhaltlich gleichen Fragen bei den verschiedenen Prüfungsthemen in Kauf genommen. Die Fragen dienen der Erhebung von Sachverhalten und sollen keine Wertung vorgeben.

Um die Unterschiede von Prüfungsthemen und Prüfungsansätzen zu demonstrieren wurden Beispiele aus verschiedenen Bereichen gewählt:

- Allgemeine Prüfungen dienen oft dazu, das Verwaltungshandeln im Bereich IT möglichst umfassend zu beurteilen. Die Fragenkataloge sind in solchen Fällen dadurch geprägt, alle Bereiche des Verwaltungshandelns abzudecken und gehen insofern eher in die Breite als in die Tiefe des Prüfungsstoffes (**Beispiel 1: Informationstechnik einer Behörde**).
- Bei der Prüfung von IT-Anwendungen kann der Schwerpunkt der Untersuchung sowohl die Entwicklung (**Beispiel 2: IT-Vorhaben**) als auch die Nutzung (**Beispiel 3: IT-Verfahren**) sein. Bei den ausgewählten Beispielen stehen Fragen der Ordnungsmäßigkeit im Vordergrund.
- Je enger der Prüfungsschwerpunkt auf einzelne Themen eingegrenzt wird, um so spezieller können auch die Fragen werden (**Beispiel 4: Beschaffung von Arbeitsplatzcomputern**, **Beispiel 5: Einsatz lokaler Netze** und **Beispiel 6: Notfallplanung**).
- Das letzte Beispiel gilt einer Prüfung zur Wirtschaftlichkeit der Beschaffung (**Beispiel 7: Beschaffung von Hardware**).

## **Beispiel 1:**

### **Informationstechnik einer Behörde**

#### **Vorbemerkung**

Die Behörde will neben der zentralen Datenverarbeitung vermehrt dezentral vernetzte Arbeitsplatzcomputer einsetzen. Die Prüfung soll einen Überblick über die IT-Aktivitäten der Verwaltung verschaffen.

#### **Inhalt des Themen- und Fragenkataloges:**

- 1 IT-Organisation  
Aufbauorganisation  
Ablauforganisation/Abwicklungsunterlagen  
Termin- und Arbeitsablaufplanung  
Personal
- 2 Rechenzentrum  
Verfügbarkeit  
Systembelastung  
Sicherheit  
Archiv
- 3 Datenfernübertragung  
Hardware  
Datenübermittlungsdienste  
Kommunikationssystem, Betriebssystem  
Nutzung
- 4 Arbeitsplatzcomputer  
Einsatz von Arbeitsplatzcomputer (APC)  
Dezentrale Datenbestände  
Vernetzung
- 5 Beschaffung und Wartung von Hardware  
Beschaffung  
Wartung
- 6 IT-Verfahren
- 7 Datenbanken
- 8 Softwareentwicklung und -pflege  
Entwicklung  
Pflege  
Fremdsoftware  
Externe Mitarbeiter  
Test und Freigabe von Programmen

# 1 IT-Organisation

## **Aufbauorganisation**

- In welche Funktionsgruppen ist das Rechenzentrum gegliedert?
- Sind Stellenbeschreibungen vorhanden?
- Entsprechen die Tätigkeiten der Mitarbeiter den Aufgabenbeschreibungen des Geschäftsverteilungsplanes?
- Inwieweit ist das Prinzip der Funktionentrennung bei der Aufbauorganisation beachtet, insbesondere im Hinblick auf IT- und Fachabteilung, Programmier- und Maschinenpersonal sowie Archiv und Operating?
- Wer ist Ansprechpartner für die Fachabteilungen?
- Wie sind die Vertretungsverhältnisse geregelt?
- Gibt es Kompetenzüberschneidungen?

## **Ablauforganisation/Abwicklungsunterlagen**

- Wie wird die Zusammenarbeit koordiniert?
- Existieren schriftliche Unterlagen, Arbeitsanweisungen oder Regelungen in denen
  - Arbeitsabläufe,
  - Zuständigkeiten,
  - Aufbau und Inhalt von Arbeitsunterlagen, Beschaffungs- und Planungsmaßnahmen festgelegt sind?
- Gewährleisten die Stellenbeschreibungen und die Arbeitsanweisungen eine ausreichende Funktionentrennung?
- Wie erfolgt die Zusammenarbeit mit den Fachabteilungen?

## **Termin- und Arbeitsablaufplanung**

- Werden die Aufträge (Daueraufträge, Einzelaufträge) nach einem Terminplan abgewickelt?
- Enthalten die Aufträge Angaben über Verarbeitungsdauer, Verarbeitungszeitpunkt, benötigte Betriebsmittel, Abhängigkeiten von anderen Aufträgen und Prioritäten?
- Ist die Terminplanung mit den Fachbereichen abgestimmt?
- Werden die Termine überwacht?
- Wie wird bei Terminüberschreitungen reagiert?

- Werden alle Arbeitsabläufe (Jobs) von der Arbeitsvorbereitung vorgegeben und kontrolliert?
- Sind Vorkehrungen für den Wiederanlauf der Verfahren getroffen worden?

### **Personal**

- Ist das Personal entsprechend den Stellenbeschreibungen eingesetzt?
- Kann das eingesetzte Personal die anfallenden Aufgaben bewältigen?
- Gibt es Verfahren, die nur personenabhängig zu betreiben sind ("unersetzbare Mitarbeiter")?
- Liegt ein Ausbildungskonzept vor?
- Welche Aus- und Fortbildungsmaßnahmen werden durchgeführt? Sind sie in diesem Umfang erforderlich und ausreichend?

## **2 Rechenzentrum**

### **Verfügbarkeit**

- Wie sind die Betriebszeiten des Rechenzentrums?
- Welche Anwendungen laufen am Tage, welche nachts?
- In welchen Zeiten steht die Anlage den Anwendern regelmäßig nicht zur Verfügung, z.B. wegen Wartungs- und Archivierungsarbeiten?
- Ist ein bedienerloser Betrieb möglich?
- Können Verarbeitungsläufe zur Entzerrung der Systembelastung in die Zeiten geringerer Systembelastung verlagert werden?
- Welche zusätzlichen Anwendungen sind geplant?
- Wie hoch sind die Ausfallzeiten von Hardware- und Softwarekomponenten? Werden darüber Statistiken geführt? Werden die Gründe für die Ausfälle festgehalten und untersucht? Sind die Risiken ausreichend abgesichert?

### **Systembelastung**

- Werden Verarbeitungsprotokolle erstellt, gesammelt und ausgewertet?
- Wird die Systembelastung (Zentraleinheit, Kanäle, Datensichtgeräte) regelmäßig überwacht?
- Wie hoch ist die durchschnittliche Systemauslastung?
- Wie verteilt sich die Systemauslastung auf die einzelnen Anwendungen?

- Wie ist das Antwortzeitverhalten bei Dialoganwendungen?
- Was wird gegen sich anbahnende Lastspitzen unternommen? Sind freie Kapazitäten vorhanden?
- Gibt es ein Datenmanagementkonzept?
- Werden die Datenbestände regelmäßig ausgewertet? Gibt es Ad-hoc-Auswertungen?
- Wie sind die Auswertungsläufe organisiert? Wann laufen die Auswertungen?

### **Sicherheit**

- Gibt es eine Risikoanalyse und ein Sicherheitskonzept?
- Wie ist die Zugangssicherung zum Rechenzentrum geregelt?
- Wird die Zugangssicherung eingehalten?
- Ist das Rechenzentrum räumlich von anderen Organisationseinheiten getrennt?
- Ist der Archivraum räumlich vom Maschinensaal getrennt?
- Gibt es einen Katastrophenplan?
- Wann wird wie gesichert?
- Wie werden Datenbestände rekonstruiert?
- Wurde die Rekonstruktion schon einmal erprobt?
- Ist im Fehlerfalle ein schneller Wiederanlauf der Verfahren ohne Datenverlust möglich?
- Haben Operatoren Zugriff auf archivierte Bänder?
- Durch welche Maßnahmen ist sichergestellt, daß nur berechtigte Personen Anwendungen starten und auf Daten zugreifen können?
- Wird der Passwortschutz sachgerecht eingesetzt?
- Wird das Systempasswort regelmäßig geändert? Wer hat Kenntnis vom Systempasswort?
- Haben die Programmierer die Möglichkeit auf den Produktionsdatenbestand zuzugreifen? Haben Programmierer Zugriff auf die Produktionskennung?
- Steht den Anwendern eine Funktion zur Verfügung, um selbst das Passwort ändern zu können?
- Wird überwacht, daß das Passwort regelmäßig geändert wird?
- Werden unzulässige Zugriffsversuche auf sensible Daten protokolliert?

- Werden personenbezogene oder andere schutzwürdige bzw. geheimhaltungspflichtige Daten gespeichert? Gibt es einen Datenschutzbeauftragten?

