Freie und Hansestadt Hamburg

Finanzbehörde

Verwaltungsvorschriften zu § 74 LHO

Vom 16. Dezember 2021

Anzuwenden ab Haushaltsjahr 2022

§ 74
IT-Verfahren

(1) Verfahren der Informationstechnik (IT) für

1. elektronische Anordnungen,
2. Buchungen,
3. Zahlungen,
4. Aufbewahrung von Nachweisen der Buchungen,
5. Geldverwaltung oder
6. Abschlüsse

dürfen nur eingesetzt werden, wenn sie von der für die Finanzen zuständigen Behörde zugelassen wurden. Diese kann im Einvernehmen mit dem Rechnungshof auf das Zulassungserfordernis verzichten. Der Schutz des Staatsvermögens vor unzulässigen Eingriffen sowie die Zuverlässigkeit, Vollständigkeit und Revisionsfähigkeit der Rechnungslegung sind zu gewährleisten.

(2) Die für die Finanzen zuständige Behörde stellt die IT-Verfahren zur Verfügung, die für das Haushalts-, Kassen- und Rechnungswesen der Freien und Hansestadt Hamburg notwendig sind. Sie kann technische Hilfstätigkeiten durch andere Verwaltungsträger verrichten lassen. Technische Hilfstätigkeiten sind insbesondere Rechenzentrumsleistungen, die Erstellung, Anpassung und Pflege von Software, technisches Monitoring, technische Analyse von Fehlern und auf diese Tätigkeiten bezogene Beratungsleistungen. Die technischen Hilfstätigkeiten des beauftragten Verwaltungsträgers sind der Freien und Hansestadt Hamburg zuzurechnen. Es ist sicherzustellen, dass die technischen Hilfstätigkeiten entsprechend den fachlichen Weisungen der für die Finanzen zuständigen Behörde verrichtet werden.

Auf Grund von § 70 Absatz 3 in Verbindung mit § 11 LHO erlässt die Finanzbehörde nach Anhörung des Rechnungshofs auf Grund von § 96 Absatz 1 LHO und Herstellung des Einvernehmens nach § 70 Absatz 3 LHO folgende Verwaltungsvorschriften:

Zu § 74:

Inhalt

Abschnitt I Allgemeine Bestimmungen 5
1 Anwendungsbereich 5
1.1 Einsatz von IT-Verfahren 5
1.2 Änderung von IT-Verfahren 5
2 Verantwortliche Stelle 6
2.1 Grundsatz 6
2.2 Behördenübergreifend eingesetzte IT-Verfahren 6
2.3 Einsatz von IT-Verfahren durch Dritte 6
3 Nachweis der Einhaltung der Standards 6

Abschnitt II Standards 7
4 Risikoanalyse 7
4.1 Inhalt der Risikoanalyse 7
4.2 Risikoidentifikation 7
4.3 Risikobewertung 8
4.4 Risikosteuerung und -kontrolle 9
4.5 Überprüfung der Risikoanalyse 9
5 IT-Sicherheit 10
5.1 Freigaberichtlinie 10
5.2 Integrität gespeicherter elektronischer Daten und Dokumente 10
5.3 Rechenzentren 10
5.4 Schutzmaßnahmen gegen System- und Programmfehler sowie Sicherheitslücken 10
6 Abgrenzung der Verantwortungsbereiche 10
6.1 Funktionentrennung 10
6.2 Berechtigungen 11
6.2.1 Anforderungen an die Berechtigungsverwaltung 11
6.2.2 Berechtigungskonzept 12
6.2.2.1 Inhalt des Berechtigungskonzeptes 12
6.2.2.2 Kontrolle der Einhaltung des Berechtigungskonzepts 12
7 Verfahrenszugriff 12
7.1 Zugriffskontrolle 12
7.2 Passwortschutz 13
8 Richtigkeit und Vollständigkeit der erfassten und verarbeiteten elektronischen Daten und Dokumente 13

8.1 Datenerfassung ... 13
8.1.1 Definition ... 13
8.1.2 Anforderungen an die Datenerfassung ... 13
8.1.2.1 Manuelle Eingabe von Daten ... 13
8.1.2.1.1 Bescheinigung der richtigen und vollständigen manuellen Datenerfassung ... 13
8.1.2.1.2 Prüfung der erfassten Daten ... 14
8.1.2.2 Elektronische Erfassung von Papierdokumenten ... 14
8.1.2.3 Übernahme von elektronischen Daten und Dokumenten ... 15
8.1.2.4 Inhaltliche Prüfung erfasster anzuordnender Daten ... 15
8.1.3 Beauftragung Dritter ... 15
8.2 Datenverarbeitung ... 16
8.3 Datenübermittlung ... 16
9 Interne Regelungen und Kontrollen ... 17
9.1 Dienst- oder Fachanweisung ... 17
9.2 Kontrollmaßnahmen ... 17
9.2.1 Grundsatz ... 17
9.2.2 Maßnahmen zur Fehlerbehebung ... 17
9.2.3 Dokumentationspflicht ... 18
10 Revisionsfähigkeit des Verfahrens ... 18
10.1 Nachweis über Geschäftsvorfälle und Prüfbarkeit ... 18
10.2 Dokumentation der Zugriffe ... 18
10.3 Prüfberechtigungen ... 19
10.3.1 Grundsatz ... 19
10.3.2 Ausnahmen ... 19

Abschnitt III Stichprobenkontrollverfahren ... 20
11 Einsatz eines Stichprobenkontrollverfahrens ... 20
11.1 Voraussetzungen ... 20
11.2 Risikoanalyse ... 20
11.3 Verantwortungsübernahme ... 21
11.4 Stichprobenprüfung ... 21
11.5 Dienst- oder Fachanweisung ... 21
11.6 Fehleranalyse und Berichtswesen ... 21
11.7 Änderung der Stichprobe ... 22

Abschnitt IV Zulassung von IT-Verfahren ... 22
12 Prüfungsverfahren und Zulassung ... 22

12.1 Zulassungsantrag 22
12.1.1 Voraussetzungen des Zulassungsantrags 22
12.1.2 Antragsfrist 22
12.2 Zulassung durch die Finanzbehörde 22
12.3 Widerruf der Zulassung 23
13 Unterrichtung des Rechnungshofs 23

Abschnitt V Übergangsbestimmungen 23
14 Noch nicht zugelassene IT-Verfahren 23
15 Zugelassene IT-Verfahren 23
15.1 Grundsatz 23
15.2 Änderung von IT-Verfahren 24
15.3 Änderung von Altverfahren 24
15.4 Überprüfung der Nachweise nach Nr. 3 24

Abschnitt I Allgemeine Bestimmungen

1 Anwendungsbereich

1.1 Einsatz von IT-Verfahren

IT-Verfahren für

- elektronische Anordnungen,
- die Erteilung von Befugnissen nach Nr. 2.4.3 VV zu § 70,
- Buchungen,
- Zahlungen,
- Aufbewahrung von Nachweisen der Buchungen nach Nr. 12 VV zu § 70,
- Geldverwaltung und
- Abschlüsse

dürfen nur eingesetzt werden, wenn sie die nachfolgenden Vorschriften und die Bestimmungen der VV zu den §§ 70 bis 73 einhalten und von der Finanzbehörde nach Nr. 12.2 zugelassen wurden. Ausgenommen von der Zulassungspflicht nach Nr. 12.2 sind die IT-Verfahren, deren Einsatz für die Freie und Hansestadt Hamburg nach § 12 des Gesetzes über die Koordinierung der Entwicklung und des Einsatzes neuer Software der Steuerverwaltung (KONSENS-G) verpflichtend ist. Der Einsatz von IT-Verfahren nach Satz 2 ist dem Rechnungshof anzuzeigen.

