Prüfbericht nach OPDV-Stellungnahme Nr. 1/2015

IDV-Suite in der Version: 4.0

(**Abschlussergebnis**)

Dokumentversion 3.24 vom 03.02.2016 14:14 [IDW PS951, Tz121]

Dieser Prüfbericht ist nur gültig, wenn er komplett weitergegeben wird, also alle Seiten vom Deckblatt bis zur Unterschriftenseite enthält.
Unvollständig weitergegebene Dokumente sind ungültig!

Eine erste Übersicht der im Rahmen der hier dokumentierten Prüfung behandelten Standards mit Verweisen auf weitere Details findet sich im Abschnitt 1.3.

Auflagen finden sich im Abschnitt 4.1.

SIZ SICHERHEIT INFORMATIK ZENTRALE SERVICES

Inhaltsverzeichnis

Versionsführung dieses Dokumentes:

Wer	Wann/ Version	Was
Hr. König	V150128 V3.21	▪ Berücksichtigung der [GoBD]
Hr. König	V150303 V3.22	▪ Statt Empfehlung zur Freigabe jetzt Nutzungshinweise der Freigabeerklärung und Freigabeerklärung
Hr. König	V150303 V3.23	▪ Die ISO/IEC 9126 ist in die ISO 250xx aufgegangen und daher aus dem Dokument entfernt worden. ▪ DIN ISO/IEC 12119 dito
Hr. König	V150601 V3.24	▪ Abschnitte zu PrüfbV, GwG, KWG, IDW PS 951, IDW PS 980 überarbeitet bzw. ergänzt.

1 Vorwort und Zusammenfassung

Die in den letzten Jahren eingeführten Internet-basierten Infrastrukturen, wie sie bspw. die auf Browsern basierenden Client- und Serverarchitekturen erfordern, eröffnen den Anwendern die komfortable Abwicklung von Transaktionen ohne komplexe Softwareinstallation auf den Arbeitsplatzsystemen. Zugleich bringen die neuen Technologien neue Risikopotentiale mit sich, die mit immer sorgfältigerer Planung, Umsetzung und Überprüfung der IT-Anwendungen und Infrastrukturen einzugrenzen sind.

Dies sicherzustellen ist Aufgabe des jeweiligen Projektmanagements, der beteiligten Fachabteilungen sowie der Innenrevision. Mit der Stellungnahme OPDV 1/2015 liegen Regularien für die Freigabe eines Systems vor. Soweit es sich um fremd entwickelte, komplexe Systeme handelt, wird der Aufwand hierfür jedoch zunehmend größer. Wenn der Einsatz des Systems dann noch bei mehreren Betreibern vorgesehen ist, dann bietet es sich an, die Freigabe in eine Programmfreigabe und eine Einsatzfreigabe aufzuspalten.

Unter **Programmfreigabe** versteht die OPDV 1/2015 *die Summe der Qualitätssicherungsmaßnahmen zur Sicherstellung der korrekten Programmfunktionalität. Ziel der Programmfreigabe ist es, sicherzustellen, dass der Anwender sich auf die Verarbeitungsergebnisse des Programmes verlassen kann*.

*Die **Einsatzfreigabe** beinhaltet die Integration des Programms in die Prozesse der Sparkasse. Hierbei sind insbesondere die Auswirkungen des Programmeinsatzes auf das Rollen- und Rechtekonzept und das IKS der Sparkasse zu betrachten. Das IKS wird in modernen Programmen in der Regel durch Parameter, die z. B. Kontrollgrenzen oder absolute Höchstbeträge steuern, unterstützt. Das Anpassen der Berechtigungen und Parameter auf die institutsindividuellen Anforderungen wird in der Fachliteratur oft auch als Customizing bezeichnet*.

Im Verlauf der Prüfung kam auch die *Checkliste Prüfungen nach OPDV 1/2015* des SIZ zum Einsatz. Diese Liste baut auf der Stellungnahme Nr. 1/2015 des Fachausschusses OPDV auf und berücksichtigt die Praktiken und Erfahrungen mit DV-Projekten innerhalb der Sparkassen-Finanzgruppe. Der Prüfbericht ist somit eine thematisch umfassende und unabhängige Analyse des Entwicklungs-, Qualitätssicherungsprozesses sowie des Praxiseinsatzes, der dem Freigabeverfahren nach OPDV 1/2015 unterliegt. Der Prüfbericht berücksichtigt insbesondere auch Aspekte des Projektmanagements, der IT-Qualität, der Softwareentwicklung sowie der IT-Sicherheit.

1.1 Benutzung / Zweck des Dokumentes

Kursive Texte kennzeichnen Originalzitate aus anderen Dokumenten oder Vorgaben.

Fett dargestellte Abschnitte außerhalb der Überschriften stellen Auflagen dar.

Die Programmfreigabe nach 1/2015 wird im Abschnitt *4 Zusammenfassende Bewertung der IT-Anwendung aus Sicht der Stellungnahmen* dokumentiert.

1.2 Prüfgegenstand

1.2.1 Identifizierung

Im Rahmen der hier dokumentierten Prüfung ist die erstellte IT-Anwendung *IDV-Suite* in der Version 4.0 und deren Herstellungsprozess bei der stromwerken[1] zu untersuchen und zu bewerten [IDW PS 880, Tz2]. Die Version 4.0 besteht aus folgenden Detailversionen:

- ExcelTracker V4.0 (Build: 3-0-408
- Excel-Sheet-Checker: 4.9 vom 05.08.2015
- Excel-File-Compare: 2.0
- ExcelProtect: V2.4 FP6
- Excel-Sheet-QA: V2.3
- Access-Checker: V2.1
- IDV-Suite Scheduler: V4.0 (Build: 206)

1.2.2 Produktbeschreibung

Gegenstand der Prüfung ist ein Softwaresystem namens *IDV-Suite*. *IDV-Suite* ist eine Unterstützungssoftware für im Institut durchzuführende Programmeinsatzfreigaben nach MaRisk AT7.2 bzw. OPDV 1/2015. *IDV-Suite* dient dabei den Mitarbeitern die Teile des Einsatzfreigabeprozesses durchführen als Unterstützungstool. Die Kernfunktionalität der *IDV-Suite*-Anwendung besteht hinsichtlich dieser Freigaben:

- Ermöglichen und potenziell Erzwingen von Bewertungsschritten
- Potenzieller Dokumentationsort für Software und Testdokumentation
- Parameterkonfiguration, Reporterstellung und Wirksamkeitskontrollunterstützung
- Fehlersuch-, Schutz- und Vergleichsfunktionen auf IDV.

Die folgenden Dokumente sind vor Vertragsunterschrift als Produktbeschreibung zu konsultieren, da sie wesentliche und für den Betrieb erforderliche Informationen beinhalten:

- SIZ-Foliensatz mit Produkteigenschaften der IDVSUITE [331].
- IDV-Suite Implementierungsleitfaden [509] beschreibt die organisatorischen und technischen Voraussetzungen im Rahmen der Installation und Betriebsvorbereitung.
- Das Handbuch (u. a. [511, 3 Die Neuerungen zur OPDV 1/2015]) stellt Optionen dar, die im Institut entschieden und umgesetzt werden müssen.

[1] Nachfolgend mit Hersteller abgekürzt.

Technisch ist *IDV-Suite* eine in Visual Basic [514, 6. Benennungsvereinbarungen für Objekte] implementierte gemischte Anwendung. Die zentrale Trackerfunktion *IDV-Suite* wird auf einem Mitarbeiter-Arbeitsplatz als Excel- bzw. Access-AddIn-Anwendung ausgeführt. Weitere Module, auch für Administratoren stehen zur Verfügung.

Das Softwaresystem ist gegliedert in mehrere Komponenten. Für eine nähere Beschreibung siehe die entsprechenden Handbücher.

Die Prüfaussage dieses Prüfberichts bezieht sich auf die folgenden Systemkomponenten (Kernbestandteile) von *IDV-Suite*:

- Excel-Tracker, Access-Tracker
  beide dienen den Nutzers der jeweiligen Trägersysteme um u. a. Bewertungen, Dokumentationen und freigaberelevante Prozessschritte durchzuführen.
- Backend, Scheduler
  dienen im Wesentlichen den Prozessverantwortlichen zur Erzeugung von Reports und zu Festlegung von Parametern.
- ACC, ECC, ExcelSheetChecker, AccessChecker
  dienen dem Nutzer und Kontrolleuren zur Ermittlung technischer Eigenschaften von Drittanwendungen.
- Excel-File-Compare
  dient dem Vergleich von Exceldateien z. B. mit hinterlegten und freigegebenen Versionen.
- Excel-Protect
  dient der automatischen Vergabe von Schutzmaßnahmen auf Excel-Dateien.
- Excel-Sheet-QA
  überprüft eine Excel-Datei auf einzelne inhaltliche Fehler.

1.2.2.1 Schnittstellen

Folgende Schnittstellen sind vorhanden:

Benutzer:

- Die beiden Tracker integrieren sich in die Trägersysteme MS-ACCESS und MS-EXCEL und stellen dort Funktionen bereit. Viele der Komponenten greifen lesend auf die zu betrachtenden ACCESS- und EXCEL-Dateien zu.
- Die Liste der von den Trackern bereitgestellten Funktionen ist konfigurierbar.

Fachliche Administration:

- Setzen von Parametern
- Freigaben
- Automatischer Versand von Benachrichtigungs-E-Mails, sofern gewünscht

Datenbank

- Relevante Daten werden in einer Datenbank abgespeichert.
- Es gibt eine Schnittstelle zur bit-Software Software-Lifecycle.

1.2.2.2 Abgrenzung

Die folgenden mit dem Produktumfang ebenfalls ausgelieferten oder auslieferbaren Systemkomponenten sind nicht Bestandteil der Überprüfung. Allgemeine Aussagen der vorliegenden Prüfungsdokumentation gelten daher nur dann auch für diese Systemkomponenten, wenn explizit darauf hingewiesen wird:

- Eine ordnungsgemäße Durchführung eines Programmfreigabeprozesses obliegt dem nutzenden Institut, die hier bereitgestellten Komponenten stellen diesbezüglich nur Werkzeuge bereit.
- Der Prüfbericht geht auf die auf der Homepage des Herstellers unter Produkt IDVSUITE[2] angebotene SOX-Kompatibilität nicht ein, da SOX i. d. R. kein für Sparkassen relevantes Thema darstellt.
- Der vorliegende Prüfbericht stellt nur einen Soll-Ist-Vergleich der zu prüfenden IT-Anwendung dar. Aus Sicht des IDW PS 951 deckt er damit maximal eine Stufe 1 ab. Alle Themen, die sich mit Stufe 2 des IDW PS 951 befassen[3] oder andere Standards, die sich mit dem Betriebsablauf einer Software befassen, sind nicht Thema des vorliegenden Prüfberichtes, es sei denn dass diese Themen in Einzelfällen explizit angegeben werden.

1.3 Prüfkriterien

Die Prüfung erfolgt auf der Grundlage der von:

- Fachausschuss Ordnungsmäßigkeit und Prüfung der Datenverarbeitung, Stellungnahme Nr. 1/2006, Anforderungen an einen ordnungsgemäßen Software-Einsatz in ihrer aktuellen Fassung.
- Fachausschuss Ordnungsmäßigkeit und Prüfung der Datenverarbeitung (OPDV) Stellungnahme Nr. 1/2015 Anforderungen an ein ordnungsgemäßes Programmeinsatzverfahren, Stand Februar 2015.

Die Prüfung erfolgte unter Hinzuziehen der folgenden Checkliste:

- Checkliste - Prüfungen nach OPDV 1/2015, Version vom 15.07.2015, SIZ

Im Rahmen der Prüfung wird vor Prüfungsbeginn kontrolliert, ob die in der Checkliste abgebildeten Standards für den konkreten Prüfling ausreichend sind. Bei Bedarf werden weitere Standards aufgenommen. Der Prüfer geht davon aus, dass im Rahmen der mit dem Prüfbericht dokumentierten Prüfung alle relevanten Standards ausreichend betrachtet wurden. Die Standards, die im Prüfling tatsächlich zu betrachten waren, finden sich auf Grund der primär auf Lesbarkeit ausgerichteten Dokumentstruktur an folgenden Stellen:

- Sämtliche Softwareentwicklungsstandards werden im Abschnitt *5 Detailbewertung der Bereitstellungs- und Wartungsprozesse (Projektverantwortung)* und seinen Unterabschnitten behandelt. Eine genaue Referenzierung erlauben die Literaturverweise in eckigen Klammern, die auf entsprechende Dokumente im Abschnitt *3 Literaturverzeichnis (inkl. Angaben zum geprüften Projekt)* referenzieren.

[2] http://stromwerken.de/produkte/idv-suite/idv-suite.html

[3] Typ 2 wird in folgenden Einzelaspekten angesprochen: [IDW PS951, Tz11], [IDW PS951, Tz16], [IDW PS951, Tz18], [IDW PS951, Tz21], [IDW PS951, Tz23], [IDW PS951, Tz56], [IDW PS951, Tz61], [IDW PS951, Tz64], [IDW PS951, Tz73], [IDW PS951, Tz75], [IDW PS951, Tz105], [IDW PS951, Tz107], [IDW PS951, Tz110], [IDW PS951, Tz111], [IDW PS951, Tz113] und [IDW PS951, Tz114].

- Im Rahmen der Prüfung hinterfragte Umsetzungen von Gesetzen, Verordnungen und fachlichen Standards werden in den Unterabschnitten des Abschnittes *6.2 Fachliche Berücksichtigung von gesetzlichen oder normativen Vorgaben* einzeln benannt. Beschreibungen umgesetzter Standards, die als Unterstandard eines anderen Standards angesehen werden können, lassen sich in vielen Fällen nur über den Index, siehe Abschnitt *11 INDEX* finden.
- Die Abbildung sämtlicher Standards zur Betriebssicherheit wird durch den sogenannten „Sicheren IT-Betrieb (SITB)“ der Sparkassen sichergestellt. Die im Rahmen der Prüfung hinterfragten und für das Prüfobjekt relevanten Konzepte (K-Nummern) dieses SITB werden in den Unterabschnitten des Abschnittes *7.4 Sicherstellung eines sicheren IT-Betriebes* genannt und ihre jeweilige Umsetzung dokumentiert.

1.4 Ziel der Prüfung

Vor Inbetriebnahme eines IT-Systems innerhalb der Sparkassen-Finanzgruppe ist eine Programmfreigabe nach OPDV 1/2015 erforderlich. In diese Freigabeerklärung fließen die Ergebnisse aller am Abnahmeprozess Beteiligten ein. Als Vorbereitung auf die Freigabe analysiert und bewertet vorliegender, von einem unabhängigen Mitarbeiter der SIZ GmbH erstellte Prüfbericht den Verlauf und die jeweiligen Arbeitsergebnisse der Herstellung durch stromwerken.

Das Ziel der Prüfung ist die Bewertung, inwieweit die Anforderungen der OPDV 1/2015 eingehalten sind, d. h. es wird im Prüfbericht eine Aussage zur Ordnungsmäßigkeit der Verarbeitung des IT-Systems getroffen. Sofern alle Anforderungen eingehalten sind, wird eine Empfehlung zur Freigabe ausgesprochen.

Als Besonderheit bezieht sich das konkrete Freigabeverfahren der SIZ GmbH für *IDV-Suite* lediglich auf eine „Programmfreigabe“. Vor einem tatsächlichen Einsatz von *IDV-Suite* innerhalb der Sparkassen-Finanzgruppe ist zusätzlich ein Institut spezifisches Einsatzfreigabeverfahren zu durchlaufen. Dies muss den örtlichen Gegebenheiten des Betreibers Rechnung tragen und den Integrationsprozess berücksichtigen. Insbesondere sind seine infrastrukturellen, organisations- und bundeslandspezifischen Vorschriften und Regelungen bzw. Gesetze einzubeziehen.

1.5 Voraussetzungen der Prüfung

Für den vorliegenden Prüfbericht ist Folgendes vorausgesetzt:

- Prüfer erfüllen die persönlichen, fachlichen und formalen Voraussetzungen für die Durchführung der Prüfung nach OPDV 1/2015.
- Das IT-System bzw. IT-Produkt unterliegt den Regelungen der OPDV 1/2015.
- Grundsätzlich haben die Betreiber wie auch der Prüfer das Vertrauen in den Hersteller, dass er seine Kompetenzen nach bestem Wissen und Gewissen einsetzt. Damit mögliche Fehler vermieden oder zumindest erkannt und beseitigt werden können, gewährte der Hersteller dem Prüfer einen umfassenden und detaillierten Einblick in seine internen Abläufe. Dies beinhaltet seine Prozesse, Verfahren, Methoden und Dokumente. Hierdurch wird das Vertrauen in die Produkte des Herstellers gestärkt. Die Offenlegung dieser betriebsinternen Informationen erfolgt im wechselseitigen Vertrauen auf die Einhaltung üblicher Vertraulichkeitsregelungen. In den Prüfbericht fließen ausschließlich Informationen, die für die Analyse und Bewertung nach OPDV 1/2015 erforderlich sind.