#### **Archiv**

- Liegt ein Archivierungskonzept vor?
- Ist die Organisation der Archivierung und Sicherung mit den Fachbereichen abgestimmt?
- Gibt es Richtlinien, die die Archivierung und Bestandsverwaltung (Einlagerung, Auslagerung von Datenträgern) regeln?
- Gibt es ein Sicherheitsarchiv?
- Werden Datenträger ausschließlich durch Archivpersonal ein- und ausgelagert?
- Werden die Datenträger nur an berechnigte Personen ausgegeben?
- Werden Bestandsnachweise geführt?
- Werden die Datenträger mit Hilfe eines maschinellen Archivierungsverfahrens verwaltet?
- Sind Aufbewahrungsfristen festgelegt und werden diese beachtet?
- Wie werden die Datenträger vor vorzeitigem Überschreiben geschützt?
- Wird die Vollständigkeit der Datenträger regelmäßig überprüft?
- Wie sind die eingelagerten Datenträger gekennzeichnet?

### **3 Datenfernübertragung**

#### **Hardware**

- Welche Datenübertragungseinrichtungen werden verwendet (Anzahl der Geräte, Leistungskennzahlen, Beschaffungszeitpunkt und -art)? Wie ist deren Wartung geregelt?
- Gibt es ein dokumentiertes Netzkonzept?

#### **Datenübermittlungsdienste**

- Welche Datenübermittlungsdienste (HfD, DATEX-L, DATEX-P, ISDN) werden genutzt?  
Wieviele Zugänge bestehen?
- Wie hoch sind die Kosten für die Datenübermittlungsdienste?
- Nach welchen Kriterien wurden die Datenübermittlungsdienste ausgewählt ?



- Liegen Wirtschaftlichkeitsbetrachtungen zum gewählten Datenübermittlungsdienst vor?
- Wird die Wirtschaftlichkeit des gewählten Datenübermittlungsdienstes regelmäßig geprüft?
- Kann ein anderer Datenübermittlungsdienst genutzt werden, um die Kosten zu verringern?

#### **Kommunikationssystem, Betriebssystem**

- Welches Kommunikationssystem wird eingesetzt?
- Welches Betriebssystem wird eingesetzt?
- Wie wurden die Systeme beschafft?
- Wie ist die Systemwartung geregelt? Wie werden neue Systemversionen eingesetzt?
- Welche Anwendungssoftware wird eingesetzt?

#### **Nutzung**

- Welche Stellen sind an das Netz angeschlossen?
- Wie hoch ist das übertragene Datenvolumen?
- Sind die Datenendeinrichtungen aus fachlicher Sicht in der vorhandenen Anzahl notwendig?
- Werden Störungen des Kommunikations- und des Betriebssystems sowie der Anwendungssoftware protokolliert?
- Werden Verfügbarkeits- und Auslastungsmessungen durchgeführt und ausgewertet?
- Wie hoch sind Verfügbarkeit und Auslastung der Systeme?

## **4 Arbeitsplatzcomputer**

#### **Einsatz von Arbeitsplatzcomputer (APC)**

- Wie hoch sind die Kosten der APC?
- Sind Wirtschaftlichkeitsberechnungen durchgeführt worden?
- Wie sind die APC ausgestattet?
- Sind die APC untereinander kompatibel?
- Sind die APC untereinander vernetzt?

- Gibt es eine Verbindung zu anderen Rechensystemen?
- Liegen Anwendungskonzepte vor?
- Welche Software ist auf den APC verfügbar?
- Wer ist für den Einsatz der APC verantwortlich?
- Wer entwickelt Programme? Gibt es Programmieraktivitäten in den Fachabteilungen?
- Gibt es Systembetreuer?
- Wie werden die Benutzer geschult und betreut?

#### **Dezentrale Datenbestände**

- Gibt es ein Datenhaltungskonzept?
- Besteht in den Fachabteilungen die Notwendigkeit eigene Datenbestände dezentral zu führen und auszuwerten?
- Werden Daten redundant gespeichert?
- Wie werden die Daten konsistent gehalten?

#### **Vernetzung**

- Liegt für die geplante Vernetzung ein Konzept vor?
- Wurden technische Alternativen untersucht?
- Welche Informationen sollen ausgetauscht werden?
- Wie werden diese Informationen zur Zeit weiterverbreitet?
- Wie hoch sind die Kosten der Vernetzung?
- Sind bauliche Maßnahmen erforderlich?
- Welche zusätzliche Hardware und Software wird benötigt?
- Wurde der erwartete Nutzen erreicht? Welche Umstände können eine wirtschaftliche Nutzung beeinträchtigen ?

## 5 Beschaffung und Wartung von Hardware

#### **Beschaffung**

- Liegen Beschaffungsrichtlinien vor?
- Sind die Zuständigkeiten der Beteiligten (Antragsteller, Fachdienst, IT-Koordinator, Organisation, Geräteausschuß, Beschaffungsstelle, Beauftragter für den Haus-

halt, Rechenzentrum) bei Beschaffungsmaßnahmen sowohl für den zentralen als auch für den dezentralen Bereich geregelt?

- Wurde der Bedarf sachgerecht und nachvollziehbar ermittelt? Ist der Hardwarebedarf aus den fachlichen Anforderungen abgeleitet worden?
- Ist der mittelfristige Hardwarebedarf in einer Beschaffungsplanung zusammengefaßt?
- Ist die Hardware in einem Bestandsverzeichnis erfaßt?
- Werden Auslastungsstatistiken erstellt?
- Wurde Hardware im Wettbewerb beschafft?
- Wurde die voraussichtliche Nutzungsdauer der Hardware ermittelt?
- Wurden Wirtschaftlichkeitsrechnungen durchgeführt, um die kostengünstigste Beschaffungsart zu ermitteln?

### **Wartung**

- Gibt es ein Wartungskonzept?
- Für welche Geräte wurden Wartungsvereinbarungen getroffen?
- Um welche Art von Wartung handelt es sich (vorbeugende Wartung, korrektive Wartung)?
- Werden Wartungsleistungen im Wettbewerb vergeben?
- Werden Wartungserfordernisse bei der Beschaffung berücksichtigt? Hat der Wartungsbedarf Einfluß auf die Beschaffungsart und auf die Auswahl der Lieferfirmen?
- Werden Wartungsverträge auf der Grundlage der BVB geschlossen?
- Werden Wartungsverträge regelmäßig auf ihre Wirtschaftlichkeit hin untersucht?
- Werden Störungen und Fehler bei Geräten dokumentiert?
- Werden diese Dokumentationen zur Bestimmung von Wartungserfordernissen regelmäßig ausgewertet?
- Sind verbindliche Zeitpläne für Wartungsintervalle vereinbart?
- Wurde die Wartungsleistung entsprechend den Vereinbarungen erbracht?
- Sind die Wartungsarbeiten dokumentiert?
- Sind Wartungsverträge für die Dauer der Gewährleistung abgeschlossen?
- Werden APC, APC-Drucker oder Bildschirme vorbeugend gewartet?

## 6 IT-Verfahren

- Gibt es für die Verfahren Richtlinien und Arbeitsanweisungen?
- Sind ausreichende Kontrollfunktionen vorgesehen?
- Werden die Richtlinien und Arbeitsanweisungen beachtet?
- Wie ist die Annahme eingehender Daten geregelt?
- In welcher Form werden Daten geliefert? Wieviele der gelieferten Daten müssen noch manuell erfaßt werden?
- Sind die Zuständigkeiten für die Datenerfassung klar geregelt?
- Ist der zeitliche Ablauf der Annahme und Erfassung von Daten erkennbar?
- Werden die eingehenden und erfaßten Daten auf Vollständigkeit untersucht? Wird der Verlust von Daten erkannt?
- Ist für jede Datenart ein bestimmter Erfasserkreis festgelegt? Sind unterschiedliche Zugriffsberechtigungen eingerichtet?
- Wie werden fehlerhafte Erfassungsbelege behandelt? Werden Erfassungsfehler protokolliert?
- Werden die Erfassungsarbeiten nachgewiesen, z.B. durch Bestätigungsnachweise?
- Werden die eingehenden Daten zeitnah erfaßt und korrigiert?
- Werden Plausibilitätskontrollen durchgeführt?
- Können eingehende Daten unmittelbar weiterverarbeitet werden? Müssen die Daten vor der Erfassung noch auf einen Erfassungsbeleg übertragen oder aufbereitet werden?
- Ist geprüft worden, wie die Kosten der Datenerfassung, z. B. durch Änderung der Organisation, andere Arbeitsmittel oder Datenfernübertragung, gesenkt werden können?
- Wie ist sichergestellt, daß sich Datenträger nur für die Dauer der Verarbeitung außerhalb des Archivs befinden?
- Wie werden die zu erfassenden Datenträger gegen Verlust, Verfälschung und unberechtigte Kenntnisnahme gesichert?

## 7 Datenbanken

- Liegt eine aktuelle Beschreibung der Datenbanken vor?
- Welche Softwarewerkzeuge zur Verwaltung der Datenbanken sind vorhanden?
- Wer hat Zugriff auf die Dienstprogramme zur Verwaltung der Datenbank?