Soweit beim Einsatz von IT-Verfahren einzelne Verfahrensschritte manuell erfolgen, sind auf diese die jeweiligen Vorschriften für manuelle Verfahrensschritte anzuwenden.

1.2 Änderung von IT-Verfahren

Die Änderung von IT-Verfahren nach Nr. 1.1 bedarf nur dann der Zulassung der Finanzbehörde, wenn die Änderung zu einer Abweichung von den Standards nach Nrn. 4 bis 10 oder den Bestimmungen der VV zu den §§ 70 bis 73 führt, die nicht bereits von der Finanzbehörde zugelassen wurde. Eine Änderung des IT-Verfahrens liegt auch dann vor, wenn sich ausschließlich manuelle Verfahrensschritte nach Nr. 1.1 Absatz 2 ändern.

Wesentliche Änderungen, die nicht der Zulassung der Finanzbehörde bedürfen, hat die oder der jeweilige Beauftragte für den Haushalt der Finanzbehörde (die für Grundsatzfragen des Kassenrechts zuständige Stelle) und dem Rechnungshof vor deren Umsetzung anzuzeigen. Nr. 3 letzter Absatz ist zu beachten.

2 Verantwortliche Stelle

2.1 Grundsatz

Verantwortlich für die Einhaltung der VV zu den §§ 70 bis 74 und für die Wirtschaftlichkeit des IT-Verfahrens ist die Behörde oder das Amt, die bzw. das das IT-Verfahren einsetzt oder einsetzen will. Dies gilt sowohl für den Einsatz selbst- als auch fremderstellter IT-Verfahren.

2.2 Behördenübergreifend eingesetzte IT-Verfahren

Abweichend von Nr. 2.1 ist bei einem behördenübergreifend eingesetzten Verfahren die Behörde oder das Amt für behördenübergreifende Vorgaben hinsichtlich des IT-Verfahrens verantwortlich, die bzw. das das IT-Verfahren programmiert oder beschafft hat. Für den ordnungsgemäßen Einsatz des IT-Verfahrens auf Grundlage der behördenübergreifenden Vorgaben bleibt die Behörde oder das Amt nach Nr. 2.1 verantwortlich.

2.3 Einsatz von IT-Verfahren durch Dritte

Wird ein IT-Verfahren im Auftrag der Freien und Hansestadt Hamburg durch eine Dritte oder einen Dritten eingesetzt, obliegt die Einhaltung dieser Bestimmungen der Behörde oder dem Amt, die bzw. das das IT-Verfahren für die Freie und Hansestadt Hamburg in Auftrag gegeben hat.

3 Nachweis der Einhaltung der Standards

Die nach Nr. 2 verantwortliche Stelle hat nachzuweisen, dass bei Einsatz des IT-Verfahrens die Standards nach Nrn. 4 bis 10 und die Bestimmungen der VV zu den §§ 70 bis 73 eingehalten werden.

Der Nachweis erfolgt durch

- die Erklärung über die Einhaltung der Bestimmungen der VV zu den §§ 70 bis 74 (siehe Absatz 3),
- die Verfahrensbeschreibung (siehe Absatz 4),
- die Risikoanalyse (siehe Nr. 4),
- das Berechtigungskonzept (siehe Nr. 6.2.2),
- die Dienst- oder Fachanweisung(en) (siehe Nr. 9.1),
- die Freigabeerklärung nach Nr. 5.2 Freigaberichtlinie,
- ggf. die Zulassung nach Nr. 12.2 oder eine vorläufige Erlaubnis zur weiteren Nutzung nach Nr. 12.3 Satz 2 und
- ggf. durch die Dienstanweisung Rücklaufkontrolle (siehe Nr. 6.2 VV zu § 70).

Darüber hinaus sind die Kontrollmaßnahmen nach Nr. 9.2 zu dokumentieren.

Für die Erklärung über die Einhaltung der Bestimmungen der VV zu den §§ 70 bis 74 ist das von der Finanzbehörde herausgegebene Muster zu verwenden.

Die Verfahrensbeschreibung soll einen Überblick über das gesamte IT-Verfahren verschaffen. Dabei sind insbesondere folgende Inhalte darzustellen:

- Hintergrund, Sinn und Zweck sowie voraussichtliches Buchungsvolumen des IT-Verfahrens,
- Maßnahmen zur Gewährleistung der IT-Sicherheit nach Nr. 5,
- Abgrenzung der Verantwortungsbereiche nach Nr. 6.1,
- Verfahrenszugriff nach Nr. 7,
- Prozesse der Datenerfassung, -verarbeitung und -übermittlung nach Nr. 8,
- ggf. der Prozess der Anordnung,
- ggf. der Prozess der Buchung,
- ggf. ein Stichprobenkontrollverfahren nach Nr. 11,
- interne Kontrollmaßnahmen nach Nr. 9.2,
- Maßnahmen zur Gewährleistung der Revisionsfähigkeit nach Nr. 10 sowie
- die Archivierung aufbewahrungspflichtiger Nachweise und die Speicherung aufbewahrungspflichtiger Daten.

Im Übrigen sollen, soweit nicht schon in diesen Verwaltungsvorschriften geregelt, für Inhalt und Aufbau der Nachweise die von der Finanzbehörde herausgegebenen Muster verwendet werden.

Die Nachweise nach Absatz 2 sind auch nach der Zulassung des IT-Verfahrens für Prüfungszwecke vorzuhalten und bei Änderungen des IT-Verfahrens zu überprüfen und entsprechend zu aktualisieren.

Abschnitt II Standards

4 Risikoanalyse

4.1 Inhalt der Risikoanalyse

Die nach Nr. 2 verantwortliche Stelle hat vor Einsatz und Änderung eines IT-Verfahrens die daraus entstehenden Risiken für das Staatsvermögen und für die Zuverlässigkeit, Vollständigkeit und Revisionsfähigkeit der Rechnungslegung zu analysieren und schriftlich zu dokumentieren. Dies erfolgt in vier Schritten:

- Risikoidentifikation,
- Risikobewertung,
- Festlegung der Maßnahmen zur Risikovermeidung oder -minderung (Risikosteuerung) und
- Bewertung der Wirksamkeit der getroffenen Maßnahmen und des verbleibenden Risikos (Risikokontrolle).

4.2 Risikoidentifikation

Es ist für alle manuellen, teil- und vollautomatisierten Arbeitsschritte bei der Anwendung des IT-Verfahrens und bei der Berechtigungsverwaltung jeweils darzulegen, welche Risiken für das Staatsvermögen und die Zu-

verlässigkeit, Vollständigkeit und Revisionsfähigkeit der Rechnungslegung bestehen. Dabei sind insbesondere auch diejenigen Arbeitsschritte zu untersuchen, die zu Ausnahmen im Sinne der Nr. 12.2 Absatz 2 in Verbindung mit dem jeweiligen Ausnahmetatbestand zu den Standards nach Nrn. 4 bis 10 und den Bestimmungen der VV zu den §§ 70 bis 73 führen. Risiken im Hinblick auf die Rechtmäßigkeit des Verwaltungshandelns sind in die Gesamtbeurteilung mit einzubeziehen. Risiken, die zu mittelbaren Schäden führen können, insbesondere Personalkosten zur Beseitigung entstandener Fehler, sind ebenfalls zu berücksichtigen.