1.6 Prüfgrundsätze und -vorgehen

Die für die Prüfung nach OPDV 1/2015 angewendeten Grundsätze sind:

- Die Prüfung begleitet den Lebenszyklus des IT-Systems bzw. IT-Produkts beginnend mit der Anforderungsdefinition bis hin zur Auslieferung an den Kunden.
- Die Prüfung bewertet sämtliche Qualitätsprozesse und schließt die fachkundige Bewertung der IT-technischen, infrastrukturtechnischen, organisatorischen, prozessualen und sicherheitstechnischen Maßnahmen ein.
- Die Prüfung bewertet auch, ob beim Softwareentwickler die Anforderungen gemäß OPDV 1/2015 eingehalten wurden.
- Die Prüfung stützt sich auf die Herstellerdokumentation.
- Die Prüfung wendet das „Prinzip des Unabhängigen Dritten“ an, d. h. die Abnahme wird von unabhängigen SIZ-Mitarbeitern überprüft. Die Aussagekraft der Überprüfung und die dadurch erzielbare Qualität wird so deutlich gesteigert. Das Arbeitsergebnis der unabhängigen Analyse ist vorliegender Prüfbericht.
- Die Prüfung wird unter der „going concern“ Annahme des Softwareherstellers durchgeführt, d. h. die Bewertungen werden unter der Voraussetzung getroffen, dass das die IT-Anwendung herstellende Unternehmen fortbesteht.
- Im vorliegenden Prüfbericht finden sich vom Prüfer für relevant erachteten Zusammenfassungen von Vorgaben und Ergebnissen. Der Prüfbericht selbst stellt nach [IDW PS951, Tz94] nur einen Auszug der kompletten Prüfungsdokumentation dar, die aus jeweils aktuellen Vorlagen generiert werden, um Findings und Referenzen im Zeitverlauf ergänzt werden und Vorabbewertungen enthalten.
- Im Prüfungsverlauf werden alle Dokumentationen im Literaturverzeichnis verzeichnet [IDW PS951, Tz95]. Im Prüfbericht werden nur die Dokumente referenziert, die zur Beschreibung des Prüfungsergebnisses benötigt werden. Das Literaturverzeichnis versucht soweit möglich Quellen- und Versionsangaben der aufgeführten Dokumente anzugeben [IDW PS951, Tz96], sofern die Dokumente nicht vom Auftraggeber selbst bereitgestellt wurden.
- Im Rahmen der Prüfung stattgefundene Sitzungen [IDW PS951, Tz98] werden im Abschnitt *1.9 Projektverlauf* unter Nennung der Teilnehmer aufgezählt.

1.7 Grenzen des Dokuments

Dieser Prüfbericht ist thematisch sehr umfassend angelegt, so dass erwartet werden kann, dass alle IT-technischen Aspekte der Programmfreigabe nach OPDV 1/2015 abgedeckt sind. Seine Grenzen werden hier konkretisiert.

- Dieser Prüfbericht betrachtet ausschließlich die in direktem Zusammenhang mit der Informationstechnologie stehenden Aspekte, die zur erfolgreichen Projektabwicklung bzw. System- und Produktentwicklung gehören. Dies schließt sämtliche zugehörigen organisatorischen wie technischen Themen ein. Bspw. gehört das Projektmanagement ebenso zu den Aspekten wie Dokumentation, Entwicklung, Herstellertests, Abnahmetests sowie IT-Qualität und IT-Sicherheit. Nur bedingt betrachtet werden dedizierte juristische oder betriebswirtschaftliche Aspekte. Auch sind Aspekte wie die Analyse des Kundenbedarfs an anderer Stelle zu betrachten.
- Die Überprüfung erfolgt immer gegen die Produktspezifikation, deren inhaltliche Korrektheit und Vollständigkeit ausschließlich in der Verantwortung des Herstel-

lers liegt. Die Spezifikation wird lediglich darauf hin überprüft, ob sie ausreichend vollständig und in sich schlüssig ist.

- Anforderungsdefinitionen bzw. zu Grunde gelegte Standards werden grundsätzlich nicht hinterfragt, es sei denn, dass sie offensichtlich unvollständig oder unangemessen sind.
- Insbesondere nicht enthalten ist eine Detailanalyse des IT-Systems bzw. Produkts bspw. im Rahmen eines Codereview [IDW PS 880, Tz22]. Solche tiefgehenden Analysen erforderten das Anwenden bspw. von IT-Sicherheitskriterien wie den „Common Criteria“ (ISO 15408) oder des Sicheren IT-Betriebs der SIZ GmbH, was inhaltlich sowie im Umfang ausdrücklich außerhalb dieser Prüfung liegt.
- Der vorliegende Prüfbericht greift der Einsatzfreigabe nach OPDV 1/2015 durch das einsetzende Institut nicht vor. Diese Freigabe bleibt exklusiv dem jeweiligen Institut vorbehalten.
- Grundsätzlich muss jeder Betreiber vor Einsatz des Produktes sein eigenes Freigabeverfahren durchführen, welches die konkreten Gegebenheiten des Betreibers berücksichtigt. Dabei ist es empfohlen und gewollt, die aus der Programmfreigabe gewonnenen Erkenntnisse in die eigene Analyse einzubinden.
- Hinsichtlich der in [IDW PS 880, Tz19] geforderten eigenen Testfälle des Prüfers wird im Rahmen der hier dokumentierten Prüfung überprüft, ob in den vorgelegten Testprotokollen auch die Prüffälle enthalten sind, die aus Sicht des Prüfers durchgeführt werden müssten. Hierzu werden sowohl Prüfungen auf in der Software erwartete Eigenschaften als auch Prüfungen auf nicht in der Software zugelassene Eigenschaften (siehe [IDW PS 880, Tz20]) herangezogen und dabei alle potentiellen Störquellen betrachtet. Einem vorgelegten Testprotokoll wird dabei nicht blind vertraut, es wird seitens des Prüfenden hier immer ein Nachweis über die Korrektheit des Testprotokolls verlangt.

1.8 Projektbeteiligte

Hersteller und Lieferant

Hersteller von *IDV-Suite* ist die stromwerken.

Lieferant von *IDV-Suite* ist die SIZ GmbH.

Auftraggeber der Prüfung

Die Prüfung wurde am 02.12.2015 beauftragt von der Geschäftsführung der SIZ GmbH [IDW PS951, Tz105].

Betreiber

Hinweis: Die potenziell erforderliche Betreiberfreigabe seitens der Rechenzentren ist nicht Gegenstand dieses Berichts.

Abnahmen

Die IT-Anwendung wurde dem Prüfer durch den Geschäftsführer des Herstellers übergeben.

Prüfinstitut

Die Prüfung wurde durchgeführt von Herrn König, Mitarbeiter der SIZ GmbH, Bonn. Die Prüfung wird unabhängig vom Projektteam [IDW PS951, Tz105] dokumentiert.

1.9 Projektverlauf

- Wesentliche Neuerungen in der hier betrachtenden Version 4.0 sind im Handbuch [511, 3 Die Neuerungen zur OPDV 1/2015] beschrieben.
- Die herstellerinterne Testphase dieser neuen Version führte am 17.08.2015 zur Herstellerfreigabe seitens des Herstellers.
- Vorversionen sind bei Sparkassen und anderen Finanzinstituten seit längerem im Einsatz, die dabei zu lösenden technischen Herausforderungen sing gelöst.
- Im Rahmen der in diesem Dokument beschriebenen Prüfungsmaßnahmen hat der Prüfer am 02.12.2015 den generellen Prüfauftrag erhalten (siehe [IDW EPS 460nF, Tz14ff], [IDW PS951, Tz105]).
- Erste Unterlagen wurden dem Prüfer am 17.08.2015 bereitgestellt. Im Rahmen der Prüfung wurden Nacharbeiten erforderlich, die z. T. am 16.11.2015 durch den Hersteller und der Rest am 29.12.2015 durch den Lieferanten bereitgestellt wurden.
- In Absprache zwischen Auftraggeber und SIZ wurde am beschlossen, den aktuellen Stand im Prüfbericht festzuhalten, dieses wurde nach interner Qualitätssicherung auch mit dem Auftraggeber abgestimmt und im Januar 2016 dem Auftraggeber übergeben.

2 Details zur Risikoklassifizierung

***IDV-Suite* stellt nach der in diesem Dokument beschriebenen Risikobeurteilung eine IT-Anwendung mit mittlerem bis hohen Risiko dar und entspricht dabei den Vorgaben der Risikostufe A bzw. B der OPDV-Stellungnahme Nr. 1/2006.**

***IDV-Suite* stellt nach OPDV Stellungnahme 1/2015 eine IT-Anwendung mit hohem Schutzbedarf dar.**

2.1 Wirtschaftliche Auswirkungen bzw. Auswirkungen auf geschäftspolitische Entscheidungen

Wirtschaftliche Auswirkungen oder Auswirkungen auf geschäftspolitische Entscheidungen werden nicht gesehen.

2.2 Auswirkungen auf die Kundenbeziehung

Auswirkungen auf die Kundenbeziehung werden nicht gesehen, da die Informationen nur Institutsintern vorgelegt, nicht aber Richtung Sparkassenkunden kommuniziert werden.

2.3 Auswirkungen auf das Sicherheitsniveau

Die IT-Anwendung unterliegt folgenden Beurteilungskriterien zu Auswirkungen auf das Sicherheitsniveau:

- Die notwendige Verfügbarkeit [IIR2, 20 Datenverarbeitungsrisiken: Verfügbarkeit] von *IDV-Suite* wird mit niedrig und deren Sicherstellung wird mit ausreichend sichergestellt bewertet.
- Zur Sicherstellung der erforderlichen Integrität der Informationen ist eine ausreichende Funktionstrennung (Segregation of Duties) in der Bedienung der IT-Anwendung erforderlich. Diese ist insbesondere durch ein Vier-Augen-Prinzip bei Operationen direkt auf der Datenbank sicherzustellen.

Andere Auswirkungen auf das Sicherheitsniveau werden nicht gesehen. Insgesamt werden dabei diese Auswirkungen durch die IT-Anwendung von der SIZ GmbH als mittleres Risiko bewertet.

2.4 Einhaltung gesetzlicher oder bankaufsichtsrechtlicher Vorschriften

Die IT-Anwendung unterliegt folgenden Beurteilungskriterien zu Auswirkungen auf die Einhaltung von gesetzlichen und sonstigen relevanten Vorschriften:

- *IDV-Suite* hat folgende Auswirkungen auf das interne Kontrollsystems (IKS):
  - Die *IDV-Suite* unterstützt den nach MaRisk AT7.2 erforderlichen Programmfreigabeprozess, der ohne diese IT-Anwendung ebenfalls durchführbar wäre.
  - Freigabeunterlagen von GoBD-relevanten Drittanwendungen unterliegen ebenfalls der GoBD. Die *IDV-Suite* stellt verschiedene Möglichkeiten bereit, um diese Anforderungen umzusetzen.

Andere Auswirkungen auf gesetzliche oder andere relevante Vorgaben werden nicht gesehen. Insgesamt werden dabei diese Auswirkungen durch die IT-Anwendung von der SIZ GmbH als mittleres Risiko bewertet.

2.5 Datenüberstellung in autorisierte Programme

Die IT-Anwendung liefert Daten an folgende autorisierte Programme aus:

- Die *IDV-Suite* besitzt eine Schnittstelle zu Bit-LifeCycle, die aber nur in ausgewählten Instituten zum Einsatz kommt.

Andere Datenübergaben in bereits bestehende Programme bestehen nicht. Insgesamt werden dabei diese Auswirkungen durch die IT-Anwendung von der SIZ GmbH als nur in einigen Instituten als relevant bewertet. Eine Vererbung des Risikos respektive Schutzbedarfes durch die Bit-Software muss seitens Institut bewertet werden.

3 Literaturverzeichnis (inkl. Angaben zum geprüften Projekt)

Bei der Prüfung wurden u. a. folgende Artefakte[4] vollständig berücksichtigt, im Dokument selbst werden weitere Referenzen durch eckige Klammern gekennzeichnet und dabei jeweils die verständliche Kurzbezeichnung des Dokumentes angegeben, z. B. [HGB, §238]:

[4] Berücksichtigte Artefakte (SW-Teile und Dokumente) werden in den Testierungsdokumenten mit abkürzender Notation der Quelle hier mit [<lit-nr>] bezeichnet, wenn dieses Artefakt im Literaturverzeichnis auftaucht. Konkrete Inhalte innerhalb dieser Quelle werden dabei möglichst auch detaillierter angegeben:
[<lit-nr>, <Abschnitt>] Der Abschnitt kann dabei auch aus der Abschnittsnummer gebildet werden
[<lit-nr>, S.<Seitennummer>] Als Seitenangabe im Dokument
[<lit-nr>, XYZ] wenn XYZ in der speziellen Dokumentenform eine Stelle eindeutig kennzeichnet, bei

[2] Arbeitshilfe für die Beurteilung von Qualitätseigenschaften bei Fremdsoftware (Erstveröffentlichung: Fachmitteilungen Nr. 7 vom 31. 3. 1999 durch den Fachausschuss OPDV, Anm. d. Red.)

[8] TÜViT im Rahmen der Überarbeitung der Checkliste für das Projekt TRAVIC Jan 2005

[16] AE-Modell der SIZ GmbH

[26] IT-Revision, Schriftlicher Lehrgang in 10 Lektionen, Management Circle Edition, 1. Auflage (2007)

[201] IDV-Suite Testumgebung und Testvorgehensweise, Version 4.0 23.07.2015
16.08.2015 19:58 1.226.252 \150817 E Unterlagen\Richtlinien und Dokus Stromwerken\IDV-Suite - Testumgebung und Testvorgehensweise.pdf

[331] SIZ-Foliensatz IDV-Suite, MaRisk-konforme Dokumentation von Excel- und Access-Dateien, Gerald Schmidhuber / SIZ, Sparda-Bank West eG, 19. August 2014

[334] 16.11.2015 14:03 5.945.874 /151116 E Nachlieferung/ATDLL_La 3.wmv

[338] 16.11.2015 14:03 4.299.662 /151116 E Nachlieferung/ATDLL_La 49.wmv

[339] 16.11.2015 14:03 2.872.725 /151116 E Nachlieferung/ATDLL_La 60.wmv

[340] 16.11.2015 14:03 4.288.405 /151116 E Nachlieferung/ATDLL_La 75.wmv

[345] 16.11.2015 14:04 5.238.085 /151116 E Nachlieferung/ATDLL_La 99 FreigabeAufhebenBeiChecksummeaenderung.wmv

[346] 16.11.2015 14:04 11.065.462 /151116 E Nachlieferung/ATDLL_La_100.wmv

[347] 16.11.2015 14:04 5.165.595 /151116 E Nachlieferung/ATMDA_La_49.wmv

[355] 16.11.2015 14:04 3.270.751 /151116 E Nachlieferung/ETXLAM_La_1_2_Checklisten_Freigabe_Initiierung.wmv

[358] 16.11.2015 14:05 6.934.099 /151116 E Nachlieferung/ETXLAM_La_27_Dateiberechtigung.wmv

[367] IDV-Suite Testfallvideos Neuerungen 4.0
16.11.2015 14:05 33.255 /151116 E Nachlieferung/IDV-Suite - Testfallvideos Neuerungen.pdf

[368] 16.11.2015 14:05 5.319.680 /151116 E Nachlieferung/IDV-Suite - Testfälle Applikation (Wt).doc

[370] 16.11.2015 14:05 133.120 /151116 E Nachlieferung/IDV-Suite - Testfälle Module (Nt).doc

[441] 16.11.2015 14:09 22.868.404 /151116 E Nachlieferung/Nt 2.wmv

[447] 16.11.2015 14:12 389.609 /151116 E Nachlieferung/TestdokumentationSWLC501SchnittstelleIDV-Suite.docx

[503] Klausel zu Rechten an Arbeitsergebnissen, 14.09.2015
16.11.2015 14:16 142.098/151116 E Nachlieferung/Richtlinien und Dokus Stromwerken/DirkWinterRechteEntwicklung.pdf

[504] Entwicklungsumgebung Version 2.0
16.11.2015 14:16 38.993 /151116 E Nachlieferung/Richtlinien und Dokus Stromwerken/Entwicklungsumgebung Stromwerken.pdf

[505] 16.11.2015 14:16 197.291 /151116 E Nachlieferung/Richtlinien und Dokus Stromwerken/IDV-Suite - Einbindung des Access-Addins Schablone.doc.docx

Tabellenkalkulationsprogrammen z. B. die Zellennummern.
Für allgemein bekannte Literaturhinweise wird statt der numerischen Angabe auch die abkürzende Bezeichnung im Text verwendet, auch wenn dieses Schriftstück nicht im Literaturverzeichnis auftaucht.

[509] IDV-Suite Implementierungsleitfaden, Version 4.0
16.11.2015 14:16 4.540.088 /151116 E Nachlieferung/Richtlinien und Dokus Stromwerken/IDV-Suite Implementierungsleitfaden.pdf

[511] IDV-Suite Handbuch V4.0 mit 126 Seiten ohne Datum
16.11.2015 14:16 4.928.414 /151116 E Nachlieferung/Richtlinien und Dokus Stromwerken/IDV-Suite.pdf

[514] Projektmanagement Softwareentwicklungsprozess Programmierrichtlinien Version 2.3, www.stromwerken.de - Stand 23.09.2015
16.11.2015 14:16 498.244/151116 E Nachlieferung/Richtlinien und Dokus Stromwerken/Projektmanagement-Softwareentwicklungsprozess-Programmierrichtlinien Stromwerken.pdf

[516] Qualitätssicherung für die Entwicklung von Anwendungen, Version 1.4, Stand 03.11.2015
16.11.2015 14:16 275.227/151116 E Nachlieferung/Richtlinien und Dokus Stromwerken/Qualitätssicherung für die Entwicklung von Anwendungen Stromwerken.pdf (ersetzt [205])

[517] Klausel zu Rechten an Arbeitsergebnissen, ohne Datum
16.11.2015 14:16 2.671.308 /151116 E Nachlieferung/Richtlinien und Dokus Stromwerken/RolfLangenbergRechteEntwicklung.pdf

[519] Wartungsvertrag (Muster einer Sparkasse)

[520] Lizenz- und Nutzungsbedingungen der Firma Stromwerken für die Software IDV-Suite und die (ggf.) zusätzlichen Module der IDV-Suite Excel-Sheet-Checker, ExcelTracker, AccessTracker, Access-Checker, Excel-File-Compare, ExcelProtect, Excel-Sheet-QA

[521] Anlage technische und organisatorische Maßnahmen 20140313 SIZ

4 Zusammenfassende Bewertung der IT-Anwendung aus Sicht der Stellungnahmen

Programmfreigabeerklärung (ähnlich Anlage zur Stellungnahme Nr. OPDV 1/2015 des Fachausschusses OPDV)			
	Thema / Unterthema		Details siehe Abschnitt
Ausreichend erfüllt	**Projektverantwortung, Erklärung zur Projektleitung**		5
Ausreichend erfüllt	**Benutzer / Fachbereiche**		6
		Es muss sichergestellt sein, dass die fachlichen Anforderungen erfüllt wurden	6.1
		Es muss sichergestellt sein, dass die gesetzlichen Anforderungen erfüllt wurden	6.2
		Die Funktionsfähigkeit muss durch Test nachgewiesen worden sein	5.3
Ausreichend erfüllt	**Produktion, Erklärung zur (EDV-/IT-) Organisation**		7

Hinweise zur Nutzung des Ergebnisses:

- [IDW PS 850, Tz90] fordert: *Lassen sich für die Auftragsdurchführung bedeutsame Sachverhalte durch den projektbegleitenden Prüfer sachlich nicht abschließend beurteilen, so sind in entsprechender Anwendung der IDW Prüfungsstandards: Verwendung der Arbeit eines anderen externen Prüfers (IDW PS 320) und Verwertung der Arbeit von Sachverständigen (IDW PS 322) sachverständige Dritte hinzuzuziehen.* ***Die unbesehene Übernahme fremder Ergebnisse ist nicht zulässig****. Der projektbegleitende Prüfer hat die Untersuchungen und Feststellungen Dritter zumindest kritisch zu würdigen. Die Verwertung von Untersuchungen und Feststellungen Dritter durch den Wirtschaftsprüfer hängt von deren Kompetenz und beruflicher Qualifikation nach Maßgabe der Erfordernisse der Unabhängigkeit, Gewissenhaftigkeit, Unparteilichkeit, Unbefangenheit und Eigenverantwortlichkeit ab*.
  Seitens einsetzendem Institut ist zur Nutzung der hier vorliegenden Programmfreigabe eine kritische Würdigung der Aussagen der SIZ GmbH zwingend erforderlich.