- Wer legt die Datenbankzugriffsberechtigungen fest?
- Können die Zugriffsrechte durch die Verwendungen von Datenbankabfragesprachen umgangen werden?
- Wie ist die Reorganisation der Datenbanken geregelt?
- Wie wird die Konsistenz, Aktualität und Gültigkeit der Daten sichergestellt?
- Welche Fachabteilungen können auf die Datenbanken zugreifen?
- Wer ist für die Änderung der Auswertungen und der Datenbankstrukturen zuständig?
- Sind die Fachabteilungen über die Auswertemöglichkeiten der Datenbanken informiert? Liegen den Fachabteilungen eine Liste der möglichen Auswertungen, Benutzerhandbücher und Verfahrensbeschreibungen vor?
- Werden die vorhandenen Auswertungsmöglichkeiten von den Fachabteilungen genutzt?
- Sind die Informationen in der gelieferten Form verwertbar oder müssen sie in den Fachabteilungen weiter aufbereitet werden?

## 8 Softwareentwicklung und -pflege

### Entwicklung

- Gibt es ein Verzeichnis der eingesetzten Software?
- Sind Programmierrichtlinien vorhanden und werden sie beachtet?
- Welche Entwurfsmethoden werden angewandt?
- Werden bei der Entwicklung Termine gesetzt und Zeitpläne aufgestellt?
- Liegt die Programmdokumentation vollständig und aussagefähig vor?
- Werden Softwarewerkzeuge benutzt, die die Dokumentation der Programme und die Programmierung unterstützen?
- Sind die Programme modular aufgebaut?
- Sind die Fehlermeldungen eindeutig und standardisiert aufgebaut?
- Wie werden die Fachbereiche beteiligt?

### Pflege

- Wie ist das Änderungsverfahren organisiert?
- Gibt es schriftliche Änderungsanforderungen der Fachabteilungen?

- Werden Änderungspläne erstellt?
- Wer überwacht die Durchführung der Arbeiten?
- Wie werden die Änderungen getestet?
- Werden die Änderungsanforderungen auf Wirtschaftlichkeit untersucht?
- Werden mehrere Änderungen zu Versionen zusammenfaßt (Versionen- oder Release-Konzept)?
- Werden die Änderungen vor dem Einsatz dokumentiert?

#### **Fremdsoftware**

- Sind die fachlichen Anforderungen an die Software vor der Beschaffung festgelegt worden?
- Ist die Software im Wettbewerb beschafft worden?
- Sind die Verträge auf der Grundlage der BVB abgeschlossen worden?
- Wird Fremdsoftware hinsichtlich fachlicher Vollständigkeit und ordnungsgemäßer Dokumentation überprüft?
- Ist im Fehlerfalle ein schneller Kundendienst gewährleistet?
- Ist es der Behörde möglich, auftretende Fehler selbst zu beheben?

#### **Externe Mitarbeiter**

- Werden die externen Mitarbeiter nur für Spezialwissen oder kurzfristige Arbeitspitzen eingesetzt?
- Können die Aufgaben ggf. von der Behörde selbst wahrgenommen werden?
- Wie werden die Leistungen abgerechnet?
- Liegen Tätigkeitsnachweise der externen Mitarbeiter vor?

#### **Test und Freigabe von Programmen**

- Gibt es Regelungen für das Abnahme- und Freigabeverfahren?
- Wer veranlaßt die Übernahme der Programme auf die Produktionskennung?
- Wer führt die Übernahme durch?
- Wer gibt die Programme unter welchen Bedingungen frei?
- Liegen Testrichtlinien vor?
- Sind Test- und Produktionsbereich voneinander getrennt?
- Wird ein Abschlußtest durchgeführt?

- Wer führt den Abschlußtest durch?
- Ist der Testumfang und das Testverfahren festgelegt?
- Mit welchen Daten werden die Tests durchgeführt?
- Wird neben der Funktionsfähigkeit der Programme auch deren Quell-Code überprüft?
- Ist der Einsatz der verschiedenen Programmversionen nachvollziehbar dokumentiert?
- Ist nachvollziehbar, welche Programme zu einer Verfahrensversion gehören?

## Beispiel 2:

### IT-Vorhaben

#### Inhalt des Themen- und Fragenkataloges:

- 1 Allgemeines
- 2 Voruntersuchung
- 3 Hauptuntersuchung
- 4 Ausführung  
Feinkonzept  
Programmierung
- 5 Einführung

#### 1 Allgemeines

- Gibt es eine Gesamtübersicht über die IT-Projekte?
- Wie sind die Projekte gegeneinander abgegrenzt?
- Wer sind die Projektverantwortlichen?
- Gibt es IT-Projekte, die vor Abschluß abgebrochen wurden ? Welches waren die Gründe dafür?
- Welche Regelungen für die Projektarbeit gibt es?
- Gibt es Vorgaben für die Dokumentation?
- Gibt es Vorgaben für die Erstellung von Programmen?
- Gibt es allgemeine Qualitätsvorgaben?
- Welche Ziele werden mit dem Projekt verfolgt?
- Hat der IT-Projektleiter im Verlauf des Projekts gewechselt?
- Wer sind die Mitarbeiter der Projektgruppe?
- Wie ist die IT-Projektgruppe organisatorisch eingebettet?
- Welche Kompetenzen hat der Projektleiter?
- Welche Kompetenzen haben die Projektmitarbeiter?
- Finden regelmäßige Projektbesprechungen statt?
- Wie werden die betroffenen Stellen über den Projektinhalt und den Stand des Projektes unterrichtet?



- Wie ist die Projektdokumentation aufgebaut und gegliedert?
- Wie werden die Projekttermine und -kosten überwacht?
- Gibt es Terminverschiebungen? Welche Gründe waren dafür maßgebend (z. B. Personalprobleme, fehlerhafte Aufwandsschätzung, fehlende Personalkapazität, andere Prioritäten)?

## 2 Voruntersuchung

- Wie lautet der Auftrag?
- Wer hat den Auftrag vergeben?
- Wer hat die Voruntersuchung durchgeführt?
- Wurde ein Arbeits-, Zeit- und Terminplan erstellt?
- Wie wurde diese Phase geplant, kontrolliert, durchgeführt? Welche Ergebnisse liegen vor?
- Wie wurde der Ist-Zustand erhoben (z.B. Analyse der Aufbauorganisation, Aufgabenanalyse, Ablaufanalyse, Kommunikationsanalyse)?
- Wie wurden Schwachstellen ermittelt? Wie wurde der Ist-Zustand bewertet?
- Wie wurde der Bedarf für das neue System ermittelt?
- Welche Anforderungen bestehen an das neue System?
- Wie wurden die Anforderungen spezifiziert?
- Handelt es sich um eine neue IT-Anwendung oder um Modifikation einer bestehenden?
- Wie wurde der zu erwartende Aufwand ermittelt?
- Wie wurde der voraussichtliche Nutzen ermittelt?
- Welche finanziellen Auswirkungen hat das Projekt?
- Sind die Auswirkungen auf die Aufbau- und Ablauforganisation beschrieben?
- Fanden Abstimmungen mit den Beteiligten statt?
- Sind alternative Konzepte untersucht worden?
- Sind mögliche Verknüpfungen mit anderen Projekten, Verfahren untersucht worden?
- Wie wurde der Bedarf für das neue System ermittelt?
- Welche Zielsetzungen bestehen im Hinblick auf das neue System?
- Liegt eine Entscheidung über die Fortführung des Projektes vor?

### 3 Hauptuntersuchung

- Wie wurde diese Phase geplant, kontrolliert, durchgeführt? Welche Ergebnisse liegen vor?
- Wer hat die Hauptuntersuchung durchgeführt?
- Wer hat das fachliche Konzept erarbeitet?
- Wer hat das technische Konzept erarbeitet?
- Ist ein Entwurf der benötigten Datenstrukturen vorhanden?
- Wie wurden Belege und Bildschirmformate entworfen?
- Wie wurden die Zugriffsberechtigungen geplant?
- Wie wurden die Benutzerschnittstellen geplant?
- Wie wurden die Einführung und die Schulung geplant?
- Berücksichtigt das Konzept die Arbeitsabläufe und Schnittstellen zu anderen Verfahren?
- Sind Datensicherungsmaßnahmen berücksichtigt worden?
- Wurde Nutzen-Kosten-Untersuchungen erstellt?
- Ist ein Arbeits-, Zeit- und Kostenplan erstellt worden?
- Wie wurden die Kosten und Zeiten ermittelt?
- Welche Arbeitsabschnitte wurden festgelegt?
- Welche Anforderungen an das IT-Basissystem wurden gestellt?
- Wie wurden die fachlich zuständigen Bereiche beteiligt?
- Sind die Auswirkungen des neuen Verfahrens einschließlich organisatorischer und verfahrensmäßiger Verknüpfungen dargestellt?
- Ist über die Fortführung des Projekts entschieden worden?