Die identifizierten Risiken sind so zu beschreiben, dass sie von nicht am IT-Verfahren beteiligten Personen nachvollzogen werden können. Dabei ist darzulegen, welche materiellen Schäden (insbesondere wirtschaftliche Schäden) und immaterielle Schäden (insbesondere Imageverlust oder Verletzung von Rechtsnormen) bei Eintritt des Risikofalles zu erwarten sind.

4.3 Risikobewertung

Jedes Risiko ist hinsichtlich seiner Eintrittswahrscheinlichkeit und des wahrscheinlichen Ausmaßes eines Schadens bei Risikoeintritt (Schadensausmaß) zu bewerten. Bereits im IT-Verfahren angelegte Sicherheitsmaßnahmen sind dabei noch außer Acht zu lassen.

Führen mehrere voneinander unabhängige Ereignisse gemeinsam zu einer erheblich größeren Gefährdung des Staatsvermögens oder der Zuverlässigkeit, Vollständigkeit oder Revisionsfähigkeit der Rechnungslegung als bei einem isolierten Eintritt des jeweiligen Risikos, sind diese Ereignisse gemeinsam zu bewerten.

Eintrittswahrscheinlichkeit und Schadensausmaß sind in jeweils drei Stufen zu schätzen:

1 - gering,

2 - mittel und

3 - hoch.

Eintritts-wahr-schein-lichkeit	Risikokennzahl		
3 (hoch) größer y %	3	6	9
2 (mittel) x-y %	2	4	6

1 (gering) kleiner x %	1	2	3
Schadens-ausmaß	1 (gering)	2 (mittel)	3 (hoch)

Die Eintrittswahrscheinlichkeit ist durch Intervalle aus Prozentzahlen zu bestimmen. Das Schadensausmaß ist bei einem materiellen Schaden durch Intervalle in Euro-Beträgen und bei einem immateriellen Schaden durch Vorgaben für nicht in Geldbeträgen messbare Risiken festzulegen.

Die Bedingungen für den Eintritt einer Stufe sind durch die nach Nr. 2 verantwortliche Stelle festzulegen und in der Risikoanalyse zu dokumentieren. Die Schätzung ist zu begründen.

Für jedes Risiko ist in einem ersten Schritt eine Risikokennzahl zu ermitteln. Die Risikokennzahl ist das Produkt der Werte für Eintrittswahrscheinlichkeit und Schadensausmaß.

4.4 Risikosteuerung und -kontrolle

Für jedes Risiko ist in einem weiteren Schritt darzulegen, welche Sicherheitsmaßnahmen zur Risikoverringerung vorgesehen sind und wie sich diese Maßnahmen auf Eintrittswahrscheinlichkeit und Schadensausmaß auswirken. Sofern die eingesetzten Sicherheitsmaßnahmen keine Risikoverringerung zur Folge haben, liegt es im Ermessen der nach Nr. 2 verantwortlichen Stelle, über den Einsatz der Sicherheitsmaßnahmen zu entscheiden, es sei denn, es handelt sich dabei um Standardanforderungen nach diesen Verwaltungsvorschriften.

Unter Gewichtung der neu berechneten Risikokennzahl ist ggf. darzulegen, aus welchen Gründen auf weitergehende Sicherheitsmaßnahmen verzichtet wird und das verbleibende Risiko akzeptiert wird. Dabei sind die durch das verbleibende Risiko bedingten möglichen Schäden gegen den Aufwand zur Erhöhung des Schutzes des Staatsvermögens sowie des Schutzes der Zuverlässigkeit, Vollständigkeit und Revisionsfähigkeit der Rechnungslegung im Rahmen des IT-Verfahrens abzuwägen.

4.5 Überprüfung der Risikoanalyse

Die nach Nr. 2 verantwortliche Stelle hat die Risikoanalyse mindestens alle zwei Jahre daraufhin zu überprüfen, ob die Identifikation und Bewertung der Risiken sowie die zur Risikominderung getroffenen Maßnahmen im Hinblick auf die mit der Anwendung des IT-Verfahrens gewonnenen Erkenntnisse weiterhin zutreffend sind. Die Überprüfung und ihr Ergebnis sind zu dokumentieren.

Sofern das Risiko gegenüber der vorherigen Risikoanalyse höher bewertet wird, ist die Risikoanalyse anzupassen und ggf. sind Maßnahmen zur Verringerung des Risikos zu ergreifen. Nr. 1.2 ist zu beachten.

5 IT-Sicherheit

5.1 Freigaberichtlinie

Die Freigaberichtlinie in der jeweils geltenden Fassung ist zu beachten.[1]

5.2 Integrität gespeicherter elektronischer Daten und Dokumente

IT-Verfahren dürfen nur eingesetzt werden, wenn hinreichende Vorkehrungen gegen den Verlust und die Manipulation gespeicherter elektronischer Daten und Dokumente, gegen unberechtigten Zugriff sowie gegen Systemfehler getroffen sind.

5.3 Rechenzentren

Die IT-Verfahren dürfen ausschließlich durch Rechenzentren betrieben werden, deren Informationssicherheit auf Basis von IT-Grundschutz durch das Bundesamt für Sicherheit in der Informationstechnik (BSI) zertifiziert ist.

Die Finanzbehörde (die für Grundsatzfragen des Kassenrechts zuständige Stelle) kann hiervon im Einvernehmen mit dem Rechnungshof eine Ausnahme zulassen, wenn eine gleichwertige Sicherheit, z. B. durch andere Zertifizierungen, gewährleistet ist. Die Gleichwertigkeit ist durch die verantwortliche Stelle zu begründen.

5.4 Schutzmaßnahmen gegen System- und Programmfehler sowie Sicherheitslücken

Es ist durch den Abschluss von Wartungsverträgen oder auf andere Weise, z. B. mittels Service Level Agreements, sicherzustellen, dass entstehende oder sichtbar werdende System- und Programmfehler sowie Sicherheitslücken unverzüglich beseitigt werden.

6 Abgrenzung der Verantwortungsbereiche

6.1 Funktionentrennung

Beim Einsatz von IT-Verfahren sind die Verantwortungsbereiche der am Verfahren beteiligten Personen und Stellen festzulegen und gegeneinander abzugrenzen. Insbesondere sind jeweils voneinander zu trennen

- die in Nr. 3.5 sowie in Nr. 4 der Freigaberichtlinie genannten Funktionen,
- die Beantragung sowie die Erteilung von Berechtigungen (Nr. 6.2.1),
- die Erfassung sowie die Prüfung von Berechtigungen im Rahmen der Berechtigungsverwaltung (Nr. 6.2.1),
- die Erfassung nach Nr. 8.1.2.1.1 sowie die Prüfung der erfassten Daten nach Nr. 8.1.2.1.2,

[1] Freigaberichtlinie vom 4. April 2005 (MittVw Seite 46) in der Fassung vom 18. November 2010 (MittVw Seite 189) auf https://fhhportal.ondataport.de/websites/1007/verwaltungsvorschriften/itvorschriften/Documents/Freigabe%20Richtlinie%2011.300.pdf

- die Feststellung der rechnerischen und der sachlichen Richtigkeit (Nrn. 2.4.2.1 und 2.4.2.2 VV zu § 70) sowie die Anordnung (Nr. 2.4.2.5 VV zu § 70),
- die Stammdatenpflege, die Buchführung (z. B. Personenkontenbuchführung) sowie die Abwicklung des Zahlungsverkehrs (Nr. 9.2 VV zu § 70),
- die Erfassung nach Nr. 11.2.1 Absatz 1 VV zu § 70 sowie die Prüfung nach Nr. 11.3 VV zu § 70 sowie
- im Rahmen der Rücklaufkontrolle die Beteiligten an den zu prüfenden Fällen sowie die Beteiligten an der Auswahl der Stichprobe und der Prüfung der Fälle (Nr. 6.2 VV zu § 70).