- [MaRisk, AT7.2, Tz3] fordert in der Kommentierung: „*Bei der Abnahme durch die fachlich und die technisch zuständigen Mitarbeiter steht die Eignung und Angemessenheit der IT-Systeme für die spezifische Situation des jeweiligen Instituts im Mittelpunkt. Gegebenenfalls vorliegende Testate Dritter können bei der Abnahme berücksichtigt werden, sie können die Abnahme jedoch nicht vollständig ersetzen*“.

- Der Prüfer weist darauf hin, dass die vorliegenden Fakten zum Zeitpunkt der Prüfung ausreichend waren, um eine Programmfreigabe zu erklären [IDW PS951, Tz112]. Diese Aussage kann jedoch nicht auf beliebige Zeiträume ausgedehnt werden [IDW PS951, Tz110]. Nicht ausreichende Umsetzungen [IDW PS951, Tz114] führten zur Nennung von Auflagen im Abschnitt *4.1 Auflagen*.

- [IDW PS 880, (54)]: Der vorliegende Prüfbericht ersetzt keine *EDV-Systemprüfung in folgenden Prüffeldern* des Institutes:
  • *Aufbauorganisation des EDV-Bereiches, z.B.*
  – *Eingliederung der EDV-Abteilung in die Unternehmensorganisation*
  – *Funktionstrennung innerhalb der EDV-Abteilung*
  • *Arbeitsabwicklung in der EDV-Abteilung*
  • *Arbeitsabwicklung in den Fachabteilungen*
  – *organisatorisches Umfeld und Verantwortlichkeiten*
  – *Einrichtung interner Kontroll- und Abstimmungsverfahren*
  • *Sicherung der Funktionsfähigkeit der EDV, insbesondere*
  – *räumliche Sicherheit*
  – *hardwaremäßige Sicherheit*
  – *Datensicherung, Wiederanlaufverfahren*.

- Bei der Nutzung des vorliegenden Prüfberichtes ist zu berücksichtigen, dass die Software losgelöst vom organisatorischen Umfeld geprüft wurde, in dem sie zum Einsatz kommen wird. Da Anwendungssysteme mittels Tabellensteuerungsdaten und/oder Erweiterung des Programmcodes auf die Bedürfnisse und Verhältnisse des Anwenders eingestellt werden, kann mit der Prüfung lediglich bestätigt werden, daß die Software bei sachgerechter Anwendung eine korrekte Nutzung bzw. Rechnungslegung ermöglicht, die den Grundsätzen ordnungsmäßiger Buchführung entspricht [IDW PS 880, (45)].

Im Rahmen der oben genannten Nutzungsbedingungen für die Programmfreigabe erteilt der Prüfer entsprechend der obigen Tabelle zur Einhaltung der Anforderungsgruppen die Programmfreigabe nach OPDV 1/2015 für die IT-Anwendung *IDV-Suite* und erklärt ergänzend nach [IDW PS 880, (46)] folgendes: Diese von mir geprüfte Software, über deren Prüfung der vorliegende Prüfbericht mit Datum vom 03.02.2016 14:14 informiert, ermöglicht bei sachgerechter Anwendung eine den Grundsätzen ordnungsmäßiger Buchführung entsprechende Nutzung.

Unterschriften finden sich auf der letzten Berichtsseite.

4.1 Auflagen

Die Kenntnis der Produktbeschreibung, mithin aller Dokumente, die die Eigenschaften der IT-Anwendung beschreiben, **wird** als verbindliche Vorgabe **vorausgesetzt**. Eine Aufstellung dieser Dokumente findet sich im Abschnitt *1.2.2 Produktbeschreibung*.

Im Betrieb sind durch das einsetzende Institut die folgenden Auflagen einzuhalten.

- Hinsichtlich der Umsetzung von MaRisk AT7.2 durch die hier geprüfte IT-Anwendung muss im Rahmen der Prüfung darauf hingewiesen werden, dass entsprechend Handbuch „*Die IDV-Suite unterstützt Unternehmen im Umgang mit …*“ [511, 2 Einleitung] nur eine Unterstützung aber keine inhaltliche Freigabefunktion zur Verfügung gestellt wird. **Im Institut ist damit organisatorisch a) sicherzustellen, dass ein ausreichend wirksamer Freigabeprozess** (PEV) **unter Nutzung der IT-Anwendung definiert und b) im Anweisungswesen entsprechend legitimiert wird**. Der Implementierungsleitfaden beschreibt hierzu weitere Maßnahmen [509, 14. Organisatorische Voraussetzungen vor Produktivnahme].
- Für MS-Access weichen die Funktionen geringfügig vom Umgang mit Excel ab, daher sind im Institut:
  - Sicherzustellen, dass für die produktiv genutzten ACCESS-Dateien auch eine Freigabe vorliegt; die Trackerfunktion wird je nach konkreter Einbindung potenziell erst aktiv, wenn sie jeweils vor der Datenbank gestartet wurde [505], [509, 10.2. User-Setup für MDA-Addin für Access]. Die Produktdokumentation weist dazu per Warnhinweis an: „*Nach jedem Start von Access müssen Sie den AccessTracker aktiv anschalten, er wird nicht automatisch gestartet. Starten Sie erst den AccessTracker und dann die Datenbank, die Sie bearbeiten möchten*“.
- Bei der Freigabe der Anwendung über die IDV-Suite kann die Freigabe durch einen Klick einer Person erfolgen. Die Sparkasse muss ggf. organisatorisch sicherstellen, dass die gemäß OPDV 1/2015 Freigabebeteiligten ihre Zustimmung erteilt haben. Formal hat die Freigabe entsprechend der angewiesenen Verfahren zu erfolgen.

Sofern in dieser Liste Auflagen enthalten sind, die im Institut weder technisch noch organisatorisch umgesetzt werden können liegen zu tragende Risiken vor. **Bei diesen Risiken sind seitens des Instituts neben der Bereitstellung ausreichender finanzieller Risikotragfähigkeit auch** die **gesetzlichen Vorgaben umzusetzen** [PrüfbV, § 14 (1)].

5 Detailbewertung der Bereitstellungs- und Wartungsprozesse (Projektverantwortung)

Zur Ermöglichung einer erfolgreichen Programmpflege [IDW PS 880, (28)] hat der Hersteller einen auf SCRUM basierenden Projektmanagementprozess festgelegt [514, 4. Projektmanagementmodell / Softwareentwicklungs]. Dieser greift entscheidend in Entwicklung und Qualitätssicherung ein. Die Beschreibung legt dar, dass die wesentlichen Ziele des SCRUM-Prozesses verstanden wurden und auch schon Optimierungen an die Organisation des Herstellers durchgeführt wurden.

5.1 Nachvollziehbares Projektmanagement

Es liegen Beschreibungen sowohl des Entwicklungs- [514] als auch des QS-Prozesses vor [516].

Die OPDV 1-2015 fordert die Nennung von Standards bei der Entwicklung und Qualitätssicherung, die ISO900x fordert die Existenz von dokumentierten und gelebten Prozessen. Der Hersteller hat eine Entwicklung nach dem internationalen SCRUM-Standard angewiesen [514, 4. Projektmanagementmodell / Softwareentwicklungs]. Dies hat direkte Auswirkungen auf den Entwicklungsprozess [514] und auf den QS-Prozess [516].

Als wichtige Festlegung hat dabei die kompetenzgerechte Herstellerfreigabe zu gelten. Die Prozessdokumentation [516, 4.8. Freigabe] definiert als Verantwortlichen für die Freigabe den „*Produktmanager*“ und konkretisiert die zu erstellende Dokumentation durch Einchecken des Komplett-Zip. Die formal in dieser Anweisung fehlende Unterschrift der Geschäftsleitung wird durch die Personalunion zwischen Produktmanager und Geschäftsführer geheilt.

Eine Nennung der zur Entwicklung genutzten Tools und Entwicklungsumgebungen liegt vor [504].

Auf regelmäßige Management-Reviews der Projekt-Aktivitäten [8] kann im vorliegenden Fall wegen Personalunion zwischen Geschäftsführung und Produktverantwortung verzichtet werden.

Eine explizite vertragliche Zusage nach [MARISK, BTR 4 Operationelle Risiken] und [COBIT4.0, AI2.10] „*Bedeutende Schadensfälle sind unverzüglich hinsichtlich ihrer Ursachen zu analysieren*“ liegt nicht vor**.** Die in der Vergangenheit aufgetretenen und in vielen Fällen dem Prüfer bekannt gewordenen Supportfälle wurden aber ausnahmelos und schnell gelöst, insofern kann der Prüfer hier keinen Änderungsbedarf erkennen.

Wartungsvertragliche Regelungen sind vorhanden, aufsichtsrechtlich aber nicht verpflichtend [FAIT2, Tz64].

5.1.1 Projektleitung

Eine Detailprüfung der Projektleitungsaufgaben [COBIT4.0, PO10.5] wird im Rahmen der Prüfung nicht durchgeführt, da in diesem Thema keine Risiken für ein nutzendes Institut erkennbar sind.

Das Anforderungs- und Fehlermanagement [8], [IDW PS 880, Tz23] wird durch das Standard-Tool Mantis unterstützt, die weiteren zur Entwicklung genutzten Tools und Entwicklungsumgebungen sind dokumentiert [504].

Der geleistete Support [11], [COBIT4.0, PO1.1] deckt nach Erfahrung des Prüfers alle Anforderungen ab.

5.1.2 Spezialprojekte

5.1.2.1 Elektronische Archivierung und Dokumentenmanagementsysteme

Der Implementierungsleitfaden ist als Produktbeschreibung heranzuziehen, siehe Abschnitt *1.2.2 Produktbeschreibung*. Er weist darauf hin [509, 2.2.8. Handelsrechtliche Archivierung der Unterlagen der IDV-Suite], dass die handelsrechtliche Archivqualität insbesondere bei der Verarbeitung GoBD-relevanter IT-Anwendungen, der genutzten Datenbank potenziell – und nur in diesen Spezialfällen- nicht ausreichend ist. Dieser, nur für sehr selten zutreffende Rahmenbedingungen, auftretende Mangel lässt sich durch Archivierung der Unterlagen –in den betroffenen Spezialfällen- in „echten Archivsystemen“ heilen. Für diese Fälle kann ein Komplettreport über die Freigabe und die dabei freigegebene Version der Excel- oder Access- Datei aus dem Datenbestand exportiert werden. Die Stellungnahme 1/2015 weist darauf hin, dass es diese Spezialfälle eigentlich nicht geben dürfte.

5.2 Fehlerfreie Herstellung der IT-Anwendung

5.2.1 Anforderungserfassung (AE)

Im Anforderungsmanagement sind nicht nur fachliche, sondern auch juristische, sicherheitstechnische und organisatorische Anforderungen zu betrachten [IDW EPS 850, Tz63] und [IDW EPS 850, Tz64]. Die Festlegung des QS-Prozesses [516, 4.2. Konzeption neuer und geänderter Anwendungsfunktionen] legt die Verantwortung für die juristische Umsetzbarkeit der Anforderungen dem Produktmanager auf, der als GF des Herstellers juristische Fragen verantwortet und organisatorische Maßnahmemöglichkeiten aus Revisionssicht beurteilen kann. Sicherheitstechnische Fragestellungen wurden im Rahmen der Prüfung ergänzt.

Im Rahmen der Releasebereitstellung wurden auch neue Funktionen umgesetzt [9, 3.2.2], [IDW PS 880, Tz5]. Das Handbuch [511, 12 Veränderungen zur Vorversion] enthält die ReleaseNotes. Das Testkonzept [367] geht auf die Neuerungen ein.

Um sicherzustellen, dass dem nutzenden Institut die im Rahmen der Produktbeschreibung erforderlichen Inhalte übermittelt werden, werden den Interessenten „Demo-Versionen“ zur Verfügung gestellt, die den kompletten Funktionsumfang für einen abgegrenzten Zeitraum bereitstellen. Eine Prüfung, ob hierbei sichtbare Produkteigenschaften auch in den Produktbeschreibenden Dokumenten erklärt werden, kann somit entfallen.

Hinsichtlich der erforderlichen Abgrenzung benennt das Implementierungshandbuch [509, 2. Setup / Vorüberlegungen / Sicherheit / Restriktionen] Abgrenzungen bzw. organisatorische Voraussetzungen. Der Prüfbericht geht im Abschnitt *4.1 Auflagen* auf Abgrenzungen ein.

5.2.2 Architektur und Schnittstellendesign, Geschäftsprozessmodellierung (GPM)

5.2.2.1 Architektur und Betriebssicherheit

Diverse Gesetze (z. B. [KWG, §11]) und Verordnungen (z. B. [IDW PS 880, Tz3], [IDW PS 880, Tz8], [FAIT2, Tz14]) fordern eine ausreichende Berücksichtigung des Themas Sicherheit. Hierbei muss die Sicherheit als Oberbegriff auch für Verfügbarkeit, Integrität und Vertraulichkeit gesehen werden. Sicherheitsaspekte sind zum Teil technisch umgesetzt und müssen manuell ergänzt werden. Der Implementierungsleitfaden [509, 2.2.2. Datenbank] beschreibt organisatorische Maßnahmen.

Das erwartete Architekturgremium [COBIT4.0, PO3.5] ist beim Hersteller definiert [514, 5. IT-Architektur], beim dem auch die Geschäftsführung des Herstellers Mitglied ist.

5.2.2.2 Schnittstellen und sicherer Datenaustausch

Schnittstellen stellen per sé ein gewisses Ausfallrisiko dar. Dies wird in einem Testprotokoll [441] ausreichend behandelt.

Die Reaktionen bei einem Ausfall [COBIT4.0, AI2.4] der Datenbankschnittstelle sind im Implementierungshandbuch [509, 2.3 Auswirkungen der Nichtverfügbarkeit der Datenbank] beschrieben. Die Schnittstelle zwischen IDVSUITE 4.0 und BitSWLC 5.0.1 ist in einem Testprotokoll berücksichtigt [447].

Sofern die Schnittstelle zu Bit-SWLC genutzt wird, enthält der Implementierungsleitfaden 509, 17. Anhang 3 – Bit- Informatik SoftwareLifeCycle (SWLC) Daten-Schnittstelle] eine Beschreibung der Schnittstelle zu diesem System und das Testprotokoll [447] bestätigt die erfolgreiche Nutzung in beiden Schnittstellenrichtungen.

5.2.2.3 Integration in den Geschäftsprozess

Die Abgrenzung zwischen technisch umgesetzten Plausibilisierungen und organisatorisch umzusetzenden Kontrollmaßnahmen stellt sich im Rahmen der Prüfung wie folgt und insgesamt ausreichend dar:

- Berechtigungen von Nutzern sind einrichtbar, einige davon basieren auf Berechtigungen im Betriebssystem, die im Rahmen der Prüfung nicht weiter geprüft wurden und einige auf Berechtigungen in der IT-Anwendung. Zu letzteren liegen Testprotokolle vor, die deren Wirksamkeit bestätigen.
- Die IT-Anwendung stellt folgende technischen Plausibilisierungen im Geschäftsprozess zur Verfügung, die jeweils von den konkreten Konfigurationswerten abhängen:
  - Eine vom Nutzer zu beantwortende Befragung zum Schutzbedarf bzw. Risiko kann zwingend vorgenommen werden. Dabei vorgenommene Eingaben werden nicht plausibilisiert.
  - Eine ausreichend schutzwürdige IT-Anwendung ohne Freigabeerklärung kann nach Ablauf einer Zeit von der Nutzung ausgenommen werden.
  - Zur Unterstützung der Vertraulichkeit wird eine Passwort-Option bereitgestellt, die mit den Mitteln des Excel eine unzulässiges Öffnen der Excel-Datei unterbindet.
- Inhaltliche Plausibilisierungen finden nicht statt, sie sind -sofern erforderlich- organisatorisch umzusetzen. Der Implementierungsleitfaden [509, 14. Organisatorische Voraussetzungen vor Produktivnahme] benennt auch die erforderliche Fachlichkeit bzw. weist auf Workshops hierzu hin.