### 4 Ausführung

#### **Feinkonzept**

- Wie sind die Programmvorgaben erstellt worden?
- Wie wurde diese Phase geplant, kontrolliert, durchgeführt? Welche Ergebnisse liegen vor?
- Gibt es Datenflußpläne?

- Gibt es ausführliche Datendefinitionen (Sätze, Strukturen, Dateien, Speicherungsform, Konsistenz- und Plausibilitätsbedingungen, Datenverarbeitungsregeln)?
- Gibt es Konfigurationsübersichten?
- Gibt es Programmstrukturpläne?
- Gibt es eine Installationsplanung?
- Gibt es eine Wartungsplanung?
- Sind Fremdfirmen beschäftigt worden? Wie wurden deren Leistungen überwacht? Ist die Fortführung der Arbeiten durch die Verwaltung sichergestellt?

### **Programmierung**

- Wie ist die Programmierung organisiert?
- Welche Entwicklungswerkzeuge werden genutzt?
- Welche Programmiersprache wird verwendet?
- Welche Qualitätsvorgaben und Programmierrichtlinien gibt es?
- Sind die Programme nach den Vorgaben entwickelt worden?
- Wie wurden die Programmtests geplant? Wie wurde getestet? Wer hat die Testfälle erstellt? Wer hat die Tests durchgeführt?
- Wie wurde die Einhaltung von Qualitätsvorgaben und Programmierrichtlinien überwacht?
- Wurden Programmreviews durchgeführt?
- Wurden die Terminvorgaben überwacht?
- Gab es Terminüberschreitungen?
- Welche Ursachen hatten die Terminüberschreitungen?
- Welche Maßnahmen wurden bei Terminüberschreitungen getroffen?
- Wie wurde der Programmierungsfortschritt überwacht?
- Wie wurde dokumentiert?
- Enthält die Dokumentation die nach den IT-Mindestanforderungen erforderlichen Unterlagen?

## **5 Einführung**

- Besteht ein Konzept und ein Terminplan für die Einführung?
- Wer war an der Freigabe beteiligt, wer hat sie bescheinigt?

- Fand eine ordnungsgemäße Freigabe statt?
- Wie wurde die Betriebsbereitschaft geprüft?
- Wie ist die Mängelbeseitigung geregelt?
- Wer hat die Schulungsunterlagen erstellt?
- Wurde gezielte Maßnahmenschulung betrieben?
- Wurden die Betriebsvoraussetzungen beim Benutzer geschaffen, z. B. im Hinblick auf Ausbildung, Handbücher, Geräte, Betreuung, sonstige Sachmittel?
- Welche Voraussetzungen wurden für den Betrieb im Rechenzentrum geschaffen?

## Beispiel 3:

### IT-Verfahren

#### Inhalt des Themen- und Fragenkataloges:

- 1 Organisation
- 2 Verfahrenspflege  
Allgemeines  
Programmierung  
Test  
Freigabe  
Schulung  
Dokumentation
- 3 Betrieb  
Dialogverfahren  
Batchverfahren
- 4 Datensicherheit/Datenschutz

#### 1 Organisation

- Welche Organisationseinheiten sind mit der IT befaßt?
- Wie sind deren Kompetenzen gegeneinander abgegrenzt?
- Wie ist die Stellvertretung geregelt? Bleibt die Funktionentrennung erhalten?

#### 2 Verfahrenspflege

##### Allgemeines

- Gibt es Richtlinien für die Durchführung von Verfahrensentwicklungen? Werden sie angewandt?
- Wer regt Änderungen oder Ergänzungen an?
- Wer erteilt Änderungsaufträge?
- Wie ist die Durchführung von Änderungsarbeiten organisiert?
- Wird bei größeren Änderungen wie bei einer Neuentwicklung verfahren?
- Welche Entwicklungs- und Dokumentationswerkzeuge werden eingesetzt?
- Welche Änderungen wurden in jüngster Zeit vorgenommen?

- Welche Änderungen sind vorgesehen? Können die Änderungen in angemessener Zeit umgesetzt werden?
- Werden regelmäßige Verfahrensüberprüfungen vorgenommen?
- Gibt es Probleme mit einzelnen Verfahrensteilen, z. B. im Hinblick auf Verfügbarkeit, Fehleranfälligkeit, Performance, Änderbarkeit?
- Wie werden die Anforderungen der Fachbereiche mit den IT-Bereichen abgestimmt?
- Werden für Änderungen Sollkonzepte erstellt?
- Können die Anforderungen der Fachbereiche bei Änderungen abgedeckt werden?
- Sind die gefundenen Lösungswege wirtschaftlich?
- Wie werden die Änderungen dokumentiert?

### **Programmierung**

- In welcher Phase der Projektentwicklung entsteht die Programmiervorgabe? In welcher Form ist sie abgefaßt? Entspricht sie den Richtlinien?
- Welche Unterlagen gehören zur Programmiervorgabe?
- Sind die Unterlagen vollständig und kann ein Programmierer daraufhin das Programm erstellen oder sind Kenntnisse des Verfahrens erforderlich, die in der Programmvorgabe nicht enthalten sind?
- Werden die Programme modular aufgebaut?
- Wie ist die Programmdokumentation aufgebaut?
- Gibt es eine Dokumentation über das Zusammenwirken der einzelnen Programmmodule?
- Gibt es Datei- und Datenbankübersichten einschließlich der Feldbeschreibungen sowie der Plausibilitäts- und Konsistenzbedingungen?
- Wer ist für die Datenbankverwaltung, Dateidefinition und Dateireorganisation zuständig?
- Sind die Plausibilitäts- und Konsistenzprüfungen vollständig umgesetzt?
- Gibt es Namenskonventionen und werden diese eingehalten?
- Welche Softwarewerkzeuge stehen dem Programmierer zur Verfügung? Wie werden diese eingesetzt?
- Welche Verarbeitungsarten werden in dem Verfahren verwendet?
- Welchen Ausbildungsstand haben die Programmierer?
- Werden die Programmieraufträge in angemessenen Zeiträumen erledigt?

- Wird mit Standardsoftware gearbeitet? Wird diese unverändert gelassen oder angepaßt?
- Wie lange werden alte Versionen aufbewahrt? Wer verwaltet diese?
- Werden mehrere Programmänderungen zu Versionen zusammengefaßt (Versionen- oder Releasekonzept)? Werden die Versionskennzeichen lückenlos vergeben?
- Wer verwaltet die Quellprogramme und die ausführbaren Programme?
- Wie ist die Übergabe neuer Programmversionen an die Datenverarbeitung geregelt?

### **Test**

- Wer ist für die Tests zuständig?
- Gibt es eine eigene Testumgebung?
- Werden nur Programmänderungen getestet oder das gesamte Verfahren, auch wenn nur Teile davon geändert wurden?
- Gibt es eine festgelegte Vorgehensweise für Tests, z. B. vorgegebene Arbeitsschritte oder maschinelle Testhilfen und eine Testdatensammlung? Lassen sich mit den Testdaten alle Arbeitsfälle nachbilden?
- Wie werden die Tests dokumentiert?
- Werden später in der Produktion auftretende Fehler dokumentiert und nachvollziehbar beseitigt?

### **Freigabe**

- Wer ist für das Freigabeverfahren zuständig?
- Welche Richtlinien bestehen für die Freigabe und Übergabe von Programmen an die Datenverarbeitung? Werden diese eingehalten?
- Welche Prüfungen werden bei der Freigabe durchgeführt?
- Werden Freigabeprotokolle erstellt?
- Wie ist der erstmalige Einsatz einer Programmversion nachweisbar?
- Wird sichergestellt, daß vorangegangene Versionen im Falle eines Fehlers noch einsatzbereit sind?
- Wie ist die Fachabteilung an der Freigabe beteiligt?

### **Schulung**

- Gibt es eine Planung für die Schulung?
- Werden die Anwender bei neuen Verfahrensteilen eingewiesen?

- Stehen aktuelle Benutzerhandbücher zur Verfügung?

#### **Dokumentation**

- Gibt es Dokumentationsrichtlinien? Werden sie eingehalten?
- Wie ist die Verfahrensdokumentation aufgebaut?
- Wird die Erstellung der Dokumentation maschinell gestützt?
- Ist die Dokumentation aktuell verfügbar?
- Sind die Schnittstellen zu anderen Verfahren dargestellt?
- Sind alle Programme dokumentiert?

### 3 Betrieb

#### **Dialogverfahren**

- Welche Dialogprogramme werden eingesetzt ?
- Gibt es Planungen für eine Weiterentwicklung?
- Gibt es Wirtschaftlichkeitsuntersuchungen?
- Wie ist die Datenermittlung, Dateneingabe und Datenabfrage organisiert?
- Welche Fachbereiche sind zuständig?
- Welche Arten von Urbelegen gibt es?
- Werden aus Urbelegen gesonderte Eingabebelege erstellt?
- Sind die Daten auf den Eingabebelegen vollständig oder muß vor der Dateneingabe eine weitere Sachbearbeitung vorgenommen werden?
- Sind die Eingabebelege eindeutig gekennzeichnet?
- Welche Plausibilitätskontrollen sind eingerichtet?
- Welche Fehler werden bei der Dateneingabe schon erkannt? Wie werden diese Fehler behoben?
- Was geschieht mit nicht unmittelbar korrigierbaren Fehlern?
- Wie ist sichergestellt, daß alle Eingabefehler bereinigt werden?
- Wie wird sichergestellt, daß die Eingabebelege vollständig sind?
- Welche Maßnahmen zur Datensicherheit, z. B. Passwortschutz, Terminalabschaltung, sind für die Dateneingabe getroffen?
- Wie ist die Betreuung der Dialogverfahren geregelt?