Sind Daten oder Dokumente von einer zweiten Person zu prüfen, ist durch systemtechnische Vorkehrungen zu gewährleisten, dass

- diese die zu prüfenden Daten und Dokumente entweder nicht ändern kann oder
- die von ihr geänderten Daten erneut von einer anderen hierzu berechtigten Person geprüft werden.

Das gilt auch für den Fall, dass die zweite Person die Daten oder Dokumente im Rahmen ihrer Prüfung nach Nr. 2.4.2.5 VV zu § 70 ändert: Die vollständigen Daten (die von ihr geänderten Daten sowie die unveränderten Daten) sind von ihr auf rechnerische und sachliche Richtigkeit nach Nrn. 2.4.2.1 und 2.4.2.2 VV zu § 70 zu prüfen und von einer anderen zur Anordnung nach Nr. 2.4.3.3 VV zu § 70 befugten Person anzuordnen.

Soweit die rechnerische und sachliche Richtigkeit nicht vollautomatisiert festgestellt wird und nicht vollautomatisiert angeordnet wird, ist sicherzustellen, dass die Anordnungsbefugten nur Geschäftsvorfälle erhalten, zu denen von dazu befugten Personen die rechnerische und sachliche Richtigkeit festgestellt worden ist, und dass nur Anordnungen von dazu befugten Personen an die für Buchungen zuständige Stelle oder an das zentrale Buchführungssystem zur automatisierten Buchung gegeben werden.

6.2 Berechtigungen

6.2.1 Anforderungen an die Berechtigungsverwaltung

Berechtigungen im IT-Verfahren dürfen nur eingerichtet werden, soweit dies zur Aufgabenerfüllung zwingend erforderlich ist (Prinzip der minimalen Berechtigung). Für die Einrichtung und den Entzug von Berechtigungen ist ein Antragsverfahren festzulegen. Pro Person soll nur eine Kennung vergeben werden. Die Erfassung der Berechtigungen im IT-Verfahren ist durch eine zweite Person zu prüfen. Die Erfassung und die Prüfung der Erfassung sind im IT-Verfahren zu dokumentieren.

Nr. 2.4.3.2.3 Absatz 2 und Nr. 2.4.3.3.3 Absatz 2 VV zu § 70 sind zu beachten. Die Verwaltung von Berechtigungen, insbesondere die Identität der Personen, die die Berechtigungen zuweisen und denen die Berechtigungen zugewiesen werden, ist im IT-Verfahren zu dokumentieren.

Das IT-Verfahren muss sicherstellen, dass zu jedem Zeitpunkt festgestellt werden kann, welche Personen, einschließlich Administratoren und andere Systemverwalter, zu welchem Zeitpunkt mit welchen Berechtigungen ausgestattet gewesen sind.

6.2.2 Berechtigungskonzept

6.2.2.1 Inhalt des Berechtigungskonzeptes

Die nach Nr. 2 verantwortliche Stelle hat vor Einsatz eines IT-Verfahrens ein Berechtigungskonzept zu erstellen. Darin ist festzulegen,

- welche Zugriffsrechte (Musterrollen, Berechtigungen) eingerichtet werden,
- für welche Funktionen die Zugriffsrechte eingerichtet werden,
- wie die Einrichtung und der Entzug von Berechtigungen erfolgt,
- wie die Berechtigungsverwaltung dokumentiert und
- wie die Kontrolle der Einhaltung des Berechtigungskonzeptes durchgeführt wird.

6.2.2.2 Kontrolle der Einhaltung des Berechtigungskonzepts

Es ist eine verantwortliche Person oder eine Organisationseinheit zu bestimmen, die die Einhaltung des Berechtigungskonzeptes kontrolliert.

Die verantwortliche Person prüft stichprobenweise, ob die Vergabe von Berechtigungen inhaltlich richtig erfolgt und ordnungsgemäß dokumentiert worden ist. Bestehen Anhaltspunkte, dass bei der Vergabe von Berechtigungen Fehler aufgetreten sind, ist die Berechtigungsvergabe unverzüglich zu berichtigen.

Die für die Berichtigung zuständige Person, die nicht mit der für die Durchführung der Kontrolle der Einhaltung des Berechtigungskonzeptes zuständigen Person identisch sein darf, ist über die Anhaltspunkte elektronisch oder schriftlich zu informieren. Sie prüft, ob die fehlerhafte Berechtigung gelöscht werden muss oder der Fehler auf andere Weise beseitigt werden kann.

Die Kontrolle der Einhaltung des Berechtigungskonzeptes ist mindestens alle zwei Jahre durchzuführen. Das Ergebnis der Prüfung und die Information der die Einhaltung des Berechtigungskonzeptes kontrollierenden Person an die für die Berichtigung zuständige Person über die Anhaltspunkte sind zu dokumentieren.

7 Verfahrenszugriff

7.1 Zugriffskontrolle

Beim Einsatz von IT-Verfahren ist sicherzustellen, dass eine Zugriffskontrolle gewährleistet ist und in den Arbeitsablauf nicht unbefugt eingegriffen werden kann.

7.2 Passwortschutz

Wird der Zugriff auf ein IT-Verfahren durch ein Passwort geschützt, sind die Vorgaben der Passwortrichtlinie[2] in der jeweils geltenden Fassung einzuhalten. Dabei ist es ausreichend, wenn die Zugriffsberechtigung beim Aufruf des IT-Verfahrens automatisiert anhand der aktiven Endgeräte-Benutzerkennung (z. B. durch Single Sign On unter Verwendung des Active-Directory-Passwortes im FHHNET) geprüft wird.

8 Richtigkeit und Vollständigkeit der erfassten und verarbeiteten elektronischen Daten und Dokumente

8.1 Datenerfassung

8.1.1 Definition

Datenerfassung ist die Übernahme von Daten und Dokumenten in ein IT-Verfahren, um diese weiter zu verarbeiten und/oder aufzubewahren. Sie kann insbesondere erfolgen durch

- manuelle Eingabe von Daten nach Nr. 8.1.2.1,
- elektronische Erfassung von Papierdokumenten nach Nr. 8.1.2.2 oder
- Übernahme von elektronischen Daten und Dokumenten nach Nr. 8.1.2.3.

Die Einrichtung von Berechtigungen (siehe Nr. 6.2) ist keine Datenerfassung.

8.1.2 Anforderungen an die Datenerfassung

8.1.2.1 Manuelle Eingabe von Daten

8.1.2.1.1 Bescheinigung der richtigen und vollständigen manuellen Datenerfassung

Manuell einzugebende Daten sind richtig und vollständig im IT-Verfahren zu erfassen.

Die Richtigkeit und Vollständigkeit der manuellen Datenerfassung ist nach Nr. 2.5.2.1 VV zu § 70 zu bescheinigen, es sei denn

- die Datenerfassung ist dem Anordnungsprozess vorgelagert und die Richtigkeit und Vollständigkeit der erfassten Daten werden bei der Feststellung und Anordnung überprüft oder
- die buchende Person erfasst die Daten der Anordnung und die Buchungsdaten im Rahmen der Buchführung nach Abschnitt III der VV zu § 70 (vgl. auch Nr. 11.3 VV zu § 70).

Die Bescheinigung kann mehrere Geschäftsvorfälle umfassen. Mit der Bescheinigung übernimmt die oder der Beschäftigte die Verantwortung für die richtige und vollständige Erfassung der Daten.