Das Datenmodell [8] ist für Schnittstellenkomponenten dokumentiert, der Implementierungsleitfaden [509, 17.4. Tabelle SwlcEingang] ff beschreibt das technische Datenmodell an der Schnittstelle.

5.2.3 Einhaltung von Programmierkonventionen

Programmierkonventionen, die auch die BSI-Vorgaben [GS-KAT, M2.134 (Richtlinien für Datenbank-Anfragen)] berücksichtigen, sind definiert [514].

Im Testkonzept [514, 4. Projektmanagementmodell / Softwareentwicklungs] wird festgelegt, dass entweder andere Entwickler oder der Produktverantwortliche Tests durchzuführen haben. Beide Gruppen kontrollieren auch Programmierkonventionen.

5.2.4 Programm- bzw. Systemdokumentation

Die grobe Architektur wird im Abschnitt *1.2.2 Produktbeschreibung* dargestellt, zu spezifischen Datenmodelle siehe unten. Die für eine Produktbereitstellung erforderlichen Informationen sind herstellerintern dokumentiert.

Der Implementierungsleitfaden [509, 17.4. Tabelle SwlcEingang] ff beschreibt das technische Datenmodell an der Schnittstelle.

5.2.5 Durchführung und Dokumentation der Entwicklertests

Die QS-Anweisung [516, 3.6.1. Entwicklertests] weist an, Entwicklertestprotokolle als Videos auf dem für QS-Dokumente relevanten Server zu hinterlegen. Die Verantwortung liegt beim Produktmanager, der als GF des Herstellers in der hier relevanten Verantwortlichkeit handelt.

5.3 Nachweis einer vollumfänglichen Qualitätssicherung

Siehe auch [SITB, K341(Test und Freigabe)].

5.3.1 Nachweischarakter von Testergebnissen

Zur Beweiskraft der Testunterlagen liefert die Prüfung folgende Ergebnisse:

- Die Testprotokolle wurden als Videos zur Verfügung gestellt, und belegen einen Umgang mit der zu testenden IT-Anwendung.
- Dem Prüfer ist bekannt, dass die IT-Anwendung in diversen Sparkassen erfolgreich im Einsatz ist.

5.3.2 Vollständige Qualitätssicherung

Die Einzelergebnisse der Testmaßnahmen aus Sicht der Prüfung:

- Funktionstests liegen als Videodokumentation vor.
- WhiteBoxtests, d.h. ein Vergleich der Oberfläche mit programmierten Abläufen sind dokumentiert [368].
- Die Zusatzmodule sind in einem Testprotokoll abgedeckt [370].
- Das Implementierungshandbuch [509, 2.2. Fälschungssicherheit / Passwortsicherheit / GoBD-relevante Dateien] benennt organisatorische Voraussetzungen zu Sicherstellung der Integrität.
- Tests zum Ausfall der Datenbank sind als Video-Protokolle vorhanden.
- Viele Videoprotokolle dokumentieren nicht nur sogenannte Positiv-Tests sondern auch die erforderlichen Negativ-Tests und berücksichtigen dabei die von der IT-Anwendung ausgehenden Risiken.

5.3.3 Lasttest

Lasttests stellen sich im Rahmen der Prüfung wie folgt dar:

- Dem Prüfer sind keine Fälle bekannt, in denen die IT-Anwendung mit der Anzahl der Nutzer ein Problem hätte. Lasttechnisch würde es sich dabei erwartungsgemäß um eine im Datenbanksystem konfigurierbare Grenze gleichzeitiger Datenbankzugriffe handeln.
- Im Rahmen des Geschäftsprozesses „Freigabe einer Datei“ wird auch der Excel-Sheet-Checker (ECC) aufgerufen. In der Vergangenheit kam es bei sehr großen Excel-Dateien zu signifikant langen Laufzeiten. Auch wenn hier inzwischen viele Optimierungen stattfanden, ist es weiterhin nicht auszuschließen, dass große Excel-Dateien weiterhin signifikante Laufzeiten verursachen. Im Einzelfall lässt sich das Laufzeitproblem aber immer durch einen separaten Arbeitsplatz und eine Kopie der Excel-Datei entschärfen.

5.3.4 Qualitätsmanagement

Das Erstellen von Videomitschnitten als Testprotokoll ist im Anweisungswesen hinterlegt [201].

Die zur Entwicklung genutzten Tools und Entwicklungsumgebungen sind dokumentiert [504].

Als Source Code Versionierungssystem wird das Standardtool Perfore benannt.

Als Projektmanagement Tool mit Dokumentationscharakter wird das Standardtool Mantis benannt [516, 3.2.1. Release].

5.4 Bereitstellung und Identifikation des Liefergegenstandes sowie seiner Quellen

Aussagen zu Versionen und entsprechenden Tools siehe im restlichen Prüfbericht.

5.4.1 Versionsverwaltung und Identifikation

5.4.1.1 Anwenderhandbuch und Hilfestellungen

Im Rahmen der Prüfung wurde das Handbuch überarbeitet. Die zuletzt geprüfte Version besitzt 126 Seiten, und ist inhaltlich an der Überschrift des Abschnittes [511, 6.10 Dateiberechtigungen (nur Excel)] erkennbar und daran, dass [511, 11 Anhang 5 – Standardfragensätze OPDV 1 / 2006 und Schutzbedarf 1 / 2015] mit einem abgrenzenden Warnhinweis beginnt.

5.4.1.2 Testkonzepte, Testprotokolle, Abnahmen und Freigabeerklärungen

Versionierungsaussagen in Testprotokollen wurden während der Prüfung überarbeitet und stellen jetzt keinen Mangel mehr dar.

6 Detailbewertung aus Sicht der Benutzer bzw. Fachbereiche

6.1 Sicherstellung der Vollständigkeit von fachlichen Anforderungen

Im Rahmen der Prüfung als fachliche Produktbeschreibung erforderliche Dokumente sind im Abschnitt *1.2.2 Produktbeschreibung* benannt, darüber hinaus werden Demo-Versionen (zeitlich begrenzte Vollversionen) zur Verfügung gestellt.

Neben der Installation sind organisatorische Maßnahmen für den Betrieb erforderlich. Das Implementierungshandbuch [509, 14. Organisatorische Voraussetzungen vor Produktivnahme] weist auf die organisatorischen Voraussetzungen hin. Der Prüfbericht ergänzt im Abschnitt *4.1 Auflagen*.

Das Implementierungshandbuch [509, 14. Organisatorische Voraussetzungen vor Produktivnahme] weist darauf hin, dass im Zusammenhang mit Schulungen [2, 1.1.5.2] auch Festlegungen der umzusetzenden Prozesse erforderlich sind.

Das Implementierungshandbuch [509, 14. Organisatorische Voraussetzungen vor Produktivnahme] weist darauf hin, dass Berechtigungsstrukturen [2, 1.1.5.4] zu definieren und umzusetzen sind.

Die Produktbeschreibung geht auf wesentliche Abgrenzungen ein, das Implementierungshandbuch wurde dazu im Rahmen der Prüfung ergänzt [509, 2.4. Was die IDV-Suite nicht kann].

Zur Sicherstellung eines wirksamen IKS [2, 1.1.4.2], [IDW PS 880, Tz15], [IDW PS 880, Tz23] weist das Implementierungshandbuch [509, 14. Organisatorische Voraussetzungen vor Produktivnahme] auf die Notwendigkeit hin, manuelle Kontrollprozesse zu definieren und umzusetzen.

6.2 Fachliche Berücksichtigung von gesetzlichen oder normativen Vorgaben

Die Verantwortung für die Kontrolle der Einhaltung aller gesetzlichen und normativen Vorgaben wird im Implementierungsleitfaden [509, 2.6. IDV-Suite Checkliste Implementierung] dem nutzenden Institut übertragen. Im Rahmen der Prüfung ergeben sich dabei folgende Detailergebnisse:

- Gesetze und Verordnungen, die durch die Software selber umgesetzt werden sollen, werden im Prüfbericht explizit angesprochen.
- Vorgaben, die erst bei deren Nutzung relevant sind, sind als umsetzbar festgestellt worden. Die genaue Umsetzungsvariante ist dabei aber durch das nutzende Institut zu definieren, entsprechende Parameter in der IT-Anwendung zu hinterlegen und anzuwenden.

6.2.1 BDSG

In der IT-Anwendung wird transparent, dass Anmeldeinformationen erfasst und in Form von Freigabetätigkeiten auch protokolliert und auf Reports dargestellt werden. Die IT-Anwendung erlaubt darüber hinaus, Beschreibungen und Testunterlagen von betrachteten Drittanwendungen zu hinterlegen. Der Prüfbericht weist darauf hin, dass auch dort durch die Mitarbeiter personenbezogene Daten hinterlegt werden könnten.

6.2.2 BetrVG

Accountdaten von Mitarbeitern werden gespeichert, siehe Abschnitt *6.2.1 BDSG*. Eine Kontrollmöglichkeit über Mitarbeiter kann der Prüfer hier nicht sehen.

6.2.3 GPSG

Handbuch [511] und Implementierungsleitfaden [509] enthalten Warnhinweise in roter Schrift, in Einzelfällen auch nur in Fettschrift.

[5] Geräte- und Produktsicherheitsgesetz

6.2.4 HGB

6.2.4.1 Aufbewahrungspflichten [HGB, §257]

Der Implementierungsleitfaden [509, 2.2. Fälschungssicherheit / Passwortsicherheit / GoBD-relevante Dateien] stellt implizit klar, welche Optionen zur Aufbewahrung bestehen. Eine handelsrechtliche Aufbewahrungspflicht besteht nur in Ausnahmefällen.

6.2.5 OWiG und MaRisk AT4.4.2 Compliance-Funktion

Der Implementierungsleitfaden [509, 14. Organisatorische Voraussetzungen vor Produktivnahme] benennt auch die Einbindung des Compliance-Beauftragten.

6.2.6 StGB

Die IT-Anwendung kann keine E-Mails empfangen sondern bietet nur die Möglichkeit, textuell vorbereitete Benachrichtigungs-E-Mails automatisiert zu versenden, ein Bezug zum StGB ist damit nicht sichtbar.

6.2.7 UrhG

Zur wirksamen Lizenzübertragung ist eine vollständige Kette zwischen Urheber und Lizenznehmer erforderlich. Im Rahmen der Prüfung wurden zur Vervollständigung der Kette auch die Rechteübertragungen der Urheber an den Hersteller übergeben [503] und [517].

6.2.8 AO (Abgabenordnung und Aufbewahrungsfristen), GoBD, GoBS und Verarbeitung buchungsrelevanter Geschäftstransaktionen

Die hier geprüfte IT-Anwendung selbst unterliegt der GoBD nicht. Test- und Freigabeunterlagen von GoBD-relevanten Drittanwendungen werden aber eventuell mit der hier geprüften IT-Anwendung erstellt und gespeichert. Nach GoBD unterliegen diese Unterlagen damit der GoBD. Die daraus resultierenden Folgen für die Aufbewahrung sind im Abschnitt *5.1.2.1 Elektronische Archivierung und Dokumentenmanagementsysteme* behandelt.

6.2.9 ZPO (Zivil-Prozess-Ordnung)

Der Implementierungsleitfaden [509, 2.2. Fälschungssicherheit / Passwortsicherheit / GoBD-relevante Dateien] stellt die Fälschungssicherheit [ZPO, §298a] dar.

6.2.10 weitere Stellungnahmen und Verlautbarungen des Fachausschuss OPDV

6.2.10.1 Stellungnahme Nr. 1/2003

Nach OPDV Stellungnahme Nr. 1/2003 sind rückrechenbare oder lesbare Passwortablagen unzulässig.

Der Excel-Sheet-Checker (ECC) bietet[6] die Funktion *Zentrale Ablage der Passwörter "für den Notfall"* an. Ein Umgang mit der zugehörigen Konfiguration ist im Institut zu beschließen.

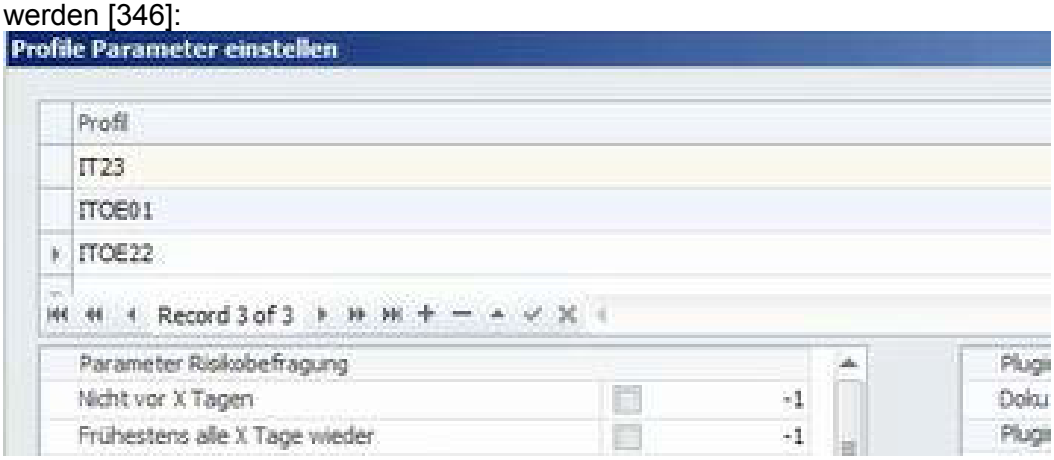
[6] http://stromwerken.de/produkte/excel-sheet-checker/excel-sheet-checker.html

Technische User benötigen rückrechenbare Passwortablagen. Der Implementierungsleitfaden [509, 2.2.3. Technischer User für den Datenbankzugriff] beschreibt die Nutzung des technischen Users.

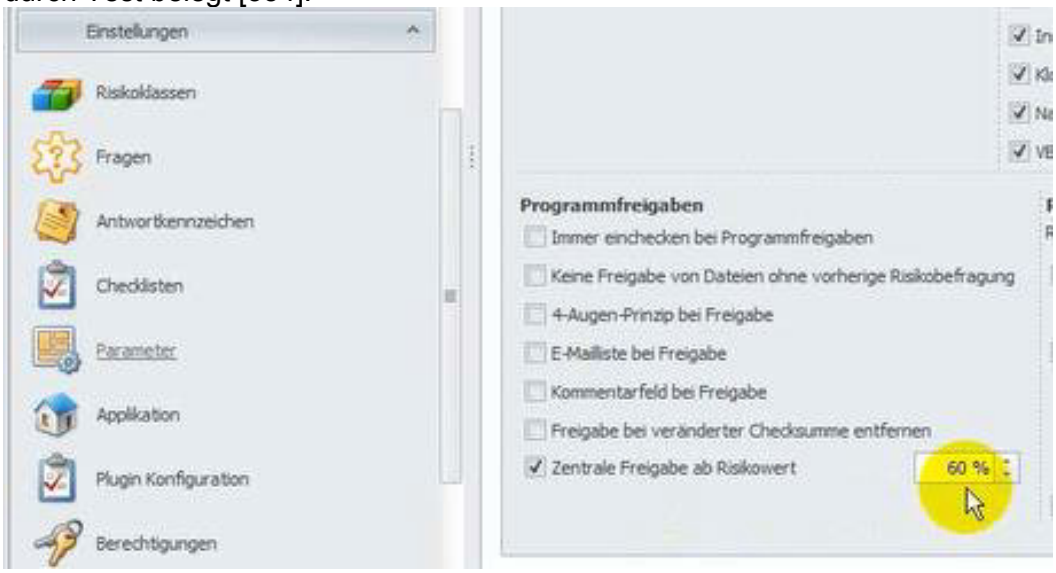
6.2.10.2 Stellungnahme Nr. 1/2015 Anforderungen an einen ordnungsgemäßen Programmeinsatz

Die IT-Anwendung unterstützt die Umsetzung der Stellungnahme Nr. 1/2015. Im Rahmen der Prüfung werden folgende Grenzen sichtbar:

- Die im jeweiligen Tracker für Access bzw. Excel in Feldern hinterlegten Dokumentationen können als Pflichtfelder konfiguriert werden [340]. Der Test belegt dabei allerdings, dass eine inhaltliche Kontrolle der Änderung nicht stattfindet. Jede Änderung zählt.
- Konfigurationsparameter können abhängig von der nutzenden OE angepasst werden [346]:

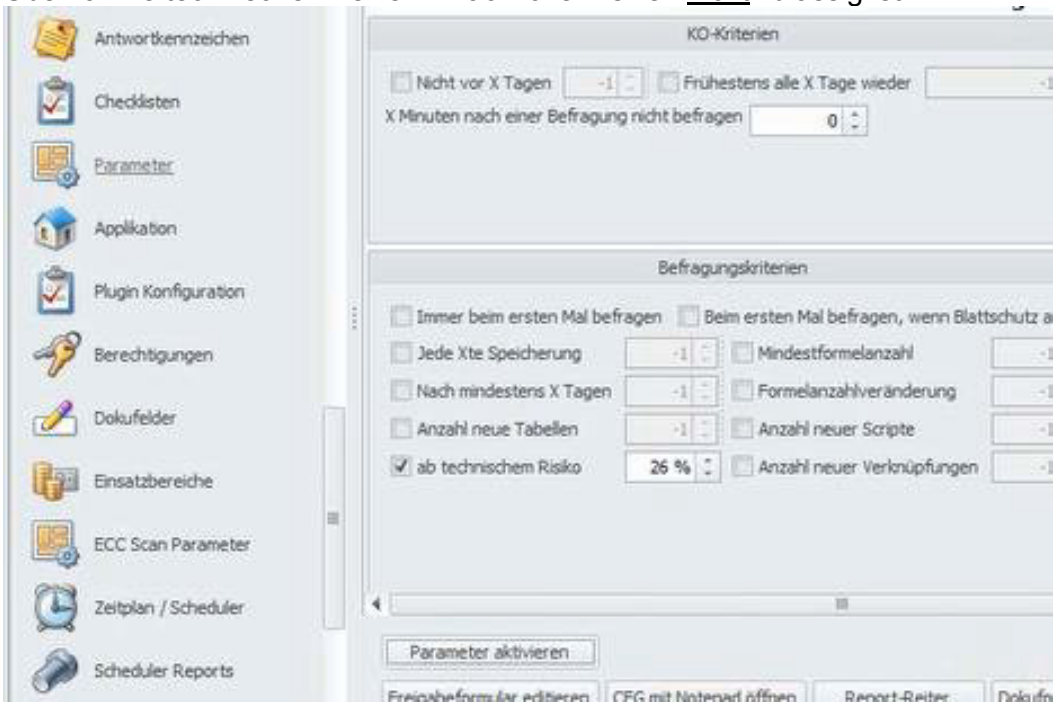


- Die IDVSUITE bietet die Möglichkeit, Freigaben ab einem einstellbaren fachlichen Risikowert nur zentral erteilen zu können, diese Auswahl ist in beiden Varianten durch Test belegt [334]:



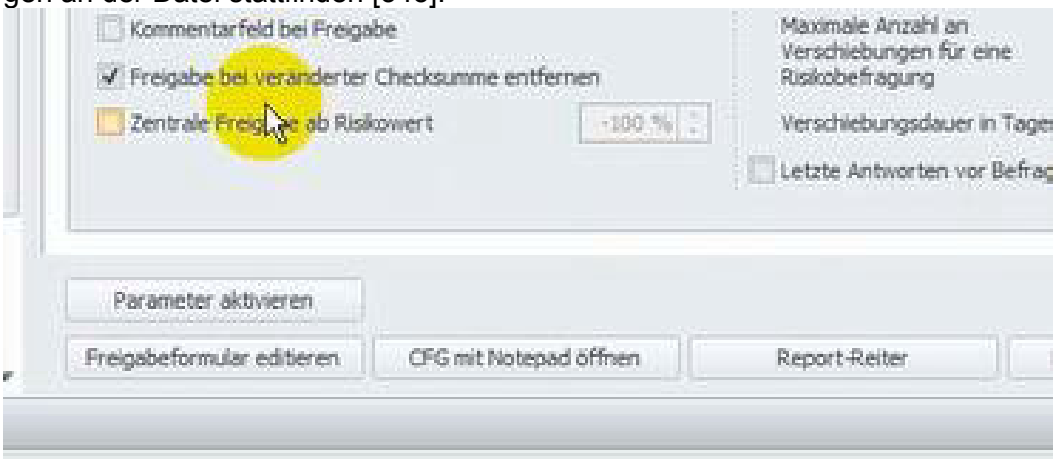
- Die IDVSUITE bietet die Möglichkeit, Risikofragen erst ab einem konfigurierbaren technischen Risikowert durchzuführen, die Funktion selbst ist per Testprotokoll bestätigt [338] [347]. Der Prüfbericht weist darauf hin, dass ein Automatismus zur

Übernahme technischer Risiken in fachliche Risiken nicht zulässig ist:



- Für die Schritte Freigabe-Initiieren und Freigabe-Abschließen können Checklisten hinterlegt werden [355]:

- Freigaben können automatisch aufgehoben werden, wenn funktionale Änderungen an der Datei stattfinden [345]:



Das Handbuch [511, 3 Die Neuerungen zur OPDV 1/2015] geht auf einige der nach 1/2015 geänderten Themen ein.

Sowohl das Handbuch [511, 5.3.2 Dateiüberwachung] als auch in der IT-Anwendung selber wird als Warnhinweis dargestellt, dass die Notwendigkeit einer Komplettüberwachung und damit automatischen Scans von Institutsvorgaben abhängt und nicht zwingend ist.

Das Handbuch [511, 5.7.9 Dokufelder] benennt „Report #54 Historisierte Parameter“ für die Einsatzfreigabe der hier geprüften IT-Anwendung.

Das Handbuch [511, 6.4 Plugin Menüleiste] benennt auch den „ Sign-Off-Prozess“, der Protokollcharakter besitzen kann.

Das Handbuch [511, 11 Anhang 5 – Standardfragensätze OPDV 1 / 2006 und Schutzbedarf 1 / 2015] enthält folgenden Warnhinweis: „*Bitte beachten Sie, dass die folgenden Standardtexte lediglich Vorschläge darstellen.* ***In jedem Fall muss das einsetzende Unternehmen die Texte prüfen und auf die eigenen Erfordernisse anpassen****. Dies betrifft insbesondere Textpassagen, die ggf. aufgrund der Rechtsform des einsetzenden Unternehmens aus rechtlicher Sicht Relevanz haben. Ferner sind Passagen, die eine Standardisierung im einsetzenden Unternehmen bedingen, anzupassen; dies könnte z. B. die explizite Nennung Standards für Testverfahren oder ähnliches sein*“.

Das Handbuch [511, 5.1 Start der IDV-Suite] benennt die Funktionalität „*können Reports erstellt … werden*“. Hierbei werden keine neuen Reports erstellt, sondern nur bestehende parametrisiert.

Über die IT-Anwendung können Berechtigungen zum Öffnen der Excel-Dateien vergeben werden, Tests belegen deren Wirksamkeit im Kontrollbereich der IT-Anwendung [358]. Aus Prüfungssicht ist darauf hinzuweisen, dass Excel-Dateien den Wirksamkeitsbereich der IT-Anwendung auch über Standardmethoden des Betriebssystems oder anderer Standardanwendungen, wie E-Mail verlassen können; die Excel-Dateien sind gemäß Herstellerdokumentation mit einem Datei-Öffnen-Passwort von „> 20 Zeichen mit 4 aus 4 Zeichengruppen (Groß/Klein/Zahlen/Sonderzeichen)“ [511, 3 Die Neuerungen zur OPDV 1/2015]) abgesichert und bieten somit über die Microsoft-Excel-Funktionalität einen komplexen Datei-Öffnen-Schutz. Vor hochgradig kriminellen Handlungen kann aber auch diese Absicherung nicht vollumfänglich schützen, da die technischen Möglichkeiten zur Sicherheit von Microsoft-Excel in sich beschränkt sind.

6.2.11 Standards des Institut der Wirtschaftsprüfer in Deutschland e.V. (IDW)

6.2.11.1 IDW PS 880

Das Ergebnis der nach [IDW PS 880, (5)] erforderlichen Bestandsaufnahme des Prüfungsobjektes befindet sich im Abschnitt *1.2.2 Produktbeschreibung*.

Die Umsetzung der GoBD-relevanten Vorgaben ist im Abschnitt *6.2.8 AO (Abgabenordnung und Aufbewahrungsfristen), GoBD, GoBS und Verarbeitung buchungsrelevanter Geschäftstransaktionen* beschrieben. Betroffen sind davon insbesondere [IDW PS 880, (7)], [IDW PS 880, (9)], [IDW PS 880, (10)], [IDW PS 880, (11)], [IDW PS 880, (16)].

Die Ergebnisse der Prüfung von Datensicherungsaspekten nach [IDW PS 880, (26)] und [IDW PS 880, (27)] findet sich im Abschnitt *7.4.5 Datensicherung (K318)*.

Die Ergebnisse der Prüfung der Programmentwicklung, -wartung und –freigabe nach [IDW PS 880, (28)] findet sich im Abschnitt *5 Detailbewertung der Bereitstellungs- und Wartungsprozesse (Projektverantwortung)*.

Nach [IDW PS 880, (44)] sind Kurzdarstellungen des Prüfungsergebnisses (z.B. einseitige Freigabebestätigungen) wegen zu geringem Informationsgehalt sowie wegen der Gefahr einer Fehlinterpretation unzulässig.

6.2.11.2 IDW PS 951

Im Rahmen der hier dokumentierten Programmfreigabe nach OPDV wird überprüft, welche Eigenschaften die zu prüfende IT-Anwendung besitzt. Es wird dabai maximal berücksichtigt, ob die vorgesehenen Kontrollmaßnahmen grundsätzlich geeignet sind (Typ1-Prüfung nach IDW PS 951). Die Prüfungssicherheit entsprechend Typ2 [IDW PS951, Tz16] ist damit explizit nicht erreicht [IDW PS951, Tz17].

Im Rahmen der hier dokumentierten Programmfreigabe nach OPDV wird die Innenrevision der bereitstellenden Organisation nicht überprüft, mithin die Aspekte [IDW PS951, Tz84], [IDW PS951, Tz85], [IDW PS951, Tz86] und [IDW PS951, Tz87] nicht hinterfragt. Aussagen der Innenrevision werden bei Bedarf zitiert und ggf. durch Stellungsnahmen des Prüfers ergänzt.

Zur Umsetzung der nach [IDW PS951, Tz94] und folgende relevanten Dokumentationsanforderungen und deren Umsetzung liefert der Abschnitt *1.6 Prüfgrundsätze und -vorgehen* die erforderlichen Erklärungen.

6.2.12 Control Objectives for Information and related Technology (COBIT) der Information Systems Audit and Control Association (ISACA)

Die für eine einzelne IT-Anwendung nach COBIT zu untersuchenden Aspekte (Control Objectives) werden in anderen Abschnitten dieses Prüfberichtes behandelt. Eine erste Referenz gibt hier der Index unter COBIT, eine Detailgegenüberstellung befindet sich in folgender Tabelle.

Control Objective aus COBIT	**Referenz auf Abschnitt des Prüfberichtes**
PO1.1 IT Value Management / Management des Wertbeitrags der IT	5.1 Nachvollziehbares Projektmanagement 5.1.1 Projektleitung
PO1.2 Business-IT Alignment / Ausrichtung Kerngeschäft und IT	5.4 Bereitstellung und Identifikation des Liefergegenstandes sowie seiner Quellen 5.4.1 Versionsverwaltung und Identifikation
PO2.1 Information Architecture Model / Informationsarchitekturmodell	5.2 Fehlerfreie Herstellung der IT-Anwendung 5.2.2 Architektur und Schnittstellendesign, Geschäftsprozessmodellierung (GPM) 5.2.2.3 Integration in den Geschäftsprozess
PO2.2 Enterprise Data Dictionary and Data Syntax Rules / Unternehmensweites Data Dictionary und Datensyntaxregeln	5.2 Fehlerfreie Herstellung der IT-Anwendung 5.2.2 Architektur und Schnittstellendesign, Geschäftsprozessmodellierung (GPM) 5.2.2.3 Integration in den Geschäftsprozess
PO2.3 Data Classification Scheme / Datenklassifikationsschema	5.2 Fehlerfreie Herstellung der IT-Anwendung 5.2.2 Architektur und Schnittstellendesign, Geschäftsprozessmodellierung (GPM) 5.2.2.3 Integration in den Geschäftsprozess

Control Objective aus COBIT	**Referenz auf Abschnitt des Prüfberichtes**
PO2.4 Integrity Management / Handhabung der Integrität	5.2 Fehlerfreie Herstellung der IT-Anwendung 5.2.2 Architektur und Schnittstellendesign, Geschäftsprozessmodellierung (GPM) 5.2.2.3 Integration in den Geschäftsprozess
PO3.3 Monitoring of Future Trends and Regulations / Überwachung von zukünftigen Trends und Bestimmungen	5.1 Nachvollziehbares Projektmanagement 5.1.1 Projektleitung
PO3.5 IT Architecture Board / IT Architekturgremium	5.2 Fehlerfreie Herstellung der IT-Anwendung 5.2.2 Architektur und Schnittstellendesign, Geschäftsprozessmodellierung (GPM) 5.2.2.1 Architektur und Betriebssicherheit
PO4.6 Roles and Responsibilities (Rollen und Verantwortlichkeiten	7 Detailbewertung aus Sicht des Betreibers 7.4 Sicherstellung eines sicheren IT-Betriebes 7.4.2 Identifikation / Authentisierung (K101)
PO4.9 Data and System Ownership / Daten und Systemeignerschaft	5.2 Fehlerfreie Herstellung der IT-Anwendung 5.2.2 Architektur und Schnittstellendesign, Geschäftsprozessmodellierung (GPM) 5.2.2.3 Integration in den Geschäftsprozess
PO4.11 Segregation of Duties / Funktionstrennung	5.2 Fehlerfreie Herstellung der IT-Anwendung 5.2.4 Programm- bzw. Systemdokumentation 6 Detailbewertung aus Sicht der Benutzer bzw. Fachbereiche 6.2 Fachliche Berücksichtigung von gesetzlichen oder normativen Vorgaben 6.2.1 BDSG 7 Detailbewertung aus Sicht des Betreibers 7.4 Sicherstellung eines sicheren IT-Betriebes 7.4.2 Identifikation / Authentisierung (K101)
PO5.5 Benefit Management / Nutzenmanagement	5.2 Fehlerfreie Herstellung der IT-Anwendung 5.2.2 Architektur und Schnittstellendesign, Geschäftsprozessmodellierung (GPM) 5.2.2.3 Integration in den Geschäftsprozess

Control Objective aus COBIT	**Referenz auf Abschnitt des Prüfberichtes**
PO10.5 Project scope statement / Beschreibung des Projektumfangs	5.1 Nachvollziehbares Projektmanagement 5.1.1 Projektleitung
PO10.7 Integrated Project Plan / Integrierter Projektplan	5.1 Nachvollziehbares Projektmanagement 5.1.1 Projektleitung
PO10.8 Project Resources / Projekt-Ressourcen	5.1 Nachvollziehbares Projektmanagement 5.1.1 Projektleitung
PO10.9 Project Risk Management / Projekt-Risikomanagement	5.1 Nachvollziehbares Projektmanagement 5.1.1 Projektleitung
PO10.10 Project Quality Plan / Projekt-Qualitätsplan	5.3 Nachweis einer vollumfänglichen Qualitätssicherung
PO10.14 Project Closure / Projektabschluss	5.1 Nachvollziehbares Projektmanagement 5.1.1 Projektleitung
AI1.4 Requirements and Feasibility Decision and Approval / Freigabe der Anforderungsdefinition und Machbarkeit	5.2 Fehlerfreie Herstellung der IT-Anwendung 5.2.1 Anforderungserfassung (AE)
AI2.1 High level Design / Grobdesign	5.2 Fehlerfreie Herstellung der IT-Anwendung 5.2.2 Architektur und Schnittstellendesign, Geschäftsprozessmodellierung (GPM) 5.2.2.1 Architektur und Betriebssicherheit
AI2.2 Detailed Design / Detailliertes Design	5.2 Fehlerfreie Herstellung der IT-Anwendung 5.2.2 Architektur und Schnittstellendesign, Geschäftsprozessmodellierung (GPM) 5.2.2.1 Architektur und Betriebssicherheit
AI2.3 Application Control and Auditability / Anwendungskontrollen und Nachvollziehbarkeit)	5.2 Fehlerfreie Herstellung der IT-Anwendung 5.2.2 Architektur und Schnittstellendesign, Geschäftsprozessmodellierung (GPM) 5.2.2.3 Integration in den Geschäftsprozess
AI2.4 Application Security and Availability / Sicherheit und Verfügbarkeit der Anwendung	5.2 Fehlerfreie Herstellung der IT-Anwendung 5.2.2 Architektur und Schnittstellendesign, Geschäftsprozessmodellierung (GPM) 5.2.2.2 Schnittstellen und sicherer Datenaustausch
AI2.8 Software Quality Assurance / Software-Qualitätssicherung	5.3 Nachweis einer vollumfänglichen Qualitätssicherung 5.3.4 Qualitätsmanagement

Control Objective aus COBIT	**Referenz auf Abschnitt des Prüfberichtes**
AI2.10 Application Software Maintenance / Wartung von Anwendungssoftware	5.1 Nachvollziehbares Projektmanagement
AI4.3 Knowledge Transfer to End Users / Transfer von Knowledge an den Endbenutzer	5.4 Bereitstellung und Identifikation des Liefergegenstandes sowie seiner Quellen 5.4.1 Versionsverwaltung und Identifikation 5.4.1.1 Anwenderhandbuch und Hilfestellungen
AI5.1 Procurement Control /Steuerung der Beschaffung	7 Detailbewertung aus Sicht des Betreibers 7.4 Sicherstellung eines sicheren IT-Betriebes
AI5.3 Supplier Selection / Lieferantenauswahl	7 Detailbewertung aus Sicht des Betreibers 7.4 Sicherstellung eines sicheren IT-Betriebes
AI5.5 Acquisition of Development Resources / Beschaffung von Entwicklungsressourcen	6 Detailbewertung aus Sicht der Benutzer bzw. Fachbereiche 6.2 Fachliche Berücksichtigung von gesetzlichen oder normativen Vorgaben
AI5.6 Acquisition of Infrastructure, Facilities and Related Services / Beschaffung von Infrastruktur, Einrichtungen und entsprechenden Diensten	7 Detailbewertung aus Sicht des Betreibers 7.4 Sicherstellung eines sicheren IT-Betriebes
AI7.1 Training /Schulung	5.4 Bereitstellung und Identifikation des Liefergegenstandes sowie seiner Quellen 5.4.1 Versionsverwaltung und Identifikation 5.4.1.1 Anwenderhandbuch und Hilfestellungen
DS5.3 Identity Management / Identitätsmanagement	7 Detailbewertung aus Sicht des Betreibers 7.4 Sicherstellung eines sicheren IT-Betriebes 7.4.2 Identifikation / Authentisierung (K101)
DS5.4 User Account Management / Management von Benutzerkonten	7 Detailbewertung aus Sicht des Betreibers 7.4 Sicherstellung eines sicheren IT-Betriebes 7.4.2 Identifikation / Authentisierung (K101)
DS5.7 Protection of Security Technology /Schutz von Sicherheitseinrichtungen	7 Detailbewertung aus Sicht des Betreibers 7.4 Sicherstellung eines sicheren IT-Betriebes 7.4.3 Key- Management (K108)

Control Objective aus COBIT	Referenz auf Abschnitt des Prüfberichtes
DS5.8 Cryptographic Key Management / Verwaltung kryptographischer Schlüssel	7 Detailbewertung aus Sicht des Betreibers 7.4 Sicherstellung eines sicheren IT-Betriebes 7.4.3 Key- Management (K108)
DS5.10 Network Security / Netzwerk-Sicherheit	7 Detailbewertung aus Sicht des Betreibers 7.4 Sicherstellung eines sicheren IT-Betriebes
DS5.11 Exchange of Sensitive Data / Austausch sensitiver Daten	7 Detailbewertung aus Sicht des Betreibers 7.4 Sicherstellung eines sicheren IT-Betriebes
DS11.4 Disposal / Entsorgung	7.3 Installation und Betriebsaufnahme

6.2.13 Mindestanforderungen an das Risikomanagement (MaRisk) der Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin)

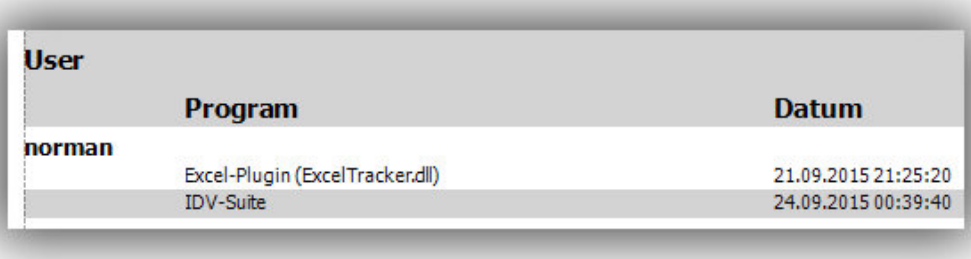
Die IT-Anwendung unterstützt bei der Umsetzung des AT 7.2. Inhaltlich sind dabei aber primär die eingesetzten Freigabeprozesse und damit organisatorische Maßnahmen erforderlich, auf die anderen Stellen des Prüfberichtes eingegangen wird.