- Wie ist die Abstimmung mit dem Rechenzentrum gewährleistet, z. B. bei Antwortzeitproblemen?
- Wird der Betrieb regelmäßig im Hinblick auf Sicherheitsverstöße und Systemverhalten überwacht? Welche Softwarewerkzeuge stehen dafür zur Verfügung?
- Welche Zugriffsrechte haben die Operatoren, Systemverwalter und Datenbankverwalter?
- Welche Fachbereiche nutzen Datenauswertungs- und Datenabfragemöglichkeiten?
- Welche Softwarewerkzeuge stehen dafür zur Verfügung?
- Wie sind die Zugriffsrechte geregelt? Werden Zugriffe überwacht?
- Wie häufig werden die Auswertungs- und Abfragemöglichkeiten genutzt?
- Wie beurteilen die Fachbereiche das Verfahren im Hinblick auf Bedienbarkeit, Datenaktualität, Antwortzeit, Stabilität?

#### **Batch-Verfahren**

- Welche Batch-Verfahren werden eingesetzt?
- Wer ist für den Betrieb der Verfahren zuständig? Wie sind die Kompetenzen gegeneinander abgegrenzt? Ist eine Funktionentrennung gewahrt?
- Welche Arbeitsanweisungen stehen zur Verfügung?
- Welche Zeitpläne für die Verarbeitung bestehen?
- Ist Zeit für Wiederholäufe eingeplant?
- Welche Maßnahmen sind für einen Fehlerfall vorgesehen?
- Ist eine Teilwiederholung von Verarbeitungsläufen möglich? Sind diese Möglichkeiten dokumentiert?
- Sind Softwarewerkzeuge zur Steuerung der Verarbeitungsabläufe eingesetzt? In welchem Umfang werden sie eingesetzt?
- Wie werden die Verarbeitungsergebnisse kontrolliert?
- Werden Verarbeitungsprotokolle aufbewahrt?
- Wer kann Aufträge zum Ändern von Verarbeitungsläufen erteilen?
- Welche Regelungen bestehen für die Datensicherung?
- Wieviele Sicherungsgenerationen gibt es?
- Wie ist das Operating organisiert?
- Bestehen Handlungsanweisungen für das Anhalten und Starten der Rechensysteme?

- Welche Datennachbereitung ist bei dem Verfahren erforderlich? Wie ist diese organisiert?
- Wie ist die Vollständigkeit der Datenausgabe sichergestellt?
- Wie werden Datenlisten verteilt?
- Welche Listen erhält die Fachabteilung? Wie werden sie dort behandelt? Werden die Unterlagen auch ausgewertet?
- Wie wird sichergestellt, daß Verarbeitungsfehler bereinigt werden?

#### 4 Datensicherheit/Datenschutz

- Sind personenbezogene Daten gespeichert, die dem Datenschutzgesetz unterliegen?
- Gibt es einen Datenschutzbeauftragten?
- Ist das Verfahren vom Datenschutzbeauftragten genehmigt?
- Wie ist der Zugriffsschutz auf die Datenbank und die Hilfsdateien organisiert?
- Wer verwaltet das Datenschutzsystem?
- Wieviel Personen haben Berechtigung für die Kontrolle des Datenschutzsystems?
- Wie ist die Funktionentrennung geregelt?
- Haben Programmierer Zugriff auf die Produktionsdaten?
- Haben Programmierer während des Test- und Freigabeverfahrens Zugriff auf Programme?
- Was ist für den Fall unerlaubter Zugriffsversuche vorgesehen?

## Beispiel 4:

### Beschaffung von Arbeitsplatzcomputern

#### Inhalt des Themen- und Fragenkataloges:

- 1 Vergabe
- 2 Vertragsabwicklung

#### 1 Vergabe

- Gibt es ein übergeordnetes Konzept für die Beschaffung von Arbeitsplatzcomputern (APC), z. B. mit Vorgaben für die Ausstattung oder die Beschaffung aus Rahmenverträgen?
- Welche Vorschriften und Regelungen werden von den beschaffenden Stellen angewandt?
- Gibt es gesonderte Regelungen für die APC-Beschaffung?
- Aus welchen Haushaltsstellen werden APC beschafft?
- Über welche Verträge wurden die APC beschafft?
- Welche Stellen sind an einer Beschaffung beteiligt?
- Wer nimmt die Fachaufsicht bei der Beschaffung von APC wahr?
- Ist eine ausreichende fach- und systemtechnische Betreuung der Anwender sichergestellt? Wie wird sichergestellt, daß der Anwender das APC-System im erforderlichen Umfang nutzen kann?
- Welche Voraussetzungen müssen vorliegen, damit eine Beschaffung eingeleitet oder ein entsprechender Vertrag geschlossen werden kann?
- Durch welche Stellen wird eine APC-Beschaffung eingeleitet?
- Welche Formen der Vergabe werden praktiziert?
- In welchen Fällen kamen Beschaffungsverträge zustande, ohne daß ein Wettbewerb durchgeführt wurde?
- Liegen für Angebotsbewertungen Kriterienkataloge vor?
- Stützen sich die Vergaben auf funktionale Anforderungen?
- Welche Stellen werden bei der Vertragsgestaltung beteiligt?

- Wie wird sichergestellt, daß alle zu beteiligenden Stellen bei der Vertragsentstehung auch beteiligt werden?
- Wie ist die Mitwirkung der Fachbereiche geregelt?
- Von welcher Stelle und wie werden die Anforderungen in eine technische Leistungsbeschreibung umgesetzt?
- Wer stellt die technische Angemessenheit und die Erfüllung der Leistungsanforderungen der zu beschaffenden APC fest?
- Wie wird die Wirtschaftlichkeit der Beschaffung festgestellt?
- Wie ist sichergestellt, daß die Beschaffung koordiniert wird?
- Wie wird sichergestellt, daß die einzelnen Arbeitsplätze bedarfsgerecht mit Standardsoftware ausgestattet sind?
- Fanden Preisverhandlungen statt?
- Wieviele APC werden über Rahmenverträge beschafft?
- Welche Menge wurde bei den Rahmenverträge zugrunde gelegt und wie wurde sie ermittelt?
- Nach welchen Kriterien wird die Entscheidung für die Beschaffungsart Kauf oder Miete bei der Beschaffung von APC getroffen?
- Welche Laufzeit haben die Rahmenverträge für APC?
- Liegen dafür Wirtschaftlichkeitsberechnungen vor?
- Sind in den Verträgen Mengen und Preisstaffelungen vereinbart?
- Wird in den Beschaffungsverträgen eine Funktionsprüfung und eine Abnahme vereinbart?
- Welche Regelungen sind für die Geräteinstallation, die Schulung, die Lieferung neuer Softwareversionen sowie die Wartung und Reparatur getroffen worden?

## 2 Vertragsabwicklung

- Wie wird die Preisangemessenheit der Rahmenverträge überwacht?
- Wie werden Rahmenverträge für APC an den Stand der Technik und die Preisentwicklung angepaßt?
- In welchen Zeitintervallen werden Rahmenverträge auf technischen Fortschritt und Preisentwicklung geprüft?
- Werden Funktionsprüfungen durchgeführt und wird darüber ein Protokoll erstellt? Wer führt die Funktionsprüfungen durch?

- Wie wird sichergestellt, daß Änderungen des Leistungsumfanges oder Preisänderungen nur auf vertraglicher Grundlage, z.B. über einen Änderungsvertrag, erfolgen?
- Wie werden Nachweise über die beschafften APC geführt? Wird die Konfiguration der eingesetzten APC einschließlich der verwendeten Software dokumentiert?