[2] Die Passwortrichtlinie ist unter https://fhhportal.ondataport.de/websites/1007/verwaltungsvorschriften/itvorschriften/Seiten/default(standard).aspx abrufbar.

Entfällt die Bescheinigung, ist in einer Dienst- oder Fachanweisung (Nr. 9.1) auf die übernommene Verantwortung für die richtige und vollständige Datenerfassung hinzuweisen.

8.1.2.1.2 Prüfung der erfassten Daten

Ist die manuelle Erfassung der Daten nach Nr. 8.1.2.1.1 zu bescheinigen, sind die Daten vor Freigabe zur weiteren Verarbeitung von einer zweiten Person hinsichtlich ihrer richtigen und vollständigen Erfassung zu prüfen.

Sind die Daten unrichtig oder unvollständig erfasst, müssen sie von einer zur Datenerfassung berechtigten Person berichtigt und von einer zweiten Person freigegeben werden.

Die Prüfung der Datenerfassung ist nach Nr. 2.5.2.1 VV zu § 70 zu bescheinigen. Die oder der Beschäftigte übernimmt mit der Bescheinigung die Verantwortung dafür, dass die Daten richtig und vollständig erfasst wurden.

Die Bescheinigung der Prüfung der Datenerfassung nach Absatz 1 kann mehrere Geschäftsvorfälle umfassen, sofern zwischen allen Prüfungen und der Bescheinigung ein enger zeitlicher Zusammenhang besteht.

8.1.2.2 Elektronische Erfassung von Papierdokumenten

Werden Dokumente in Papierform elektronisch erfasst, z. B. durch Scannen, ist zu prüfen, ob die geänderte Form ein vollständiges Abbild der ursprünglichen Form ist. Die Prüfung ist zu dokumentieren. Der Zusammenhang einzelner Unterlagen muss gewahrt bleiben.

In einer Dienst- oder Fachanweisung ist festzulegen,

- die für die elektronische Erfassung zuständige Organisationseinheit,
- zu welchem Zeitpunkt die Dokumente erfasst werden (z. B. beim Posteingang, während oder nach Abschluss der Vorgangsbearbeitung),
- welches Schriftgut erfasst wird,
- dass die bildliche und inhaltliche Übereinstimmung des Abbilds mit dem Original zu prüfen ist und
- wie die Beseitigung von Fehlern und deren Dokumentation zu erfolgen hat.

Ein Abbild des Papierdokuments in schwarz-weiß ist ausreichend. Eine vollständige Farbwiedergabe ist nur erforderlich, wenn der Farbe Beweisfunktion zukommt. Wann dies der Fall ist, bestimmt die nach Nr. 2 verantwortliche Stelle.

Nach der elektronischen Erfassung sind die Papierdokumente mindestens drei Monate aufzubewahren, soweit sich nicht aus anderen Vorschriften längere Aufbewahrungsfristen ergeben.

Die Papierdokumente sind dem weiteren Bearbeitungsvorgang zu entziehen. Sofern aus organisatorischen Gründen nach der elektronischen Erfassung eine weitere Vorgangsbearbeitung des Papierbelegs erfolgt, muss nach Abschluss der Bearbeitung der bearbeitete Papierbeleg erneut erfasst werden und ein Bezug zum ersten erfassten Objekt hergestellt werden (gemeinsamer Index).

Nr. 8.1.2.1.1 Absatz 4 gilt entsprechend.

8.1.2.3 Übernahme von elektronischen Daten und Dokumenten

Die vollständige und unveränderte Übernahme von elektronischen Daten und Dokumenten ist durch automatisierte Kontrollen (z. B durch einen Saldenabgleich) zu überprüfen. Die Prüfung ist zu dokumentieren.

Die bei der Prüfung festgestellten Fehler sind zu analysieren und zu beheben. Es sind Maßnahmen zur Vermeidung derartiger Fehler zu treffen. Das Ergebnis der Analyse und die getroffenen Maßnahmen sind zu dokumentieren.

Die Finanzbehörde (die für Grundsatzfragen des Kassenrechts zuständige Stelle) kann im Einvernehmen mit dem Rechnungshof in begründeten Ausnahmefällen ein anderes Prüfverfahren zulassen. Dieses muss gewährleisten, dass Daten und Dokumente vollständig und unverändert übernommen werden.

Elektronische Daten und Dokumente müssen in einem IT-Verfahren in elektronischer Form weiterverarbeitet werden.

8.1.2.4 Inhaltliche Prüfung erfasster anzuordnender Daten

Werden anzuordnende Daten in einem IT-Verfahren nach Nr. 1.1 erfasst, muss gewährleistet sein, dass die inhaltliche Richtigkeit dieser Daten im Rahmen des Anordnungsverfahrens anhand von begründenden Unterlagen prüfbar ist.

Die Finanzbehörde (die für Grundsatzfragen des Kassenrechts zuständige Stelle) kann eine Ausnahme hiervon zulassen, soweit die inhaltliche Richtigkeit der anzuordnenden Daten in dem sie übergebenden IT-Verfahren, das nicht nach Nr. 1.1 in den Anwendungsbereich dieser Verwaltungsvorschriften fällt, geprüft wird und dabei gewährleistet ist, dass

- die Daten vollständig und richtig erfasst werden,
- nur hierzu berechtigte Personen die inhaltliche Richtigkeit der Daten prüfen,
- die Prüfung dokumentiert wird,
- die geprüften Daten unveränderbar sind und
- diese Anforderungen für Prüfungsinstanzen in angemessener Zeit nachvollziehbar sind.

Darüber hinausgehende Ausnahmen von Absatz 1 kann die Finanzbehörde (die für Grundsatzfragen des Kassenrechts zuständige Stelle) nur im Einvernehmen mit dem Rechnungshof zulassen.

Im Falle der Beantragung einer Ausnahme nach Absatz 2 oder 3 sind die aus dem Verzicht auf die Nachprüfbarkeit der anzuordnenden Daten im Anordnungsprozess resultierenden Risiken für das Staatsvermögen und für die Zuverlässigkeit, Vollständigkeit und Revisionsfähigkeit der Rechnungslegung im Rahmen der Risikoanalyse nach Nr. 4 zu analysieren und zu dokumentieren.

8.1.3 Beauftragung Dritter

Die verantwortliche Stelle nach Nr. 2 kann natürliche Personen, die nicht Beschäftigte der Freien und Hansestadt Hamburg sind, oder juristische Personen des privaten oder des öffentlichen Rechts (Dritte) damit beauf-

tragen, für sie Daten manuell in ein IT-Verfahren einzugeben oder Dokumente in Papierform elektronisch zu erfassen, wenn diese zuverlässig sind und ein sachlicher Grund für die Beauftragung vorliegt.

Die Anforderungen an die Datenerfassung nach den Nrn. 8.1.2.1 und 8.1.2.2 sind für Dritte vertraglich festzulegen, soweit nicht die Anwendbarkeit der VV zu den §§ 70 bis 74 vereinbart oder bei einer Abordnung das Weisungsrecht auf die Freie und Hansestadt Hamburg übergegangen ist.

Nr. 2.4.4.4 Absätze 2 und 3 VV zu § 70 sind anzuwenden.

Diese Anforderungen gelten auch, wenn Daten in einem IT-Verfahren manuell eingegeben oder Papierdokumente in einem solchen elektronisch erfasst werden, das nicht nach Nr. 1.1 in den Anwendungsbereich dieser Verwaltungsvorschriften fällt, und anschließend an ein IT-Verfahren nach Nr. 1.1 übergeben werden.

8.2 Datenverarbeitung

Sind Daten geprüft und ggf. angeordnet, ist sicherzustellen, dass sie im weiteren Verlauf der Datenverarbeitung nicht mehr geändert werden können.