6.3 Fachliche Administration der IT-Anwendung

Die IT-Anwendung kann und muss parametrisiert werden. Die hierbei hinterlegten Werte lassen sich kontrollieren [16], das Handbuch [509, 2.2.1. Anwendung] benennt „*Report #56 - Historisierte Parameter*“.

6.4 Korrekte Bedienung durch den Anwender

Abweichungen vom Standardverfahren sollten identifizierbar sein. Der Implementierungsleitfaden [509, 10.6. Deaktivierte Plugins finden] referenziert Report #60 zur Aufdeckung eines potenziell umgangenen technischen Schutzes:



User	Program	Datum
norman		
	Excel-Plugin (ExcelTracker.dll)	21.09.2015 21:25:20
	IDV-Suite	24.09.2015 00:39:40

Zur Meldung auftretender Störungen stellt der Produktüberlassungsvertrag [519, Präambel, Vertragsgegenstand] eine postalische Supportadresse zur Verfügung.

Für die Nutzung werden Einweisungen der Mitarbeiter empfohlen. Bei Fehleingaben [IDW PS 880, Tz17] von Administratoren steht ein Parameterreport zur Verfügung, bei Fehleinga-

ben von Nutzern sind organisatorische Kontrollprozesse erforderlich. Technische Plausibilisierungen finden an den wesentlichen Stellen nicht statt.

6.5 Internes Kontrollsystem (IKS) der Sparkasse

Erforderliche Kontrollen auf Zugriffsberechtigungen sind zu unterscheiden:

- Der Implementierungsleitfaden [509, 5. Programmordnerberechtigungen] beschreibt erforderliche Berechtigungen auf Ordnern. Die Kontrolle erfolgt mit den Standardmethoden des Betriebssystems.
- Der Implementierungsleitfaden [509, 10.6. Deaktivierte Plugins finden] benennt „*Report #60 Zugriff auf Programme / Module nach Usern*“ um Berechtigungen innerhalb der IT-Anwendung zu kontrollieren.

Zur Kontrolle der Verarbeitung [2, 3.3] liefert die Prüfung folgende Ergebnisse:

- Der von der IT-Anwendung primär unterstützte Geschäftsprozess ist bereits ein Kontrollprozess. Das Institut hat insofern festzulegen, welche Kontrollen auf diese Kontrollen stattfinden sollen.
- Zu Kontrollen stellt die IT-Anwendung diverse Reports zur Verfügung.

7 Detailbewertung aus Sicht des Betreibers

7.1 Sicherstellung der Vollständigkeit von technischen Anforderungen

Der Implementierungsleitfaden [509, 2. Setup / Vorüberlegungen / Sicherheit / Restriktionen] beschreibt Installationsalternativen mit Voraussetzungen [2, 1.1.2.5].

7.2 Technische Bereitstellung der Software durch den Lieferanten

In der IT-Anwendung ist ein zeitlich begrenzter Lizenzschlüssel als Kopierschutz enthalten, dies wird durch Nutzung der Demo-Version transparent [2, 1.1.2.11].

7.3 Installation und Betriebsaufnahme

Die im Rahmen der Einsatzfreigabe respektive Betriebsaufnahme erforderlichen Schritte werden im Implementierungsleitfaden [509] an verschiedenen Stellen zusammengefasst: [509, 2.5. IDV-Suite Checkliste - Vorarbeiten des einsetzenden Unternehmens] und [509, 2.6. IDV-Suite Checkliste Implementierung] enthalten Checklisten und verweisen dabei insbesondere auch auf die organisatorischen Voraussetzungen [509, 14. Organisatorische Voraussetzungen vor Produktivnahme].

Um den nach [HGB, §239] erforderlichen Nachweis einer unveränderten Nutzung erbringen zu können, beschreibt der Implementierungsleitfaden [509, 21. Anhang 7 – Tabellencharakter gemäß GoBD], welche Tabellen unter welchen Bedingungen andere Inhalte erhalten können.

7.4 Sicherstellung eines sicheren IT-Betriebes

7.4.1 Trennung der Umgebungen (K018)

Um eine Trennung der Umgebungen im Institut sicherstellen zu können, beschreibt der Installationsleitfaden [509, 13. Installation einer parallelen Testumgebung im Produktivnetz] eine entsprechende Installationsmöglichkeit.

7.4.2 Identifikation / Authentisierung (K101)

Der Implementierungsleitfaden [509, 14.1. Trennung zwischen Entwicklung und Test im IDV-Prozess über die IDV-Suite] beschreibt die Trennungsmöglichkeiten zwischen Entwickler und Tester.

Der Schutz der Daten besteht aus technischen und organisatorischen Maßnahmen [2, 3.1.3], [IDW PS 880, Tz23], [2, 3.1.16], [8]. Der Implementierungsleitaden [509] stellt die vorhandenen und zu ergänzenden Schutzmaßnahmen dar.

7.4.3 Key- Management (K108)

Die IT-Anwendung greift bei entsprechender Konfiguration auf den institutseigenen E-Mail-Dienst zu. Der Implementierungsleitfaden [509, 5.1.1. Sicherheit von SMTP-Servern] liefert die für die Absicherung des Mail-Servers erforderlichen Informationen [COBIT4.0, DS5.7].

Der Implementierungsleitfaden [509, 2.2.3. Technischer User für den Datenbankzugriff] beschreibt den zum Schutz der hinterlegten Account-Daten [2, 1.2.7.6], [4], [IDW PS 880, Tz17], [IDW PS 880, Tz24]), [GS-KAT, M2.7] des technischen Users genutzten Verschlüsselungsalgorithmus grob und als proprietär.

ODBC-Verbindungen gelten nach BSI als nicht immer ausreichend sicher [GS-KAT, G 4.27 Unterlaufen von Zugriffskontrollen über ODBC][7]. Die IT-Anwendung dokumentiert im Implementierungsleitfaden [509, 2.2.5. ODBC und Passwortsicherheit] daher eine leicht abgewandelte Nutzungsform zur Umgehung dieser Sicherheitslücken.

7.4.4 Berechtigungskonzept (K115)

Details zum Berechtigungskonzept sind dokumentiert, Verweise siehe Abschnitt *6.5 Internes Kontrollsystem (IKS) der Sparkasse*.

Die Trackerfunktionen der IT-Anwendung können über AD-Gruppen ein- und ausgeschaltet werden [339]:

7.4.5 Datensicherung (K318)

[7] https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/g/g04/g04027.html

Die Datensicherung obliegt dem Institut. Der Implementierungsleitfaden [509, 18. Anhang 4 – Datensicherung] beschreibt die Datensicherungsmethoden auf dem Server.

8 Ergebnisse aus der Prüfung der Vorversion 3.0 aus 2012

8.1 Detailbewertung der Bereitstellungs- und Wartungsprozesse (Projektverantwortung)

8.1.1 Nachvollziehbares Projektmanagement

Bei dem Hersteller bestehen Vorgaben bzgl. der Durchführung des Entwicklungs- und Qualitätssicherungsprozesses. Diese genügen grundsätzlich den Anforderungen an ISO 9000.

Die bestehenden Vorgaben bzgl. der Durchführung des Entwicklungs- und Qualitätssicherungsprozesses erfüllen bei ordnungsgemäßer Umsetzung die Anforderungen.

8.1.1.1 Projektleitung

Der erforderliche Support [11], [COBIT4.0, PO1.1] wird über das SIZ wahrgenommen. Hier sind grundsätzlich ausreichend Kapazitäten vorhanden um die Anforderungen abzudecken.

8.1.2 Fehlerfreie Herstellung der IT-Anwendung

Die erforderliche Fehlerfreiheit [IDW PS 880, Tz28[8]] der Anwendung zur Verwaltung und Abwicklung des Programmfreigabe und –einsatzverfahrens kann grundsätzlich durch die Entwicklungs- und Qualitätssicherungsverfahren von stromwerken sichergestellt werden. Dies bedeutet jedoch nicht automatisch, dass die in den Excel- und Accessdateien erstellten Anwendungen fachlich und inhaltlich abgenommen sind. Dies muss individuell über das Programmfreigabeverfahren des einsetzenden Unternehmens gewährleistet werden.

8.1.2.1 Anforderungserfassung (AE)

Die Komponenten der Anwendung sind entsprechend unter Punkt 1.2.2 dargestellt.

Erforderliche vertragliche Vereinbarungen [14, 1.2.5b#5], [IDW PS 880, Tz23] mit dem Hersteller für die Wartung und den Havariefall sind über einen entsprechenden Vertrag sichergestellt.

Das Handbuch enthält die erforderlichen Angaben [2, 1.1.2.10], [3] zur Kontaktaufnahme bei erforderlicher Unterstützung bei der Anwendung.

Die geforderte Unterscheidung [8] funktionaler- und nicht-funktionaler Anforderungen wird über die Anforderungsdatenbank sichergestellt.

Dies gilt auch für angemessene [8] Vorgehen bei der Erfassung der Anforderungen.

---

[8] (IDW PS 880, Tz28) *Zur Beurteilung der Möglichkeiten einer künftigen Programmpflege sind die DV-technischen Werkzeuge und die organisatorischen Maßnahmen bei der Programmentwicklung zu untersuchen. Die Beurteilung der Programmentwicklungsumgebung ist insbesondere dann erforderlich, wenn Bestandteile der Verfahrensdokumentation in der Entwicklungsumgebung generiert bzw. gespeichert werden. Weiterhin muss über die Entwicklungsumgebung bzw. über die Bibliotheksverwaltungsprogramme die notwendige Versionsführung nachgewiesen und die Änderungsdokumentation erstellt werden können. Die Freigabeverfahren und Wartungsmethoden sind im Hinblick auf mögliche Prüfungen späterer Programmversionen von Bedeutung.*

Die Anwendung bildet grundsätzlich die Anforderungen der OPDV 1/2006 bei Anwendungen auf Trägersystemen ab. Während die IDV-Suite eine Freigabe der Anwendung mit einem Klick ermöglicht, ist die Freigabeerklärung nach OPDV 1/2006 mit institutsspezifisch zwei oder drei Unterschriften durchzuführen. **Dieses muss prozessual vom einzusetzenden Unternehmen berücksichtigt und abschließend bewertet werden, damit die Vorgehensweise trotzdem OPDV-konform ist**. Da in den einsetzenden Unternehmen häufig bereits (manuelle) Prozesse zur Freigabe von Programmen auf Basis von Trägersystemen implementiert sind und diese Unternehmen diese Prozesse weiterhin nutzen wollen, hat sich der Hersteller Stromwerken angabegemäß bewusst für diese „1-Click-Freigabe“ entschieden. Ergänzend hierzu gibt der Hersteller an, dass eine Schnittstelle zur Workflow-gesteuerten Software Bit-Informatik SoftwareLifecycle dann auch solche Unternehmen unterstützt, die mit SWLC den Freigabeprozess technisiert haben.

Die beim Hersteller verwendete Anforderungsdatenbank stellt auch sicher, dass:

- Anforderungen von der entwickelnden Einheit gereviewed werden [8],
- Anforderungen identifizierbar und nachverfolgbar sind [8],
- eine Erfassung der Benutzerschnittstellen stattfindet [8], die dann im Handbuch beschrieben werden und
- sowohl Design- und HW-Anforderungen [8] erfasst werden.

Der Entwicklungsprozess sieht die Erstellung von Prototypen [8] vor.

Die erforderlichen Handbücher [2, 1.1.5.3], [3], [ISO/IEC 9126] liegen vor, Fehlermeldungen werden online erläutert.

Die Datenherkunft [10] ist im Handbuch benannt.

Das Handbuch enthält auch Angaben zum Softwarehersteller [2, 1.1.2.3], [3].

Eine widerspruchsfreie Produktbeschreibung [2, 1.1.1.2] liegt als Benutzerhandbuch und Implementierungsleitfaden [509] vor.

Eine Information des einsetzenden Institutes über Programmupdates [14, 1.2.5b#16] erfolgt per E-Mail.

Informationen zur Wartung [2, 1.1.2.12], [3], [IDW PS 880, Tz23] werden im Vertrag und ergänzend im Benutzerhandbuch genannt.

Der Wartungsvertrag gibt an, was die Wartung im Einzelnen umfasst [2, 1.1.2.13], [3].

8.1.2.2 Architektur und Schnittstellendesign, Geschäftsprozessmodellierung (GPM)

8.1.2.2.1 Architektur und Betriebssicherheit

Der dokumentierte Entwicklungsprozess [8], [COBIT4.0, AI2.2] listet die Akteure und deren Aufgaben.

Er enthält die erforderlichen [8] Aussagen.

Die Anwendung wird für Banken, Sparkassen und Versicherungen angeboten [8].

Die Geschäftsprozessmodelle [8] sind im Benutzerhandbuch zugeordnet.

Hilfestellungen [8] erfolgen online..

Der Hersteller verwendet einen Implementierungsleitfaden [8].

Die Softwareauslieferung [8] erfolgt per Download und Key.

Die Schnittstelle [8] zur Bit Software *Lifecycle* ist zwischen den beiden Softwareherstellern beschrieben und nicht extern zugänglich.

Die Schnittstelle für die Excel ID Dateien ID wird in Excel in internen, versteckten Variablen abgelegt.

8.1.2.2.2 Schnittstellen und sicherer Datenaustausch

Bei Ausfall der Schnittstelle zur Bit Software *Lifecycle* können vorübergehend keine Daten in diese Datenbank geliefert werden. Nach Wiederherstellung der Schnittstelle können die Daten jedoch wieder übertragen werden. Eine Zeitkritikalität wird hierbei nicht gesehen.

8.1.2.2.3 Integration in den Geschäftsprozess

Die erforderliche Einbindung [26, L8, S17] in den unterstützten Programmfreigabeprozess des einsetzenden Institutes wird durch das übergebene Fachkonzept konform mit der OPDV 1-2006 dargestellt.

Das DV-Konzept stellt das Daten- und Informationsmodell und die ereignissteuernden Prozesse dar [26, L8, S17].

Die Einhaltung der informationstechnischen Relationen wird über den Implementierungsleitfaden sichergestellt [26, L8, S17].

8.1.2.3 Programm- bzw. Systemdokumentation

Die an die Programmdokumentation zu stellenden Anforderungen [2, 1.3.x] sind aufgrund der Verwendung von Programmierrichtlinien eingehalten.

Einen wesentlichen Anteil an der Vollständigkeit der Programmdokumentation [2, 1.3.x], [4] hat das Benutzerhandbuch.

Die erforderlichen Kontroll- und Abstimmverfahren [IDW PS 880, Tz13] sind über das Benutzerhandbuch sichergestellt.

Die Darstellung der Fehlerbehandlung (Fehlerprüfung mit Angabe der Fehlermeldungen und der daraus resultierenden Maßnahmen) [2, 1.3.2.6], [OLG Koblenz, Az.: 1 U 1614/05] wird in der Onlinehilfe angeboten.

Die Datensicherung und Wiederherstellung der Anwendung und der Daten [2, 1.3.2.7], [IDW PS 880, Tz23] liegt in der Verantwortung des einsetzenden Unternehmens. Grundsätzlich sollte die Datenbank über die Sicherungsmechanismen des genutzten Datenbanksystems und die Applikation über "normale" File-Sicherungsmechanismen periodisch gesichert werden.

Die erforderliche Trennung von Rollen und Verantwortlichkeiten [2, 1.3.2.15], [7], [8 -> Rollentrennung] wird über die Anwendung umgesetzt und **über das Benutzerhandbuch dokumentiert.**

Eine Herstellerfreigabe [2, 1.3.2.23], [4] liegt vor.

8.1.2.4 Durchführung und Dokumentation der Entwicklertests

Für die Durchführung der Entwicklertests gibt es bei stromwerken dokumentierte Vorgaben im Entwicklungskonzept, der Qualitätssicherung für die Entwicklung von Anwendungen sowie entsprechende Programmierrichtlinien. Wir konnten uns davon überzeugen, dass stromwerken nach diesen Vorgaben die Entwicklung und Tests der Anwendungen vorgenommen hat. Somit kann die Durchführung und Dokumentation der Entwicklertests als ordnungsgemäß bewertet werden.

8.1.3 Nachweis einer vollumfänglichen Qualitätssicherung

Siehe auch [SITB, K341(Test und Freigabe)].