## Beispiel 5:

### Einsatz lokaler Netze

#### Inhalt des Themen- und Fragenkataloges:

- 1 Planungsziele/Konzeption
- 2 Ist-Aufnahme
- 3 Durchführung
  - Technischer Teil
  - Netzwerk-Topologie
  - Netzserver-Ausstattung
  - Software
  - Organisatorischer Teil
- 4 Kosten
- 5 Nutzung

#### 1 Planungsziele/Konzeption

- Welche Anforderungen bestehen seitens der Fachabteilung?
- Wurden die zu erreichenden Ziele quantitativ festgelegt, z. B. Einsparungen an Mitteln oder Personal, Lastannahmen, Antwortzeiten?
- Wurden bei der Erstellung der Anforderungen die Benutzer beteiligt?
- Wurde die Gesamtrealisierung in einzelnen Arbeitsabschnitten durchgeführt?
- Wurde die Planung während der Realisierung geändert?
- Wurde ein organisatorisches Konzept erstellt, in dem z. B. die zu unterstützenden Aufgaben und die vorgesehenen Arbeitsabläufe beschrieben sind?
- Welche Standardisierungsaspekte wurden bei der Planung berücksichtigt?
- Wurden Abweichungen von Standards vorgesehen?
- Welche Rahmenvorgaben übergeordneter Stellen lagen den Planungen zugrunde?
- Wurde das Netz auch dazu geplant, mit Großrechenanlagen zu kommunizieren und mit welchen Verfahren soll kommuniziert werden?
- Wurden die Aspekte der Verfügbarkeit, Datenintegrität und Sicherheit (Zugangs- und Zugriffsschutz) planerisch berücksichtigt?
- Welche der geplanten Aufgaben könnten ohne eine Vernetzung abgewickelt werden?

- Wurden externe Berater hinzugezogen?
- Wie wurde die notwendige und auch künftig ausreichende Leistungskapazität ermittelt, z. B. für Übertragung von Text, Grafik und Bildern?

## 2 Ist-Aufnahme

- Welcher Realisierungsgrad ist zum Zeitpunkt der örtlichen Erhebungen erreicht, insbesondere bei der Ausstattung der Hardware, dem Einsatz von Standardsoftware, der Entwicklung von Anwendersoftware sowie der Schulung?
- Welche Aufgaben werden derzeit in welchen Organisationseinheiten mit Hilfe des Netzes abgewickelt?
- Entspricht der Realisierungsgrad der Planung?
- Bestehen inhaltliche Abweichungen von der Planung?
- Liegen diese Abweichungen in Verzögerungen bei der Ausstattung der Hardware, dem Einsatz von Standardsoftware, der Entwicklung von Anwendersoftware oder der Schulung?
- Ist die Nutzung des Netzes eingeschränkt und welche Gründe gibt es dafür, z. B. fehlende organisatorische Anpassung, Akzeptanzprobleme, unvollständige Datensammlungen, fehlende Datenverbindungen zu Kommunikationspartnern?
- Welche der in der Planung dargestellten Ziele wurden erreicht?
- Sind diese Ziele (teilweise) durch andere Maßnahmen, z. B. Umorganisation, Schulung, Aufgabenbeschreibung und Personalverstärkung, erreicht worden?
- Ist eine Erfolgskontrolle durchgeführt worden und welches Ergebnis hatte sie?

## 3 Durchführung

### Technischer Teil

- Welche Netzwerk-Management Funktionen sind vorhanden, z. B. Datensicherung, Wartung, Fehlerdiagnose?
- Bestehen Schnittstellen zu anderen lokalen oder öffentlichen Netzen?
- Wird eine Netzwerk-Management-Software eingesetzt?
- Welche Betriebssysteme werden eingesetzt?
- Wie groß sind die Antwortzeiten und die Stabilität des Systems?

### **Netzwerk-Topologie**

- Welches Übertragungsverfahren wurde gewählt, z. B. Ethernet, Token Ring?
- Welche Arbeitsplätze sind angeschlossen? Sind die angeschlossenen Arbeitsplätze auf mehrere Gebäude oder Grundstücke verteilt?
- An welchen Stellen ist zusätzliche Hardware installiert, z. B. Drucker?
- Welche Kabelarten wurden verwendet?

### **Netzserver-Ausstattung**

- Welche Rechnertypen werden eingesetzt und entsprechen die Erweiterungsmöglichkeiten den jetzigen und absehbaren Anforderungen in Bezug auf Anschluß von Geräten anderer Hersteller, Anschluß von leistungsfähigen externen Speichern sowie Anschluß von zusätzlichen Bildschirmen, Druckern und anderen Peripheriegeräten?
- Wie groß ist die Festplattenkapazität und ist diese ausreichend?
- Wer ist für die Netzwerk-Software zuständig?
- Wie wird die Funktionsfähigkeit des Netzes überprüft?

### **Software**

- Wer ist für Fragen der Software zuständig?
- Ist die eingesetzte Software netzwerkfähig?
- Wird ausschließlich lizenzierte Standardsoftware eingesetzt?
- Werden oder müssen neue Anwendungen entwickelt werden?

### **Organisatorischer Teil**

- Welche Organisationseinheit ist für die Beschaffung von Hard- und Software und für die Erweiterungsplanung zuständig?
- Gibt es einen Netzwerk-Verwalter?
- Wer ist für die Verwaltung der Benutzer des Netzes verantwortlich und welche Aufgaben nimmt er wahr?
- Gab es einen Hauptauftragnehmer, der die Gesamtverantwortung für die Erstellung eines betriebsbereiten Netzes hatte?
- Ist eine fortlaufende und vollständige Dokumentation des Planungs-, Entscheidungs- und Umsetzungsprozesses vorhanden?
- Gab es ein Schulungskonzept?



## 4 Kosten

- Ist die Wirtschaftlichkeit der geplanten Maßnahmen durch entsprechende Untersuchungen nachgewiesen?
- Wie hoch sind die einmaligen Kosten für das Netz, z. B. Leitungen, Leitungverstärker- und Verteiler, Server, APC, Drucker und sonstige Hardware, Netzsoftware, Anwendersoftware sowie Kosten für Installation und Schulung?
- Wie hoch sind die laufenden Kosten für Miete, Wartung und Personal sowie für Server und Netzwerksoftware?
- Wurden Mittel für den weiteren Ausbau des Netzes eingeplant?

## 5 Nutzung

- Wieviel Personal wird zum Betrieb des Netzwerkes benötigt?
- Wofür werden die Kommunikationsmöglichkeiten des Netzes genutzt?
- Gibt es verbindliche Regelungen für die Benutzer des Netzes und wird deren Einhaltung überprüft?
- Wie wird die Betriebsbereitschaft des Netzes im Störfall wiederhergestellt? Welche vertraglichen Regelungen wurden für diesen Fall getroffen?
- Haben die Benutzer eine Ausbildung erhalten, die sie in die Lage versetzt, die Möglichkeiten des Netzes wie geplant zu nutzen?
- Gibt es Erfahrungsberichte über die Nutzung des Netzes und wurden aus dort beschriebenen Schwachstellen Maßnahmen abgeleitet?
- Wurde durch den Einsatz des Netzes die Wirtschaftlichkeit verbessert, z. B. im Hinblick auf
  - verbesserte Personalauslastung,
  - weniger Überstunden und Fehlzeiten,
  - geringere Informationstransportkosten,
  - bessere Qualität der Arbeitsergebnisse,
  - bessere und aktuellere Informationen,
  - höhere Übersichtlichkeit im Arbeitsablauf,
  - geringere Belastung der Mitarbeiter?

## Beispiel 6:

### Notfallplanung

#### Inhalt des Themen- und Fragenkataloges:

- 1 Anforderungen an die Notfallplanung  
Kosten eines Ausfalls  
Maximal tolerierbare Ausfalldauer
- 2 Ermittlung des Kapazitätsbedarfs  
Speicherkapazitäten für Verfahren  
Datenübertragung  
Nachverarbeitung  
Verwaltung des Rechensystems
- 3 Bereitstellung von Ersatzrechensystemen  
Auswahlkriterien  
Technische Bedingungen  
Organisatorische Bedingungen
- 4 Sicherungskonzept und Wiederanlaufmaßnahmen  
Verfahrensdaten  
Verfahrenssoftware  
Systemsoftware  
Auslagerungsarchiv
- 5 Wiederanlaufkonzept  
Wiederanlaufaktivitäten  
Durchführung des Wiederanlaufs
- 6 Notfallorganisation  
Alarmorganisation  
Schadensaufnahme  
Wiederanlauforganisation
- 7 Tests und Übungen

#### 1 Anforderungen an die Notfallplanung

##### Kosten eines Ausfalls

- Wie hoch ist der Schaden bei Ausfall des Rechensystems?
- Nach welchen Kriterien ist die Berechnung angestellt worden?

### **Maximal tolerierbare Ausfalldauer**

- Welche Verfahren werden eingesetzt?
- Nach welchen Gesichtspunkten wird die maximal tolerierbare Ausfalldauer erhoben?
- Wie wird gewährleistet, daß Änderungen, die die Verfügbarkeitsanforderungen betreffen, berücksichtigt werden?
- Was beinhalten die Verfügbarkeitsanforderungen eines Verfahrens, z. B. Antwortzeiten, Datenaufkommen in Spitzenzeiten und im normalen Betrieb?
- Gibt es Kriterien für die Zuordnung von Verfahren zu Prioritätsstufen?
- Werden die Anforderungen für neue Verfahren und Änderungen eingeführter Verfahren erhoben?
- Wird die Gültigkeit bestehender Anforderungen kontrolliert?
- Gibt es verbindliche Regelungen zur Erhebung und Kontrolle der Anforderungen?