Die Finanzbehörde (die für Grundsatzfragen des Kassenrechts zuständigen Stelle) kann in Ausnahmefällen zulassen, dass die Daten nach ihrer Erfassung und / oder ihrer Anordnung durch eine an der Datenerfassung und / oder Anordnung nicht beteiligten Person manuell zur weiteren Verarbeitung freigegeben werden, wenn sichergestellt ist, dass die Daten weder geändert noch gelöscht werden können und deren Verarbeitung nicht grundlos verzögert wird.

Die richtige und vollständige Datenverarbeitung ist automatisiert zu dokumentieren. Gleiches gilt bei Störungen, die zum Abbruch der Datenverarbeitung geführt haben. Es ist technisch zu gewährleisten, dass insbesondere im Störungsfall alle elektronischen Daten oder Dokumente verarbeitet werden und bereits verarbeitete elektronische Daten und Dokumente nicht erneut verarbeitet werden.

8.3 Datenübermittlung

Elektronische Daten und Dokumente sind über die Schnittstellen zu übermitteln, die von der das IT-Verfahren anbindenden Stelle vorgegeben werden.

Nr. 8.3.2 Absatz 2 VV zu § 70 ist zu beachten.

Werden elektronische Daten von einem IT-Verfahren für elektronische Anordnungen über Schnittstellen in ein Nebenbuch nach Nr. 8.1 Absatz 3 VV zu § 70 übernommen, muss ersteres sicherstellen, dass die übergebenen Daten den Vorgaben der Nrn. 2.3.3 und 11.2 VV zu § 70 entsprechen.

9 Interne Regelungen und Kontrollen

9.1 Dienst- oder Fachanweisung

Für jedes IT-Verfahren ist von der nach Nr. 2 verantwortlichen Stelle eine Dienstanweisung zu erlassen. Sie ist bei Änderungen des IT-Verfahrens oder der ihm zugrunde liegenden Prozesse, mindestens alle zwei Jahre, daraufhin zu überprüfen, ob Änderungen erforderlich sind. Sind abgrenzbare Sachverhalte zu regeln, können auch mehrere Dienstanweisungen erstellt werden.

In der jeweiligen Dienstanweisung sind den am Verfahren beteiligten Beschäftigten verbindliche Vorgaben für Arbeitsabläufe zu machen, durch die die Einhaltung der VV zu den §§ 70 bis 74 LHO gewährleistet wird. Insbesondere sind dort die unter den Nrn. 6.2.2.1, 6.2.2.2, 8.1.2.2, 8.1.2.3 Absatz 2, 9.2 und 11 angesprochenen Inhalte zu regeln.

Bei behördenübergreifend eingesetzten IT-Verfahren ist von der nach Nr. 2.2 verantwortlichen Stelle eine Fachanweisung nach dem Bezirksverwaltungsgesetz und/oder ein ausformuliertes Muster einer Dienstanweisung zu erstellen. Die nach Nr. 2.1 verantwortlichen Stellen haben die Dienstanweisung jeweils in Kraft zu setzen. Alternativ kann der Senat von der nach Nr. 2.2 verantwortlichen Stelle gebeten werden, eine Dienstvorschrift für alle Behörden und Ämter zu erlassen, die das IT-Verfahren einsetzen. Bei Bedarf können auch mehrere Muster von Dienst- oder Fachanweisungen jeweils zu Teilaspekten entworfen werden.

9.2 Kontrollmaßnahmen

9.2.1 Grundsatz

Während des Einsatzes von IT-Verfahren ist sicherzustellen, dass die nach Nr. 2 verantwortliche Stelle die Einhaltung der Standards nach Nrn. 4 bis 10 und der Bestimmungen der VV zu den §§ 70 bis 73 regelmäßig überprüft. Die Abgrenzung der Verantwortungsbereiche nach Nr. 6 ist hierbei zu beachten.

Dabei ist auch zu kontrollieren, ob das eingesetzte IT-Verfahren dem dokumentierten und genehmigten Verfahren entspricht (Programmidentität).

Erforderlich sind sowohl systemtechnische als auch manuelle Kontrollen. Der Höchstzeitraum zwischen den Kontrollen ist ausgehend von der Eintrittswahrscheinlichkeit der durch das IT-Verfahren verursachten Risiken für das Staatsvermögen und für die Zuverlässigkeit, Vollständigkeit und Revisionsfähigkeit der Rechnungslegung (siehe Nr. 4) in der Dienst- oder Fachanweisung festzulegen.

Unabhängig von der Eintrittswahrscheinlichkeit muss eine Kontrolle des IT-Verfahrens und seiner Anwendung mindestens alle zwei Jahre erfolgen.

9.2.2 Maßnahmen zur Fehlerbehebung

Werden bei der Kontrolle nach Nr. 9.2.1 Abweichungen des IT-Verfahrens vom dokumentierten und genehmigten Verfahren festgestellt, ist auf

die Einhaltung des dokumentierten Verfahrens hinzuwirken. Andernfalls sind die Nachweise nach Nr. 3 Absatz 2 entsprechend der Verfahrensänderung unverzüglich anzupassen. Nr. 1.2 ist zu beachten.

9.2.3 Dokumentationspflicht

Die durchgeführten Kontrollen nach Nr. 9.2.1 und die ggf. erforderlichen Maßnahmen zur Fehlerbehebung sind zu dokumentieren.

10 Revisionsfähigkeit des Verfahrens

10.1 Nachweis über Geschäftsvorfälle und Prüfbarkeit

Das IT-Verfahren ist so auszugestalten, dass die Grundsätze der Buchführung nach Nr. 7.2 VV zu § 70 LHO eingehalten sind, insbesondere dass über sämtliche Geschäftsvorfälle ein sachlicher und zeitlicher Nachweis erbracht werden kann. Geschäftsvorfälle müssen sowohl vollständig als auch auszugsweise sowie geordnet nach Zeitpunkt, Sach- und ggf. Personenkonten dargestellt werden können. Der Nachweis muss von einer sachverständigen, nicht am Verfahren beteiligten Person in angemessener Zeit dahingehend prüfbar sein, ob

- die verfahrensrechtlichen Vorgaben dieser Verwaltungsvorschriften und der Bestimmungen der VV zu den §§ 70 bis 73 eingehalten wurden (formelle Richtigkeit),
- die inhaltlichen Anforderungen an eine Anordnung, Buchung, Zahlung oder an einen Abschluss, insbesondere das Vorliegen eines Rechtsgrundes, erfüllt sind (sachliche Richtigkeit) und
- die Vergabe der Buchungsbelegnummern fortlaufend nachgewiesen werden können.

Werden die Geschäftsvorfälle nicht bereits bei der Datenerfassung dokumentiert, sondern erst auf einer nachfolgenden Verarbeitungsstufe, ist durch Kontrollen oder andere Maßnahmen die Vollständigkeit der Geschäftsvorfälle von deren Entstehung bis zu deren Dokumentation sicherzustellen.

In IT-Verfahren für Anordnungen sind bereits angeordnete Vorgänge so zu kennzeichnen, dass sie nicht erneut angeordnet werden können.

IT-Verfahren sind so auszugestalten, dass die Vorgaben nach Nrn. 2.3.4.3 Absatz 1, 7.2 und 12 VV zu § 70 (Zusammenhang zwischen Anordnung und begründenden Unterlagen bzw. zwischen dem Nachweis der Buchung und der Buchung selbst) elektronisch umgesetzt werden können.