8.1.3.1 Nachweischarakter von Testergebnissen

Die Tests werden durch die Entwickler intern selbst durchgeführt. Die Entwicklertests, sind formalisiert und werden in der Regel über Mitschnitte im Videoformat dokumentiert.

Die im Rahmen der Tests gefundenen Fehler werden in MANTIS als neue Fälle eingetragen und dort von den Entwicklern begutachtet und behoben.

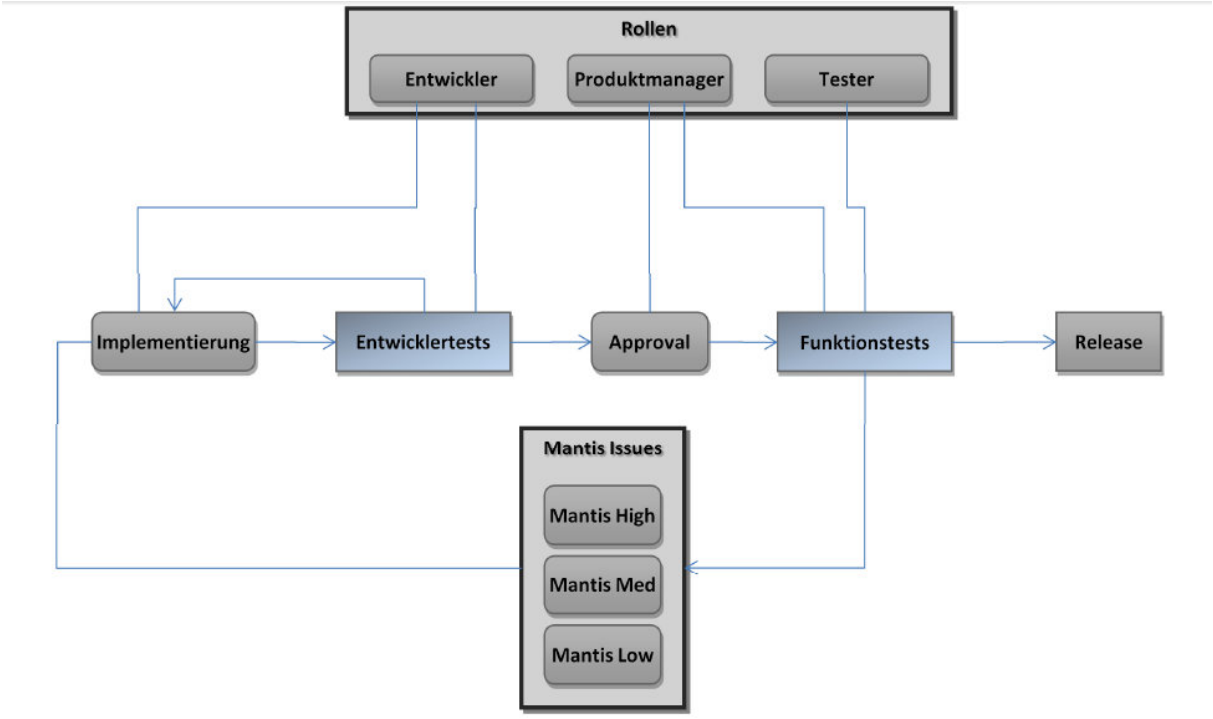
Der Abschluss der einzelnen Tests wird durch den Tester dokumentiert.

Nach erfolgreichem Abschluss der Testphase und nach Fertigstellung aller benötigen Dokumentationen zur Anwendung ist eine Programmversion abgenommen und freigegeben.

Der vollständige Ablauf wird im Abschnitt *8.1.3.2 Vollständige Qualitätssicherung* beschrieben.

8.1.3.2 Vollständige Qualitätssicherung

Die Qualitätssicherung erfolgt gemäß folgendem Konzept:



Hierbei hat der Produktmanager bei neuen oder geänderten Anwendungsfunktionen folgende Aufgaben:

- Inhalte/Aktionen: Erstellung der Einträge in Mantis und Zuweisung des erforderlichen Entwicklers.
- Ggf. Definition eines Testfalls im Testfalldokument.
- Überprüfung und Dokumentation, welche gesetzlichen Anforderungen für den Einsatzkontext
- der Anwendung besonders zu berücksichtigen sind
- Aus der Beschreibung der Anforderung sollten folgende Aspekte, insofern erforderlich, hervorgehen:
    - Fachlichen Hintergrund

- Aufbau einer Maske [z.B. Filterfunktionen, Ergebnisliste]
- Aktionen [z.B. Aktualisieren, Speichern]
- Workflow [Abfolge von Masken und Verarbeitungsschritten]
- Standardeinstellungen [beim Aufruf] / Konfigurierbarkeit

Bei der Umsetzung der Arbeitspakete hat der Entwickler die Aufgaben:

- Programmierung der im Arbeitspaket enthaltenen Funktionen inkl. Code-Dokumentation
- Ablage des Programmcodes im Repository inkl. Dokumentation der Änderungen
- Durchführung von Entwicklertests
- Dokumentation von Update-relevanten Änderungen (Änderungen in Datenbank,
- Struktur einer INI-Datei, Vorlagen, verwendete Komponenten) in Mantis
- Dokumentation von Update-relevanten in Releasebeschreibung in Mantis (eigener Absatz, was im Handbuch aufgenommen werden soll, sowohl im Change-Teil als auch im beschreibenden Teil)
- Der Entwickler ist selbst für die Qualität der von ihm entwickelten und getesteten Funktionen aus technischer und fachlicher Sicht verantwortlich.

Testfallkonzeptionen zum Test eines Funktionspakets bestehen aus mehreren Teilschritten durch den Produktmanager, Entwickler und Tester.
Inhalte/Aktionen:

- Entwicklung von Testfällen und Testdatenbestand für neue Funktionspakete
- Erweiterung/Anpassung der Standardtestfälle und des zugehörigen Testdatenbestands
- der Anwendung
- Beauftragung / Durchführung des Funktionstest
- Bewertung des Umsetzungsergebnisses / Testfallergebnisse aus fachlicher Sicht
- Abnahme der GUI/Usability eines Arbeitspakets, Dokumentation in Mantis
- Bemerkungen: Bei Änderungs-/Korrekturbedarf soll generell ein Nachtest erfolgen, um die Abnahme des APs zu bestätigen.

Integrationstests werden für den jeweiligen Release werden vom Tester durchgeführt. Hierbei übernimmt er folgende Aufgaben:

- Durchführung der für die Anwendung definierten Standardtestfällen [Integrationstest,
- ggfs. Lasttests]
- Dokumentation von Testergebnissen der Standardtestfälle
- Information des zuständigen Entwicklers über das Testergebnis per E-Mail (manuell
- oder z.B. per Mantis)
- Bei Major- werden alle Standardtestfälle durchlaufen, bei einem Minor- Releases oder Fixpack-Release können in Absprache mit dem Produktmanager die Tests auf einen Auszug der Standardtestfälle begrenzt werden.
- Bei Änderungs-/Korrekturbedarf soll generell ein Nachtest durch den Tester erfolgen. Der Umfang des Nachtests (alle Testfälle vs. nur Bugfix) wird vom Tester festgelegt.

Das eigentliche Release wird durch den Produktmanager nach folgenden Arbeiten freigegeben:

- Prüfung der Prozesssicherheit
  - Wurden alle vorherigen Schritte erfolgreich abgeschlossen?
  - Stichprobenartig inhaltliche Prüfung der Ergebnisse
  - Inhaltliche Prüfung und Abnahme der Releasedokumente (für Kunden)
- Einchecken des Releases als Komplett-Zip (Vollversion, Update, Source, Testdoku, Freigabedokument).

Aufgrund dieser etablierten Prozess halten wir die vollständige Qualitätssicherung für gegeben.

8.1.3.3 Lasttest

Grundsätzlich muss das zum Frontende korrespondierende Datenbanksystem die Kommunikation ermöglichen. Es könnten Verzögerungen auftreten, wenn viele User gleichzeitig speichern und hierbei größere Datenmengen verarbeitet werden. Dies ist aber relativ unwahrscheinlich. Der Tracker ist so programmiert, dass er, sollte mal keine Verbindung möglich sein einfach nicht aktiv wird bzw. z. B. bei der Doku den User darauf hinweist. Prinzipiell ist die Useranzahl nicht beschränkt.

Die Applikation wurde zusammen mit zwei Kunden über einen längeren Zeitraum entwickelt. Hierbei konnten bei den Pilottests Erfahrungen bzgl. der Last der Anwendungen gesammelt werden. Eines der Unternehmen (800 User) nutzt das System ohne Lastprobleme seit 2 Jahren. Eine Grenze konnte hierbei bisher nicht festgestellt werden, Zeitmessmechanismen sind im Logging integriert, sodass man die Performance jederzeit überprüfen kann. Entsprechende Maschinen wurden hierbei eingesetzt.

Abhängig ist die Last auch von der implementierten Datenbankumgebung. Die Tracker werden nur beim Speichern und beim Öffnen bzw. beim Klick eines Users auf die Dokumentation aktiv. Dadurch ergibt sich eine sehr geringe Last, da selten sehr viele User gleichzeitig speichern.

8.1.3.4 Qualitätsmanagement

Ein standardisiertes und eingeführtes QMS [8], nach dem das Projekt durchgeführt wird, existiert gemäß Vorgaben zur Entwicklung und Qualitätssicherung.

Der Produktverantwortliche übernimmt die Rolle zur Verantwortlichkeit für QS-Maßnahmen [8].

Erforderliche [9, 4.2] Qualitätssicherungsbelege werden gemäß Testkonzept und –dokumentation erstellt.

Das Ressourcenmanagement [8] findet bei Erforderlichkeit statt und stellt Arbeitsumgebung und Arbeitsmittel ausreichend zur Verfügung.

Eine Trennung von Entwicklungs- und Testsystemen [13], [IDW RS FAIT1 Ziffer 4.3] als Voraussetzung für ein angemessenes Freigabeverfahren(siehe auch [GS-KAT, M2.5]) liegt vor.

Die Anwendung IDV-Suite erfüllt grundsätzlich die Anforderungen der OPDV 1/2006 entsprechend der implementierten Funktionalität des Programms; GoB-relevante Vorgänge werden in der IDV-Suite nicht erzeugt oder verarbeitet. **Für die Einhaltung der GoB in den Trägeranwendungen des Unternehmens ist das Unternehmen selbst verantwortlich**.

Testkategorien in den Bereichen Daten-Volumen, HW-Konfigurationen und Speicher [8], [IDW PS 880, Tz6] wurden im Rahmen von Pilottestbetrieben überprüft.

Ein Vorgehen [8] für die Auslieferung der abgenommenen Software besteht.

Das Downloadpaket enthält Software, Installationsprozedur, Benutzerhandbuch etc. und ist als Auslieferungseinheit vollständig [8].

8.1.4 Bereitstellung und Identifikation des Liefergegenstandes sowie seiner Quellen

8.1.4.1 Versionsverwaltung und Identifikation

Stromwerken unterscheidet bei der Versionierung des Produktes in folgende Kategorien:

Major-Releases sind Releases mit .0-Versionsnummer, z. B. 2.0 oder 3.0. In Major-Releases muss das komplette "Standard-Testprogramm" sowie das Testprogramm für neue Funktionen durchgeführt werden.

Minor-Releases sind Releases mit .X >0 Versionsnummer, z. B. 2.1 oder 2.2. Minor-Releases bedingen mindestens den Test der neuen Funktionen und ggf. (Teil-)Tests des "Standard-Testprogramms".

Fixpacks sind Releases mit FP-Kennzeichnung, z.B. 2.1 FP1. Fixpacks bedingen mindestens den Test der neuen Funktionen und, falls erforderlich, (Teil-)Tests des "Standard-Testprogramms".

Der Produktmanager übernimmt hierbei folgenden Aktivitäten:

- Erstellung der Dokumentation für den Kunden
- Aktualisierung der Anwendungsdokumentation: Beschreibung von neuen und geänderten
- Funktionen, Erstellung von Releasenotes
- Anpassung von Installations- und Updateanleitung (nach Bedarf)
- Erstellung von Programmpaketen [Setup und Update]

Die Releaseverteilung wird vom Produktmanager veranlasst und beinhaltet folgende Vorgehensweise:

- Bereitstellung des Releases auf dem Stromwerken-Server, bei Bedarf auch als Vor-Release für Pilot-Kunden
- Information wenn erforderlich per E-Mail an SIZ
- Information per E-Mail an (ausgewählte) Kunden
- Anpassung der Release-Notes, die bei Klick auf "Update" angezeigt werden, auf dem Stromwerken-Server.

8.1.4.2 Lieferumfang

Die erforderliche Entsprechung von Dokumentation und Programm [GoBS, Tz1.2] [HGB, §§238, 239 und 257] und [AO §§145 und 146] ist gegeben.

Die Produktbeschreibung trägt eine eindeutige Dokumentbezeichnung und Versionsangabe [2, 1.1.2.1], [3].

8.2 Detailbewertung aus Sicht der Benutzer bzw. Fachbereiche

8.2.1 Sicherstellung der Vollständigkeit von fachlichen Anforderungen

Die Produktbeschreibung benennt die Arbeitsaufgabe[2, 1.1.2.4], [3].

Sie klärt über die erforderlichen Informationen [2, 1.1.x], [3] auf.

Einzuhaltende Bedingungen und durchführbare Anpassungen [2, 1.1.5.4], [3] werden in der Produktbeschreibung genannt.

Die Software stellt ein Mittel zur Verhinderung unerlaubter (versehentlicher oder absichtlicher) Änderungen [2, 1.1.3.3], [3] an den in Excel und Access hinterlegten Programmierungen zur Verfügung.

8.2.2 Korrekte Bedienung durch den Anwender

Es ist eine Onlinehilfe implementiert.

Das Benutzerhandbuch enthält die vollständige [2, 1.2.1], [3] Anwenderdokumentation.

8.2.3 Internes Kontrollsystem (IKS) der Sparkasse

Es erfolgt zwar an der Excel- oder Access Datei eine Implementierung einer ID, diese verändert jedoch keine Daten innerhalb der Datei [2, 3.2.6].

Die Integritätssicherung [2, 3.2.11], [8], [IDW PS 880, Tz17] der bearbeiteten Objekte (Excel- und Accessdateien) erfolgt bei entsprechender Parametereinstellung in der Datenbank einschließlich Versionierung.

8.3 Detailbewertung aus Sicht des Betreibers

8.3.1 Technische Bereitstellung der Software durch den Lieferanten

Die Versionsbereitstellung wird vom Produktmanager veranlasst und beinhaltet folgende Vorgehensweise:

- Bereitstellung der Version auf dem Stromwerken-Server
- Information wenn erforderlich per E-Mail an SIZ
- Information per E-Mail an Kunden
- Zusendung des Schlüssels für die Nutzung der Anwendung per E-Mail an den Kunden durch Stromwerken

8.3.2 Installation und Betriebsaufnahme

Die zu verwenden Programme und DLL`s sowie die Datenbereiche werden ausführlich dargestellt, so dass im einsetzenden Institut die Kontrolle auf zum unveränderten Einsatz (§239 Abs. 3 HGB) der Komponenten durchgeführt werden kann.

Es besteht eine Checkliste zur Überprüfung der ordnungsgemäßen [10] Installation.

8.3.3 Betriebsbereitschaft in einer Sparkasse oder deren VRZ

8.3.3.1 Fremdkomponenten

8.3.3.1.1 Betriebssystem, Laufzeitumgebungen und andere Fremdkomponenten

Das Produkt arbeitet mit folgenden Datenbanksystemen zusammen:

- SQL-Server (SQL-Server 2005 und 2008 getestet),
- SQL-Anywhere bzw. iAnywhere (SQL-Anywhere 11 getestet) und
- MySQL (Version 5.0.27-log / Protokoll 10 getestet).

8.3.4 Sicherstellung eines sicheren IT-Betriebes

8.3.4.1 IT-Dokumentation (K015)

Die IT-Anwendung muss seitens des einsetzenden Unternehmens in die Sicherheitsstruktur eingebunden werden können. Für Sparkassen lässt sich dies über das Rechenzentrum der FI realisieren.

Unternehmen, die die Anwendung nicht im FI-Umfeld betreiben müssen die Einbindung in die Sicherheitsstruktur individuell bewerten.

Über den Implementierungsleitfaden werden ausreichend Angaben zu ggf. notwendigen Maßnahmen (z.B. Makrosicherheit) gegeben, um die Anwendung sicher betreiben zu können.

8.3.4.2 Trennung der Umgebungen (K018)

Bei Stromwerken bestehen getrennte Entwicklungs- und Testumgebungen für **Protokollierung (K110)**

Alle Parameterveränderungen werden historisiert in entsprechenden Historientabellen abgelegt. Die Auswertung erfolgt (derzeit noch) über die Datenbankkonsole. Für die nächste Version 4.0 sind hierfür eigene Reports innerhalb der Suite angedacht.

Die Protokollierungsdaten sind vom einsetzenden Unternehmen hinsichtlich der Konformität auf das eigene Protokollierungskonzept zu überprüfen.

8.3.4.4 Auswertung der Protokolle (K111)

Bei der Auswertung der Protokollierungsdaten sind insbesondere datenschutzrechtliche Bestimmungen im Rahmen der Vorabkontrolle sowie ggf. Mitbestimmungsrechte durch das einsetzenden Unternehmen zu berücksichtigen.

8.3.4.5 Berechtigungskonzept (K115)

Das Berechtigungssystem für die IDV-Suite kann über den Menüpunkt Programmparameter / Applikationsparameter aktiviert werden. Grundsätzlich ist das Berechtigungssystem nicht für die Suite aktiviert. Es kann ein Masterpasswort vergeben werden, um die Aussperrung aus der Anwendung zu verhindern.

Die Berechtigungen können rollenbasiert vergeben werden. Hierbei ist es möglich, die Rollen nach OE / Profil / User aufzugliedern. Hierüber kann auch das Reporting datenschutzkonform so gesteuert werden, dass jeder nur seine eigenen Dateien betrachten kann.