## **2 Ermittlung des Kapazitätsbedarfs**

### **Speicherkapazitäten für Verfahren**

- Welche Kriterien werden bei der Ermittlung des Bedarfs an Speicherkapazitäten für die einzelnen Verfahren einbezogen ?
- Wird der Kapazitätsbedarf kontrolliert?
- Wird bei neuen Verfahren oder Änderungen an bestehenden Verfahren der Kapazitätsbedarf für das Notfallkonzept erhoben?
- Gibt es verbindliche Richtlinien zur Erhebung des Kapazitätsbedarfs?
- Sind die Ergebnisse der Bedarfsanalyse dokumentiert?
- Wird die Dokumentation regelmäßig aktualisiert?

### **Datenübertragung**

- Wird der Datenübertragungs-Bedarf für jedes Verfahren ermittelt?
- Wird bei der Berechnung der Minimalkonfiguration zwischen Zeiträumen der Spitzenbelastung des Netzes und dem Normalbetrieb unterschieden?
- Wird der Kapazitätsbedarf kontrolliert?
- Wird bei neuen Verfahren oder Änderungen an bestehenden Verfahren der Kapazitätsbedarf für das Notfallkonzept erhoben?

- Gibt es verbindliche Regelungen zur Erhebung des Kapazitätsbedarfs?
- Sind die Ergebnisse der Bedarfsanalyse dokumentiert?
- Wird die Dokumentation regelmäßig aktualisiert?

#### **Nachverarbeitung**

- Wird für jedes Verfahren der Kapazitätsbedarf an Druckereinrichtungen und Nachverarbeitungsanlagen erhoben?
- Wird für jedes Verfahren der Bedarf an Verbrauchsmaterial erhoben?
- Wird ein bestimmtes Kontingent von Verbrauchsmaterial ausgelagert?
- Gibt es spezielle Verarbeitungsverfahren zur Erzeugung von Druckausgaben?
- Gibt es Verfahren, für die eine Nachverarbeitung der Druckausgaben erforderlich ist, z. B. Mikroverfilmung, Separierer, Kuvertiermaschinen, Poststraßen, Frankiermaschinen?
- Wird der Kapazitätsbedarf kontrolliert?
- Wird bei neuen Verfahren oder Änderungen an Verfahren der Kapazitätsbedarf für das Notfallkonzept erhoben?
- Gibt es verbindliche Richtlinien zur Erhebung des Kapazitätsbedarfs?
- Sind die Ergebnisse der Bedarfsanalyse dokumentiert?
- Wird die Dokumentation regelmäßig aktualisiert?

#### **Verwaltung des Rechensystems**

- Werden zur Verwaltung des Rechensystems zusätzliche Hard- und Softwarekapazitäten benötigt, z. B. Terminals, Konsolen, Drucker?
- Ist die Speicherplatzbelegung des Ersatzrechensystems vorbereitet?
- Ist die Belegung der Peripherie, die für den Wiederanlauf benötigt wird, organisiert?
- Wird der Kapazitätsbedarf kontrolliert?
- Wird bei Änderungen im Bereich der Administration der Kapazitätsbedarf für das Notfallkonzept erhoben?
- Gibt es verbindliche Richtlinien zur Erhebung des Kapazitätsbedarfs?
- Sind die Ergebnisse der Bedarfsanalyse dokumentiert?
- Wird die Dokumentation regelmäßig aktualisiert?

### 3 Bereitstellung von Ersatzrechensystemen

#### **Auswahlkriterien**

- Welche Kriterien sind bei der Auswahl eines Ersatzrechensystems zugrundegelegt worden, z. B. Kosten des möglichen Schadens, Kosten für zusätzliches Gerät, Kosten für Leitungsumschaltungen, Kosten für zusätzliches Personal, organisatorischer Aufwand, Verfügbarkeit in der tolerierbaren Ausfalldauer, Fehler-, Störungs- oder Ausfallstatistiken, Beschaffungszeiten?
- Welche Alternativen wurden berücksichtigt, z. B. komplettes, voll funktionsfähiges Ersatzsystem, Beschaffung von Systemen und Komponenten im Bedarfsfall?

#### **Technische Bedingungen**

- Ist eine Basisausstattung in Minimalkonfiguration verfügbar, mit der die Verfahren höchster Priorität betrieben werden können?
- Wird bei Bedarf die Basiskonfiguration erweitert?
- Sind die versorgungstechnischen Anforderungen festgelegt?
- Werden Änderungen der Anforderungen kontrolliert, z. B. im Hinblick auf die Basisausstattung, die Versorgungstechnik oder die Konfiguration?
- Sind die technischen Vorkehrungen zur Erweiterung der Basiskonfiguration getroffen?

#### **Organisatorische Bedingungen**

- Sind organisatorische Vorkehrungen zur Inbetriebnahme des Ersatzrechensystems getroffen?
- Ist die Zuordnung von Betriebsmitteln geregelt?
- Ist der Einsatz der Peripherie für den Wiederanlauf festgelegt?
- Sind organisatorische Vorkehrungen zur Erweiterung der Basiskonfiguration getroffen, z. B. Verabredungen mit dem Hersteller, Organisation der Beschaffung, Dokumentation der erforderlichen Aktivitäten?
- Ist geregelt, wie Bedarfsänderungen bezüglich des Ersatzsystems erhoben und den zuständigen Stellen mitgeteilt werden?

## 4 Sicherungskonzept und Wiederanlaufmaßnahmen

### Verfahrensdaten

- Werden die Daten jedes Verfahrens gesichert (Bestandsdaten, Änderungsdaten, Schnittstellendaten)?
- Werden die Sicherungsanforderungen von den Fachbereichen festgelegt (Umfang, Häufigkeit, Aufbewahrungsfristen)?
- Werden die Sicherungsanforderungen auf Gültigkeit kontrolliert?
- Mit welcher Methode werden die Verfahrensdaten gesichert, z. B. verfahrensspezifisch, systemweite Voll- oder Teilsicherungen, Differenzsicherungen?
- Wird das gleiche Sicherungsverfahren für den laufenden Produktionsbetrieb genutzt?
- Ist sichergestellt, daß die Sicherungen vollständig sind?
- Erfolgt eine Auslagerung der Datensicherungen? Ist die Zuständigkeit für die Auslagerung eindeutig festgelegt?
- Kann ein Datenbestand gegebenenfalls zurückgesetzt werden?
- Werden die Sicherungen auf Vollständigkeit, Korrektheit und Aktualität geprüft?
- Wird bei neuen Verfahren oder Änderungen an bestehenden Verfahren das Sicherungsverfahren für das Notfallkonzept festgelegt oder überprüft?
- Gibt es verbindliche Richtlinien für die Erstellung und Änderung des Sicherungskonzeptes?
- Ist das Sicherungskonzept dokumentiert?

### Verfahrenssoftware

- Gibt es ein Bestandsverzeichnis der Verfahrenssoftware einschließlich der Versionen?
- Werden Versionsänderungen der Verfahrenssoftware bei Sicherungen besonders berücksichtigt?
- Sind die Abhängigkeiten von Daten und Verfahren bekannt und dokumentiert?
- Ist zu jedem Zeitpunkt definiert, welche Daten- oder Konsistenzverluste in einem Notfall eintreten?
- Wird bei jeder Anwendung verzeichnet, welche Systemsoftware erforderlich ist ?
- Wird das Sicherungskonzept sowie der Wiederanlauf explizit getestet?
- Gibt es verbindliche Richtlinien für Aufbewahrungsfristen?

- Sind die Handbücher und Programmdokumentationen ausgelagert?
- Erfolgt nach jeder Aktualisierung eine erneute Auslagerung?
- Werden das Sicherungskonzept und die Wiederanlaufmaßnahmen kontrolliert?
- Werden bei neuen Verfahren oder Änderungen an bestehenden Verfahren das Sicherungskonzept sowie die Wiederanlaufmaßnahmen überprüft?
- Gibt es verbindliche Richtlinien zur Erstellung eines Sicherungskonzeptes und zur Auswahl von Wiederanlaufmaßnahmen?
- Wird die Dokumentation des Sicherungskonzeptes und der Wiederanlaufmaßnahmen regelmäßig aktualisiert?
- Wird die Dokumentation nach der Änderung ausgelagert?

### **Systemsoftware**

- Gibt es ein aktuelles Bestandsverzeichnis der Systemsoftware?
- Wird die Systemsoftware regelmäßig gesichert?
- Werden die Systemparameter des Betriebssystems und der systemnahen Software regelmäßig gesichert?
- Werden Versionsänderungen der Systemsoftware bei Sicherungen besonders berücksichtigt?
- Müssen Systemparameter für den Wiederanlauf geändert werden? Ist die Parametrisierung vorbereitet?
- Müssen Systemgenerierungen durchgeführt werden?
- Wird das Zugriffsschutzsystem installiert?
- Wird das Sicherungskonzept sowie der Wiederanlauf getestet?
- Sind Aufbewahrungsfristen für die Sicherungen der Systemsoftware festgelegt?
- Existiert eine Aufstellung der täglich durchzuführenden regelmäßigen und zusätzlichen Datenverarbeitungsabläufe?
- Wird die Aufstellung der Datenverarbeitungsabläufe regelmäßig ausgelagert?
- Werden das Sicherungskonzept und die Wiederanlaufmaßnahmen kontrolliert?
- Gibt es verbindliche Richtlinien zur Erstellung des Sicherungskonzeptes und der Auswahl von Wiederanlaufmaßnahmen für systemnahe Software?
- Wird die Dokumentation des Sicherungskonzeptes und der Wiederanlaufmaßnahmen regelmäßig aktualisiert?