10.2 Dokumentation der Zugriffe

Zugriffe auf das IT-Verfahren sind im System zu dokumentieren. Es muss jederzeit nachgewiesen werden können, welche Person zu welcher Zeit welche Aktionen ausgeführt hat. Der Nachweis muss zumindest folgende Daten enthalten:

- das Datum, die Uhrzeit und die Benutzerkennung der oder des Beschäftigten, die bzw. der auf das IT-Verfahren zugegriffen hat, sowie
- wenn Änderungen vorgenommen wurden, die Bezeichnung des Geschäftsvorfalls oder des sonstigen Gegenstands, auf den zugegriffen worden ist, und die geänderten Daten mit altem und neuem Stand.

10.3 Prüfberechtigungen

10.3.1 Grundsatz

Im Berechtigungskonzept nach Nr. 6.2.2 sind Berechtigungen im IT-Verfahren vorzusehen, die durch direkte Zuordnung zu einer Person einen ausschließlich lesenden Zugriff auf alle Daten und Systemeinstellungen zu Prüfungszwecken ermöglichen. Deren Zuordnung muss unmittelbar auf Anforderung erfolgen können.

Die Prüfbarkeit von Daten und Systemeinstellungen umfasst alle Inhalte des IT-Verfahrens wie z. B.

- Stammdaten,
- Bewegungsdaten,
- Systemparameter und Konfigurationsdaten,
- im System vordefinierte Rollen und Profile für Zugangs- und Zugriffsberechtigungen,
- Daten der Berechtigungsverwaltung,
- Protokollierungstabellen und Logdateien sowie
- die systeminterne Dokumentation.

Dazu gehört auch die Nachvollziehbarkeit

- der Änderungen von Berechtigungen im IT-Verfahren,
- der Veränderung des Programmcodes z. B. im Rahmen eines Transportsystems,
- der Inhalte des vom Verfahrenseigner hinzugefügten Programmcodes sowie
- des Aufbaus des IT-Verfahrens und seiner Bestandteile sowie der Betriebsumgebung des Verfahrens.

Die Prüfung muss von einer sachverständigen, nicht am Verfahren beteiligten Person in angemessener Zeit möglich sein und ohne, dass die nach Nr. 2 verantwortliche Stelle sie beeinflussen kann oder den genauen Prüfungsgegenstand erfährt.

Es ist sicherzustellen, dass die Prüfung von Daten und Systemeinstellungen nicht zu deren Änderung führt.

10.3.2 Ausnahmen

Von den Anforderungen an die Prüfberechtigungen in Nr. 10.3.1 Absatz 1 kann die Finanzbehörde (die für Grundsatzfragen des Kassenrechts zuständige Stelle) im Einvernehmen mit dem Rechnungshof Ausnahmen nach Nr. 12.2 Absatz 2 zulassen, wenn gewährleistet ist, dass

- alle Daten und Systemeinstellungen des IT-Verfahrens nachvollziehbar und
- die Daten maschinell lesbar sind.

Abschnitt III Stichprobenkontrollverfahren

11 Einsatz eines Stichprobenkontrollverfahrens

11.1 Voraussetzungen

Die Finanzbehörde (die für Grundsatzfragen des Kassenrechts zuständige Stelle) kann im Einvernehmen mit dem Rechnungshof zulassen, dass die abschließende Prüfung des Inhalts einer elektronischen Anordnung durch die anordnende Person (Nr. 2.4.2.5 VV zu § 70) durch ein Stichprobenkontrollverfahren ersetzt wird. Ein solches liegt vor, wenn die Beteiligung einer zweiten Person nur zur Prüfung eines Teils der Vorgänge (einer Stichprobe) vorgesehen ist. Es setzt grundsätzlich voraus:

- Die anfallenden Geschäftsvorfälle sind hinsichtlich ihrer Risiken einzuschätzen und dementsprechend in Grundgesamtheiten einzuteilen. Dabei dürfen nur die Geschäftsvorfälle zu einer Grundgesamtheit zusammengefasst werden, die sowohl gleichartige Sachverhalte als auch gleichartige Risiken aufweisen.
- Die Übertragbarkeit der Stichprobenergebnisse auf eine Grundgesamtheit muss durch mathematische Gesetzmäßigkeiten gewährleistet sein, so dass aus der Stichprobe Informationen gewonnen werden können, die für die jeweilige Grundgesamtheit repräsentativ sind (mathematisch-statistisches Stichprobenkontrollverfahren).
- Bei der Ermittlung des Stichprobenumfangs sind die Risiken der einzelnen Grundgesamtheiten zu berücksichtigen.
- Die Auswahl der Stichprobe muss dem Zufallsprinzip folgen.
- Es ist durch systemtechnische Vorkehrungen zu gewährleisten, dass die in die Stichprobe gelangten Geschäftsvorfälle erst nach ihrer Prüfung weiterverarbeitet werden.
- Die Parameter zur Berechnung der Stichprobe, die Auswirkungen auf die quantitative und qualitative Zusammensetzung der Stichprobe haben, müssen im IT-Verfahren frei einstellbar sein.
- Alle Geschäftsvorfälle müssen hinsichtlich ihrer Zuordnung zu einer Grundgesamtheit und ihrer weiteren Bearbeitung auswertbar sein.

11.2 Risikoanalyse

Das aus dem Verzicht auf eine Prüfung durch eine zweite Person resultierende Risiko für das Staatsvermögen sowie für die Zuverlässigkeit, Vollständigkeit und Revisionsfähigkeit der Rechnungslegung ist in der Risikoanalyse nach Nr. 4 zu untersuchen.

Die Kategorisierung der Geschäftsvorfälle in Grundgesamtheiten aufgrund ihres Risikopotentials ist darzustellen und zu begründen.

Der Einsatz eines Stichprobenkontrollverfahrens ist unzulässig bei Geschäftsvorfällen, die einen hohen Risikogehalt aufweisen (Risikofälle). Das ist insbesondere der Fall bei

- Geschäftsvorfällen, bei denen die Person, die die Feststellung der rechnerischen und sachlichen Richtigkeit trifft, anordnungsrelevante Daten von Debitoren oder Kreditoren (z. B. Bankverbindungen) selbst

erfasst oder in einem bestehenden Personenkontenstammsatz ändert,
- Geschäftsvorfällen, bei denen die anordnungsrelevanten Daten von Debitoren oder Kreditoren (z. B. Bankverbindungsdaten) von einer weiteren Person ohne inhaltliche Kontrolle auf Veranlassung der Person, die die Feststellung der rechnerischen und sachlichen Richtigkeit trifft, erfasst worden sind,
- Geschäftsvorfällen, die zu Zahlungen auf unbestimmte Zeit führen,
- unbefristeten Niederschlagungen nach § 62 Absatz 1 Nr. 2 und bei dem Erlass von Forderungen nach § 62 Absatz 1 Nr. 3,
- der Auszahlung von unklaren Zahlungseingängen und
- Anordnungen, die vorherige Anordnungen inhaltlich ändern (siehe Nr. 4.2 VV zu § 70).

11.3 Verantwortungsübernahme

Bei Einsatz eines Stichprobenkontrollverfahrens übernimmt die für das IT-Verfahren verantwortliche Stelle nach Nr. 2 für die Geschäftsvorfälle, die nicht in die Stichprobe gelangen, die Verantwortung dafür, dass diese ungeprüft weiterverarbeitet werden. Auf eine Anordnung wird in diesen Fällen verzichtet. Es ist eine Stelle zu bestimmen, die die Verantwortung dafür trägt, dass jederzeit eine ausreichende Ermächtigung durch den Haushaltsplan vorliegt.