9 Detailbewertung bei ganz oder teilweise ausgelagertem Betrieb

9.1 Gesetzliche und normative Vorgaben

9.1.1 §11 BDSG, §§241,311 BGB - Datenschutz

Lieferant für Sparkassen ist die SIZ GmbH. Im Rahmen der Prüfung wurden folgende Ergebnisse im Verhältnis Supportleistungen und BDSG ermittelt:

- Dem Prüfer sind keine Supportfälle bekannt, in denen der Gesamtinhalt der Anwendungsdatenbank zu betrachten war.
- In Supportfällen sind „Eigenentwicklungen eines Institutes auf Excel-Basis“ in der Vergangenheit zu betrachten gewesen. Diese Excel-Dateien können potenziell personenbezogene Daten beinhalten. Um die Reaktion einer Komponente der IT-Anwendung auf diese spezielle Excel-Datei mit dem Support abzusprechen, ist es i.d.R. erforderlich, dem Supportleister diese Excel-Datei zur Verfügung zu stellen. Um die damit verbundene Weitergabe personenbezogener Daten zu unterbinden, enthält die IT-Anwendung eine Komponente „*DateiAnonymisierer.xls*“ [509, 2.4. Was die IDV-Suite nicht kann…], die es erlaubt, die weiterzugebende Excel-Datei zu anonymisieren.

- Ein Anonymisierungstool für Access-Dateien steht noch nicht zur Verfügung. Dem Institut sollten aber die Tabellenspalten mit personenbezogenen Daten bekannt sein, um dort selbst eine Anonymisierung durchführen zu können.
- Inwieweit damit Supporthandlungen noch der Auftragsdatenverarbeitung nach BDSG unterliegen, muss der Datenschutzbeauftragte des Institutes entscheiden. Sollte er eine Relevanz sehen, hier weitere Prüfungsergebnisse:
  - Das Standard-Supportvertragsmuster [520] enthält keine technischen und organisatorischen Maßnahmen und erfüllt damit nicht für sich das BDSG. Um diesem Mangel abzuhelfen, stellt der Lieferant eine „*Anlage: Technische und organisatorische Maßnahmen nach § 9 BDSG*“ [521] auf Nachfrage zur Verfügung.
  - Der Lieferant versichert, regelmäßige SITB-Audits durchzuführen, in denen auch Datenschutzthemen angesprochen werden. Deren Ergebnisse werden nicht extern zur Verfügung gestellt.
  - Der Lieferant hat auch einen Datenschutzbeauftragten ernannt.

Unabhängig von der Feststellung, ob eine rechtlich relevante Auslagerung vorliegt oder nicht, stellt die Tatsache, dass der Betrieb der Anwendung nicht durch das Institut selbst sondern durch ein Rechenzentrum betrieben wird, eine nach BDSG relevante Auftragsdatenverarbeitung dar.

Final zu bewerten ist nicht ein potenziell existierender Mustervertrag, sondern der tatsächlich zwischen einsetzendem Institut und Betreiber vereinbarte Vertrag, insofern haben die folgenden Aussagen nur vorläufigen Charakter. **Das einsetzende Institut muss prüfen, ob alle Belange ausreichend erfüllt sind**.

gesetzliche Vorgabe an den Vertragsinhalt nach BDSG §11 Abs. 2 (BDSG-Novelle II: In Kraft getreten am 1. September 2009 zum Thema Auftragsdatenverarbeitung)	**Hinweis auf Behandlung im Mustervertrag**
Gegenstand und Dauer des Auftrages	
Umfang, Art und Zweck der vorgesehenen Erhebung, Verarbeitung oder Nutzung von Daten, deren Art und der konkrete Kreis der davon Betroffenen	
die nach §9 BDSG zu treffenden technischen und organisatorischen Schutzmaßnahmen (Mussvorgabe!)	
Grundvorgaben zur Berichtigung, Löschung und Sperrung von Daten	
nach §11 Abs. 4 BDSG bestehende Pflichten des Auftragnehmers, insbesondere diejenigen von ihm vorzunehmenden Kontrollen	
eventuelle Erlaubnis gegenüber dem Auftragnehmer zur Einschaltung von Subunternehmern	
Kontrollrechte des Auftraggebers und die sich daraus ergebenden Duldungspflichten des Auftragnehmers (Mussvorgabe für Auftraggeber zur Durchführung solcher Kontrollen)	
mitteilungspflichtige Verstöße des Auftragnehmers oder bei ihm beschäftigter Personen gegen Vorschriften zum Schutz personenbezogener Daten oder gegen im Auftrag getroffene Vereinbarungen	
Rahmen und Umfang von Weisungsbefugnissen, die zugunsten	

gesetzliche Vorgabe an den Vertragsinhalt nach BDSG §11 Abs. 2 (BDSG-Novelle II: In Kraft getreten am 1. September 2009 zum Thema Auftragsdatenverarbeitung)	**Hinweis auf Behandlung im Mustervertrag**
des Auftraggebers gegenüber dem Auftragnehmer bestehen	
Rückgaberegelungen bezüglich überlassener Datenträger und Vorgaben zur Löschung von beim Auftragnehmer gespeicherten Daten nach Auftragsbeendigung	

10 ANLAGEN

10.1 GLOSSAR

BEGRIFF ↖	DEFINITION
Abnahmetest	Der Abnahmetest dient dem Ziel, zu zeigen, dass das Vertrauen in das System für den produktiven Einsatz gerechtfertigt ist
Angemessen	Entsprechend [IDW EPS 300, Tz8] stellt in der hier vorliegenden Dokumentation dieser Begriff *die „Angemessenheit" der Prüfungsnachweise einen qualitativen Maßstab für die eingeholten Prüfungsnachweise, deren Verlässlichkeit und Relevanz für die Prüfung einer Aussage in der Rechnungslegung dar*. Siehe auch „ausreichend".
anonymisieren	[BDSG, §3(6)]: *Anonymisieren ist das Verändern personenbezogener Daten derart, dass die Einzelangaben über persönliche oder sachliche Verhältnisse nicht mehr oder nur mit einem unverhältnismäßig großen Aufwand an Zeit, Kosten und Arbeitskraft einer bestimmten oder bestimmbaren natürlichen Person zugeordnet werden können*.
Ausreichend	Entsprechend [IDW EPS 300, Tz8] stellt in der hier vorliegenden Dokumentation dieser Begriff keine Schulnote dar sondern beschreibt lediglich einen quantitativen Maßstab, siehe auch „angemessen".
Qualität	DIN ISO 8402 (Entwurf März 1992): "*Die Gesamtheit von Merkmalen einer Einheit (entity in der engl. Fassung) bezüglich ihrer Eignung, festgelegte und vorausgesetzte Erfordernisse zu erfüllen*." DIN 55350 (Teil 11) : "*Qualität ist die Gesamtheit von Eigenschaften und Merkmalen eines Produkts oder einer Tätigkeit, die sich auf deren Eignung zur Erfüllung gegebener Erfordernisse bezieht.*" Qualität ist kein absoluter Wert, sondern muss immer relativ zu gegebenen Erfordernissen gesehen werden. Qualitätsbewertungen beinhalten also immer einen Vergleich zwischen Qualitätsvorgaben, die aus den gegebenen Erfordernissen abgeleitet werden (Soll-Werte) und den tatsächlich erreichten Ausprägungen der Merkmale (Ist-Werte). Qualität ist ein Maß für die Erfüllung von Anforderungen.
Qualitätslenkung	Arbeitstechniken und Tätigkeiten, die zur Erfüllung der Qualitätsforderungen angewendet werden. Der Zweck dieser Arbeitstechniken und Tätigkeiten ist sowohl die Überwachung

BEGRIFF ↖	DEFINITION
	eines Prozesses als auch die Beseitigung von Ursachen nicht zufrieden stellender Leistung. Mit Qualitätslenkung sind also vor allem die konstruktiven Maßnahmen wie z. B. Einsatz von Entwicklungsmethoden, Werkzeugen oder auch die Verwendung von Programmierrichtlinien gemeint.
Qualitätsmanagement	Tätigkeiten aller Führungsebenen, welche die Qualitätspolitik, Ziele und Verantwortung festlegen sowie diese durch Mittel wie Qualitätsplanung, Qualitätslenkung, Qualitätssicherung und Qualitätsverbesserung im Rahmen des Qualitätsmanagementsystems verwirklichen. Dies gilt sowohl projektspezifisch als auch projektneutral.
Qualitätsmanagementplan	Synonym zu Qualitätsplan
Qualitätsplan	Dies ist das Dokument, in dem für ein einzelnes Projekt die spezifischen Qualitätsbezogenen Arbeitsweisen, Hilfsmittel und Tätigkeiten dargelegt sind. Er bezieht sich auf die anwendbaren Teile des Qualitätsmanagement- und Verfahrenshandbuchs.
Qualitätsplanung	Die Qualitätsplanung umfasst: Identifizieren, Klassifizieren und Gewichten der Qualitätsmerkmale von geplanten Projektergebnissen sowie Festlegen der Ziele, der Qualitätsforderungen und der einschränkenden Bedingungen. Vorbereitung der Anwendung des Qualitätsmanagementsystems samt Ablauf- und Zeitplänen. Vorbereitung von Qualitätsmanagementplänen und das Treffen von Vorkehrungen für Qualitätsverbesserungen.
Qualitätssicherung	Alle geplanten und systematischen Tätigkeiten, die innerhalb des Qualitätsmanagementsystems verwirklicht sind und die wie erforderlich dargelegt werden, um angemessenes Vertrauen zu schaffen, dass ein Projekt/Team/Bereich/... die Qualitätsforderung erfüllen wird. Im Bereich der Softwareentwicklung sind dies in erster Linie analytische Maßnahmen wie Reviews oder Tests.
Regressionstest	Der Regressionstest besteht aus der Wiederholung von bereits durchgeführten Testfällen und dient zum Nachweis, dass die bereits vorher enthaltene Funktionalität der Betrachtungseinheit nach wie vor korrekt erbracht wird. Unter einem Regressionstest (v. lat. Regression = Rückschritt) versteht man in der Softwaretechnik die Wiederholung aller oder einer Teilmenge aller Testfälle, um Nebenwirkungen von Modifikationen in bereits getesteten Teilen der Software aufzuspüren. Solche Modifikationen entstehen regelmäßig z. B. aufgrund der Pflege, Änderung und Korrektur von Software. Der Regressionstest gehört zu den dynamischen Testtechniken. Aufgrund des Wiederholungscharakters und der Häufigkeit dieser Wiederholungen eignen sich Regressionstests gut für

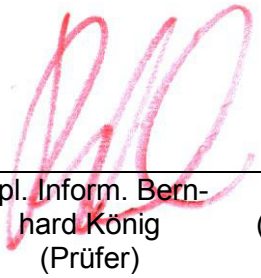
BEGRIFF ↖	DEFINITION
	eine automatisierte Ausführung. In der Praxis steht der Begriff des Regressionstests für die reine Wiederholung von Testfällen. Die Testfälle selbst müssen anhand anderer Techniken spezifiziert und mit einem Soll-Ergebnis versehen sein, welches mit dem Ist-Ergebnis eines Testfalls verglichen wird. Ein direkter Bezug auf die Ergebnisse eines vorherigen Testdurchlaufs findet nicht statt. Im Gegensatz dazu ordnet Liggesmeyer (Lit.: Liggesmeyer) den Regressionstest in die Gruppe der Diversifizierenden Tests ein. Dadurch wird im Unterschied zu Funktionsorientierten Testtechniken die Korrektheit der Testergebnisse nicht anhand der Spezifikation entschieden, sondern durch Vergleich der Ausgaben der aktuellen Version mit den Ausgaben des Vorgängers. Ein Testfall gilt beim Regressionstest als erfolgreich absolviert, wenn die Ausgaben identisch sind.
Review	Ein Review ist eine Form der Qualitätssicherung durch Begutachtung. Ein Team von Experten begutachtet in einem Zeitraum von meist wenigen Stunden ein Dokument bzw. Arbeitsergebnis, typischerweise eine Spezifikation. Die hauptsächlichen Ziele sind, die Qualität eines Arbeitsergebnisses zu gewährleisten und den Projektfortschritt transparent zu machen. Reviews sind mehr oder weniger formal geplante und strukturierte Analyse- und Bewertungsprozesse und konzentrieren sich auf Angaben, die die Weiterentwicklung in mehr oder minder starkem Umfang gefährden: Unvollständige oder fehlende Angaben Widersprüchliche Angaben Falsche Angaben Missverständliche oder interpretierbare Angaben.
Schadpotenzial	Schadpotenziale sind konkrete Gefährdungen, die aus der Funktion oder der technischen Realisierung eines Systems für seine Umgebung oder seine Komponenten erwachsen können. Dabei sind alle Einwirkungsmöglichkeiten des Systems auf seine Umgebung oder auf seinen internen Zustand zu beachten. Beispiele: Das Datennetzüberwachungswerkzeug erlaubt dem Benutzer die Analyse und Beeinflussung von Verkehrflüssen. Der Paketmonitor erlaubt dem Benutzer das Auslesen von Paketinhalten. Das Partitionierungswerkzeug für Festplatten erlaubt die Zerstörung der dort gespeicherten Daten. Der Editor erlaubt die Modifikation von Dateien. Schadpotenziale beantworten Fragen wie "Welche Systemfunktion ermöglicht wem welche Einwirkungen?" oder salopp formuliert "Welche konkreten Gefahren könnten von diesem

BEGRIFF ↖	DEFINITION
	System ausgehen?"
Schutzbedarf	Eine spezifische Voraussetzung der IT-Sicherheit eines bestimmten Systems, also eine notwendige Bedingung zur Sicherung der Integrität und Verfügbarkeit des Systems sowie der Informationsvertraulichkeit innerhalb des Systems. Schutzbedürfnisse sind sehr konkret formulierte Erfordernisse der IT-Sicherheit eines Systems. Sie identifizieren seine Verwundbarkeiten, indem sie das schutzbedürftige Objekt (Subsystem), seinen konkreten Schutzbedarf und (vorzugsweise) die Konsequenzen mangelnden Schutzes nennen. Sie antworten auf die Fragestellung "Welches konkrete Objekt braucht welchen Schutz zur Vermeidung welcher Gefahr?" oder, salopper formuliert, "Was muss im einzelnen verhindert werden?"
Schwachstelle	Eine Sicherheitsschwäche in einer Anwendung (z. B. durch Fehler in der Analyse, Entwurf, Implementierung oder Betrieb)
SEU	mehrdeutig: **S**mallest **E**xecutable **U**nit (Die kleinste selbstständig ausführbare Programmeinheit.) **S**oftware-**E**ntwicklungs-**U**mgebung
Sicherheit	Die Kombination aus Vertrauenswürdigkeit, Integrität und Verfügbarkeit.
Sicherheitsanforderung	Sicherheitsanforderungen sind eine Abstraktionsstufe von Schutzbedürfnissen. Sicherheitsanforderungen dürfen nie hinter den Schutzbedürfnissen, aus denen sie abgeleitet sind, zurückbleiben. Ein System kann an seine Umgebung ohne weiteres Sicherheitsanforderungen stellen, die seine konkret identifizierten Schutzbedürfnisse zusammenfassen und auch übersteigen. Dies dient der Definition und Homogenisierung von Sicherheitsstandards und Sicherheitsniveau ebenso wie der Vorhaltung einer Sicherheitsreserve, der Zukunftssicherheit von Sicherheitskonzepten und schließlich der Verträglichkeit von Systemen untereinander im Falle der Integration in einem Supersystem. Sicherheitsanforderungen sind also ein Instrument, strategische Marschrichtungen für Sicherheitsmaßnahmen vorzugeben. Sicherheitsanforderungen geben Antwort auf die Fragestellung "Welche Schutzprinzipien werden in welcher Stärke für welche Objektklassen gefordert?" (Es ist zu beachten, dass nicht mehr gefragt wird, was erforderlich ist, sondern was unter Berücksichtigung der Erfordernisse gefordert wird!)
Sicherheitslücke	Eine Diskrepanz zwischen den Sicherheitsanforderungen eines Systems und den Sicherheitsrisiken, denen es ausgesetzt ist. Damit können bestimmte Schadpotenziale des Systems und die damit korrespondierenden Sicherheitsrisiken seines Anwendungszweckes eintreten. Die reguläre Sicherheitsaktivität zur präventiven Entdeckung von Sicherheitslücken ist der Sicherheitsprofilabgleich. Sicherheitslücken kön-

BEGRIFF ↖	DEFINITION
	nen aber auch a posteriori im Rahmen der Sicherheitsaktivität "Panik", identifiziert werden.
Sicherheitsmechanismus	Die Logik oder der Algorithmus, die eine bestimmte sicherheitsspezifische oder sicherheitsrelevante Funktion in Hard- oder Software implementiert. Beispiele hierfür sind der DES-Algorithmus für eine Verschlüsselung bzw. das Kerberos-Protokoll für die Realisierung eines Single-Login Verfahrens.
SITB	[SITB] Der „Sichere IT-Betrieb der SIZ GmbH“ beschreibt Sicherheit entsprechend aller für Finanzinstitute in Deutschland geltenden Regeln und bietet auch eine Zertifizierung nach SITB an. Viele Sparkassen haben ihr Sicherheitsmanagement entsprechend SITB zertifizieren lassen.
Zugangskontrolle	Die Datenverarbeitungsanlagen dürfen nur von Befugten benutzt werden. Unter Zugangskontrolle ist die gesamte Anmeldeprozedur samt Passwortverfahren etc. zu verstehen.
Zugriffsschutz	Benutzer dürfen nur die Daten nutzen und verarbeiten, für die sie autorisiert sind. Die Grundlage hierfür bildet das Berechtigungskonzept.

11 INDEX

12 Unterschrift



Bonn, Mittwoch, 3. Februar 2016	Dipl. Inform. Bernhard König (Prüfer)	Dr. Thomas Stock (Qualitätssicherung des vorliegenden Prüfberichtes, siehe Änderungshistorie)