### **Auslagerungsarchiv**

- Erfolgt eine Bestandsführung der ausgelagerten Sicherungen, Dokumentationen und Unterlagen?
- Ist der Zugriff auf die Betriebssystem Sicherungen sichergestellt, die im Notfall als erstes eingespielt werden müssen?
- Wann erfolgt eine Auslagerung von Datenträgern?
- Sind die Verantwortlichkeiten und Zuständigkeiten für die Auslagerung und den Zugriff auf die Datensicherungen eindeutig geregelt?
- Ist der Transport der Sicherungsdaträger geregelt und dokumentiert ?
- Sind Verantwortliche für die korrekte und vollständige Auslagerung benannt?
- Gibt es einen geregelten Änderungsdienst für die Auslagerung und Aufbewahrung von Datenträgern ?

## 5 Wiederanlaufkonzept

### **Wiederanlaufaktivitäten**

- Werden neben dem Totalausfall auch Teilausfälle berücksichtigt?
- Sind alle Aktivitäten für einen Wiederanlauf dokumentiert?
- Ist die Reihenfolge der Wiederanlaufaktivitäten an den Prioritäten der Verfahren orientiert?
- Ist die Verfügbarkeit der Datensicherungen sichergestellt?
- Gibt es eine Gesamtaufstellung der erforderlichen Dokumentationen?
- Sind alle benötigten Dokumentationen ausgelagert?

### **Durchführung des Wiederanlaufs**

- Kann anhand der Beschreibungen ein fachkundiger Dritter die Aktivitäten durchführen?
- Sind die Zuständigkeiten zur Durchführung der Aktivitäten eindeutig geregelt?
- Gibt es jeweils benannte Vertreter?
- Ist sichergestellt, daß die Personen erreichbar sind?
- Ist geregelt, wer die Personen in einem Notfall informiert und über welche Kommunikationsmedien dies erfolgt?



## 6 Notfallorganisation

### Alarmorganisation

- Gibt es Alarmpläne für Feuer, Wasser, Klima, Strom, Sabotage, Einbruch/Diebstahl, Bombendrohung?
- Wird zwischen Alarmplänen während der Dienstzeit und außerhalb der Dienstzeit unterschieden?
- Gibt es Alarmpläne für den Betrieb des Rechensystems und für den Wachdienst?
- Gibt es regelmäßige Schulungen für die Personen, die das Rechensystem betreiben?
- Werden die getroffenen Vorkehrungen für eine Alarmierung kontrolliert?
- Besteht ein geregelter Änderungsdienst?
- Sind die Zuständigkeiten für die Kontrolle sowie den Änderungsdienst eindeutig zugeordnet?
- Sind alle getroffenen Vorkehrungen für eine Alarmierung dokumentiert?

### Schadensaufnahme

- Gibt es Schadensmeldungen?
- Sind die Schadensmeldungen auf Teilschäden abgestimmt?
- Ist eindeutig festgelegt, wer für die Ausarbeitung und Erstellung der Schadensmeldungen zuständig ist?
- Ist eindeutig festgelegt, an wen die ausgefüllten Schadensmeldungen weiterzuleiten sind?
- Ist festgelegt, wie die Schadensmeldungen zu interpretieren und auszuwerten sind?

### Wiederanlauforganisation

- Gibt es ein Notfallorganigramm, z.B. mit den Funktionen für Sicherheitsbeauftragte, Bau- und Versorgungstechnik, dezentrale Systeme, Rechenzentrum, Datenübertragung/Netzwerk, systemnahe Software, Verfahrenssoftware, Nachverarbeitung, Logistik, Archiv/Arbeitsvorbereitung oder Organisation?
- Gibt es für jede Funktion eine Aufgabenbeschreibung?
- Gibt es einen Maßnahmenkatalog für Teilausfälle?
- Gibt es einen Notbetrieb zur Änderung von Programmen, einschließlich Test- und Freigabeverfahren?
- Werden die Vorkehrungen der Wiederanlauforganisation kontrolliert?

- Gibt es eine zentrale Stelle, die für die Zusammenführung und Koordination des Sicherheitskonzeptes zuständig ist?
- Ist ein regelmäßiger Änderungsdienst für das Sicherheitskonzept eingeführt?

## 7 Tests und Übungen

- Werden regelmäßige Tests durchgeführt, z. B. Teilstests der Sicherungskonzepte, der Wiederanlaufmaßnahmen oder vollständige Tests mit Echtbetrieb?
- Gibt es eine Testplanung?
- Gibt es Kriterien, nach denen die Testplanung erstellt wird?
- Werden die Tests protokolliert?
- Gibt es eine Nachbesprechung mit definiertem Teilnehmerkreis ?
- Wem werden die Testergebnisse mitgeteilt?
- Wann erfolgt eine Testankündigung?
- Werden Organisationstests durchgeführt (Schreibtischtests)?
- Wird das Testkonzept entsprechend den Ergebnissen des letzten Test angepaßt?

## Beispiel 7:

### Beschaffung von Hardware

#### Vorbemerkung

Die Beschaffung von Hardware kann durch Kauf oder Miete (Herstellermiete oder Leasing) erfolgen. Ob Kauf oder Miete günstiger ist, hängt im wesentlichen von der Nutzungsdauer der zu beschaffenden Geräte ab. Nach einer bestimmten Anzahl von Mietperioden ist am sogenannten Break-even point die Summe der auf den Beschaffungszeitpunkt abgezinsten Mietzahlungen gleich dem Kaufpreis. Überschreitet die (voraussichtliche) Nutzungszeit der Geräte den Break-even point, ist Kauf rechnerisch wirtschaftlicher als Miete (siehe auch Anhang 4). Die wirtschaftliche Beschaffungsart ist jeweils vor der Beschaffung zu ermitteln.

#### Inhalt des Themen- und Fragenkataloges:

- 1 Organisation
- 2 Durchführung
- 3 Kontrolle

#### 1 Organisation

- Erfolgt die Beschaffung zentral oder dezentral?
- Wer koordiniert die Beschaffungsmaßnahmen?
- Liegen Konfigurationsplanung und Beschaffung von Hardware bei einer Stelle?
- Ist festgelegt, wer für Wirtschaftlichkeitsbetrachtungen sowie für die Überwachung der Mietverträge (z. B. Kündigung, Austausch der Hardware) zuständig ist?
- Erhält die Beschaffungsinstanz die erforderlichen Informationen, z.B. zur voraussichtlichen Nutzungsdauer, um Berechnungen durchführen zu können?
- Wer entscheidet über die Beschaffungsart?
- Welche Rahmenvereinbarungen wurden getroffen?

#### 2 Durchführung

- Wird die Entscheidung so dokumentiert, daß man die Gründe für die gewählte Beschaffungsart nachvollziehen kann?

- Werden Verträge auf der Grundlage der BVB abgeschlossen?
- Wird vor einer Beschaffung die günstigste Finanzierungsart anhand von Wirtschaftlichkeitsrechnungen ermittelt?
- Wird bei den Berechnungen mit Abzinsungsfaktoren (Barwert) gerechnet?
- Wird der Break-even point ermittelt?
- Gibt es Regelungen, aus denen hervorgeht, wie und in welchem Umfang Wirtschaftlichkeitsberechnungen durchzuführen sind?
- Anhand welcher Kriterien wird die voraussichtliche Nutzungsdauer der Hardware ermittelt?
- Anhand welcher Kriterien wird entschieden, ob Kauf oder Miete als Beschaffungsart in Frage kommt?
- Werden Beschaffungen im Wettbewerb durchgeführt?
- Sind Rahmenverträge geschlossen?
- Wird geprüft, ob Einzelverträge günstiger sind?
- Werden bei Änderungen eines Vertrages neue Wirtschaftlichkeitsberechnungen durchgeführt?
- Werden Geräte regelmäßig unabhängig vom Bedarf gegen technisch verbesserte Hardware ausgetauscht?
- Enthalten Mietverträge eine Kaufoption?

### 3 Kontrolle

- Welche Unterlagen stehen zur Verfügung, die einen Überblick über Beschaffungsart, Installationsdaten und Nutzungsdauer der Hardware liefern?
- Geht aus der Übersicht auch der Break-even point hervor?
- Werden laufende Mietverträge regelmäßig auf ihre Wirtschaftlichkeit untersucht?
- Wird geprüft, ob es wirtschaftlich ist, bei bestehenden Mietverträgen eine Kaufoption auszuüben?
- Sind die Geräte, für die Mietzahlungen geleistet werden, noch im Einsatz?