11.4 Stichprobenprüfung

Für die Prüfung der in die Stichprobe gelangten Geschäftsvorfälle gelten die Vorschriften, die für alle Geschäftsvorfälle außerhalb eines Stichprobenkontrollverfahrens gelten.

Werden bei der Stichprobenprüfung Fehler festgestellt, sind diese unverzüglich zu berichtigen. Die fehlerhaften Fälle sind nach der Berichtigung erneut zu prüfen.

11.5 Dienst- oder Fachanweisung

Das Stichprobenkontrollverfahren ist in einer Dienst- oder Fachanweisung für die prüfenden Anwenderinnen und Anwender nachvollziehbar und verbindlich zu regeln, insbesondere sind die einzelnen Verantwortlichkeiten eindeutig abzugrenzen. Gegenüber den übrigen Anwenderinnen und Anwendern ist Stillschweigen über die quantitative und qualitative Zusammensetzung der Stichprobe zu wahren.

11.6 Fehleranalyse und Berichtswesen

Die Stichprobenfälle sind durch das IT-Verfahren auswertbar zu markieren; festgestellte Fehler sind auswertbar innerhalb des IT-Verfahrens zu dokumentieren.

Die aufgetretenen Fehler sind regelmäßig, mindestens aber jährlich daraufhin zu analysieren, ob das Stichprobenkontrollverfahren wirksam und

wirtschaftlich und ob eine Anpassung der Parameter oder der Parameterwerte notwendig ist. Das Ergebnis der Analyse ist zu dokumentieren und der oder dem zuständigen Beauftragten für den Haushalt zu berichten. Bei Auffälligkeiten, z. B. systematisch auftretende Fehler, sind unverzüglich Maßnahmen zu ergreifen, die dem entgegenwirken.

11.7 Änderung der Stichprobe

Im IT-Verfahren hinterlegte Parameter und Parameterwerte dürfen nur mit Zustimmung der oder des Beauftragten für den Haushalt oder einer von ihr bzw. ihm hierzu bevollmächtigten Person geändert werden.

Abschnitt IV Zulassung von IT-Verfahren

12 Prüfungsverfahren und Zulassung

12.1 Zulassungsantrag

12.1.1 Voraussetzungen des Zulassungsantrags

Die Zulassung eines IT-Verfahrens ist bei der Finanzbehörde (die für Grundsatzfragen des Kassenrechts zuständige Stelle) zu beantragen.

Der Antrag muss die nach Nr. 3 Absatz 2 erforderlichen und vollständigen Nachweise enthalten, ggf. die erforderlichen Ausnahmen ausdrücklich benennen und diese in der Risikoanalyse berücksichtigen (siehe Nr. 3 Absatz 2 dritter Spiegelstrich in Verbindung mit Nr. 4).

Die Freigabeerklärung kann ggf. nachgereicht werden; sie muss jedenfalls bis zur Zulassung vorliegen.

Der Antrag ist von der oder dem Beauftragten für den Haushalt zu stellen.

12.1.2 Antragsfrist

Die Zulassung eines IT-Verfahrens ist von der nach Nr. 2 verantwortlichen Stelle mindestens zwei Monate vor dem geplanten Einsatz des IT-Verfahrens zu beantragen. Soll eine Ausnahme von den Standards nach den Nrn. 4 bis 10 oder den Bestimmungen der VV zu den §§ 70 bis 73 in Anspruch genommen werden, ist der Antrag der Finanzbehörde fünf Monate vor der geplanten Inbetriebnahme zuzuleiten. Die Zulassung einer Änderung eines IT-Verfahrens (Nr. 1.2) ist mindestens drei Monate vor der geplanten Änderung zu beantragen.

12.2 Zulassung durch die Finanzbehörde

Die Finanzbehörde prüft anhand der vorgelegten vollständigen Nachweise, ob die Standards nach Nr. 4 bis 10 und die Bestimmungen der VV zu den §§ 70 bis 73 eingehalten sind. Ist dies der Fall, lässt die Finanzbehörde das IT-Verfahren zu.

Weicht das IT-Verfahren von den Standards nach Nrn. 4 bis 10 oder den Bestimmungen der VV zu den §§ 70 bis 73 ab, entscheidet die Finanzbehörde, ob sie das IT-Verfahren mit den beantragten Ausnahmen zulässt, wenn die Voraussetzungen des jeweiligen Ausnahmetatbestandes vorliegen.

12.3 Widerruf der Zulassung

Die Finanzbehörde kann die Zulassung widerrufen, wenn sie aufgrund nachträglich eingetretener oder bekannt gewordener Tatsachen berechtigt wäre, das IT-Verfahren nicht zuzulassen. Bei einem Widerruf entscheidet sie zugleich, ob und ggf. unter welchen Voraussetzungen das IT-Verfahren ohne die Zulassung vorläufig weiter genutzt werden darf.

13 Unterrichtung des Rechnungshofs

Die Finanzbehörde unterrichtet den Rechnungshof unverzüglich, wenn IT-Verfahren nach Nr. 12.2 zugelassen wurden und übersendet die vollständigen Nachweise (Nr. 3).

Sie unterrichtet den Rechnungshof auch unverzüglich, wenn die Zulassung für IT-Verfahren nach Nr. 12.3 widerrufen wurde.

Abschnitt V Übergangsbestimmungen

14 Noch nicht zugelassene IT-Verfahren

IT-Verfahren im Sinne der Nr. 1.1, für die innerhalb von sechs Monaten nach Inkrafttreten dieser Verwaltungsvorschriften die Zulassung nach Nr. 12.1.2 beantragt wird, kann die Finanzbehörde mit Zustimmung der verantwortlichen Stelle nach Nr. 2 nach den Vorschriften der Anlage 10 VV ZBR in der Fassung vom 1. Juni 2013 zulassen.

15 Zugelassene IT-Verfahren

15.1 Grundsatz

Wurde vor Inkrafttreten dieser Vorschriften in die Einführung eines IT-Verfahrens durch die Finanzbehörde nach den zum Zeitpunkt der Erteilung bestehenden Vorschriften eingewilligt, so besteht diese Zulassung fort.

15.2 Änderung von IT-Verfahren

Änderungen von vor Inkrafttreten dieser Vorschriften zugelassenen IT-Verfahren müssen die Anforderungen dieser Verwaltungsvorschriften erfüllen.

Bestehende Ausnahmegenehmigungen nach Nr. 10 Anlage 10 VV ZBR in der Fassung vom 1. Juni 2013 bleiben in diesem Fall bestehen, wenn sich die Änderung nicht auf den Ausnahmetatbestand auswirkt. Ist hingegen der Prozess des IT-Verfahrens betroffen, für den die Ausnahme erteilt wurde, ist ihr Fortbestehen nach diesen Vorschriften zu prüfen.

Betrifft eine Änderung Prozesse eines IT-Verfahrens, die manuell erfolgen, gelten die vorstehenden Vorschriften entsprechend.

15.3 Änderung von Altverfahren

Bei IT-Verfahren, die vor dem 1. Juni 2013 zugelassen wurden, muss bei einer wesentlichen Änderung das Zulassungsverfahren erneut in Bezug auf das gesamte IT-Verfahren durchgeführt werden.

15.4 Überprüfung der Nachweise nach Nr. 3

Soweit für die Nachweise nach Nr. 3 Absatz 2 in diesen Verwaltungsvorschriften eine regelmäßige Überprüfung vorgesehen ist, sind diese spätestens zwei Jahre nach Inkrafttreten dieser Vorschriften aufgrund der darin enthaltenen Vorgaben zu überprüfen und entsprechend zu aktualisieren.