Einführung in die IT-Prüfung

Marie-Luise Nee
Robert Schmittwilken

LWL
Für die Menschen.
Für Westfalen-Lippe.

Herausgeber
Landschaftsverband Westfalen-Lippe
LWL-Rechnungsprüfungsamt
Piusallee 7
48147 Münster
Telefon: 0251 591-5361
Telefax: 0251 591-227
E-Mail: rechnungspruefungsamt@lwl.org
Internet LWL: www.lwl.org
Internet LWL-Rechnungsprüfungsamt: www.lwl-rpa.de

Bearbeitung
Marie-Luise Nee, IT-Prüferin im LWL-Rechnungsprüfungsamt
Robert Schmittwilken, IT-Prüfer im LWL-Rechnungsprüfungsamt

Bearbeitungsstand
01.04.2019

Urheberrecht
Das Werk einschließlich aller seiner Teile ist urheberrechtlich geschützt. Jede Verwertung, die nicht ausdrücklich vom Urheberrechtsgesetz zugelassen ist, bedarf der vorherigen Zustimmung der Leitung des LWL-Rechnungsprüfungsamtes. Dies gilt insbesondere für Vervielfältigungen, Bearbeitungen, Übersetzungen, Mikroverfilmungen und die Einspeicherung und Verarbeitung in elektronischen Systemen.

Inhaltsverzeichnis Seite

1. Einleitung....1
2. Grundlagen der IT-Prüfung....1
2.1. Prüfungsauftrag....2
2.1.1. Gesetzliche Pflichtprüfungen....2
2.1.2. Übertragene Aufgaben....3
2.1.3. Einzelprüfungsaufträge....3
2.1.4. Abgeleitete Prüfungsaufträge....3
2.2. Prüfungsgegenstände....4
2.3. Prüfungsmaßstäbe....7
2.3.1. Rechtmäßigkeit....8
2.3.2. Zweckmäßigkeit....9
2.3.3. Wirtschaftlichkeit....9
2.4. Informationssicherheit....10
2.5. Prüfhilfen / Werkzeuge....11
2.5.1. IT-Standards....11
2.5.1.1. ISO-Standards....12
2.5.1.2. BSI-Grundschutz....13
2.5.2. Prüfstandards....17
2.5.2.1. IDW-Prüfungsstandards....17
2.5.2.2. ISACA-Standards....20
2.5.3. Prüf-Tools....22
2.5.3.1. Datenanalyse-Software....22
2.5.3.2. Geschäftsprozessmanagement-Werkzeuge....24
2.5.4. SAP-Prüfhilfen....28

2.5.4.1. DSAG-Prüfleitfaden SAP® ERP 6.0 28
2.5.4.2. GRC Software 30
3. Qualifikation der IT-Prüfer*innen 32
4. Rahmenbedingungen 34
4.1. IT-Risiken 34
4.2. Internes Kontrollsystem (IKS) 36
4.3. Aufbauprüfung vs. Funktionsprüfung 39
4.4. Prüfuniversum und risikoorientierte Prüfplanung 40
4.5. Aufbau einer Wissensbasis 44
4.5.1. Überblick über die internen Regelungen der Verwaltung 44
4.5.2. Wissensbasis zu den wichtigsten Verfahren 45
4.5.3. Aufbau und Ausbau von IT- und IT-Prüf-Wissen 45
5. Prüfungsdurchführung - Beispiele 47
5.1. Prüfung von rechnungslegungsrelevanten Verfahren vor der Anwendung 47
5.1.1. Prüfungsauftrag 47
5.1.2. Prüfungsgrundlagen 48
5.1.3. Durchführung einer einführungsbegleitenden Prüfung 52
5.2. Prüfung von rechnungslegungsrelevanten Verfahren in Betrieb 56
5.2.1. Prüfung von wesentlichen Änderungen 56
5.2.2. Prüfung bestehender Verfahren 57
5.3. Prüfung der Basis-Infrastruktur und allgemeiner Prozesse 57

Literaturverzeichnis/Literaturhinweise

Audicon	Prüfen mit IDEA, 37
BOC	Das Geschäftsprozessmanagement-Werkzeug ADONIS – Stärken und Einsatzszenarien, 2
BSI	IT-Grundschutz-Kompendium, 2. Edition 2019, 1
BSI	BSI-Standard 200-1 – Managementsysteme für Informationssicherheit (ISMS), 9
BSI	BSI-Standard 200-2 – IT-Grundschutz-Methodik, 17
Bungartz, Oliver	Handbuch Interne Kontrollsysteme, Steuerung und Überwachung von Unternehmen, Berlin, 2012
DIIR (Hrsg.)	Revision von IT-Verfahren in öffentlichen Institutionen, Praxisleitfaden für den Prüfungsprozess, DIIR-Schriftenreihe Band 53, Berlin 2015
DSAG	Prüfleitfaden SAP® ERP 6.0 – Best-Practice-Empfehlungen des Arbeitskreises Revision u. Risikomanagement, 6
IBS Schreiber	CASAP®-Zertifizierung – Exam-Candidates-Guide, 5
ISACA	ISACA-Leitfaden – Grundlagen der IT-Revision für den Einstieg in die Praxis, 19, 2016
ISACA	ISACA-Leitfaden und Nachschlagewerk IDW PS 330 <-> DIN ISO/IEC 27001 Referenztabelle, Frankfurt/Main, 2011
ISACA	ITAFTM – Rahmenwerk der Berufspraktiken für die IT-Prüfung, 3. Auflage
Secorvo	Zentrale Bausteine der Informationssicherheit, Das Begleitbuch zum T.I.S.P., Karlsruhe, 2014
Schulz	Einführung in die Prüfung der Wirtschaftlichkeit des Verwaltungshandelns
Schmidt/Brand	IT-Revision in der Praxis, Carl Hauser Verlag 2011, 19
Streffing	Einführung in die örtliche Rechnungsprüfung, 64

TeleTrust (Bundesverband IT-Sicherheit e. V.)	Handreichung zum „Stand der Technik" im Sinne des IT-Sicherheitsgesetzes (ITSiG), in der jeweils aktuellen Fassung, veröffentlich im Internet

Quellenverzeichnis

URL.: https://audicon.net/fileadmin/audicon/media/dokumente/prospekte/Pruefen-mit-IDEA-Audicon-GmbH.pdf

URL.: https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzAbout/itgrundschutzAbout_node.html

URL.: https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKompendium/elementare_gefaehrdungen/elementare_Gefaehrungen_Uebersicht_node.html

URL.: https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKompendium/bausteine/SYS/SYS_1_1_Allgemeiner_Server.html

URL.: https://ch.boc-group.com/uploads/files/ADONIS_Whitepaper_DE_07.pdf

URL.: https://open.hpi.de/courses

URL.: https://www.checkaud.de/checkaud-for-sap-systems/funktionalitaet/

URL.: https://www.dhpg.de/de/blog/detail/neuer-standard-fuer-it-pruefungen-erleichtert-zertifizierungen/

URL.: https://www.dsag.de/fileadmin/media/Leitfaeden/090511_Leitfaden_SAP_ERP6_screen.pdf

URL.: https://www.idw.de/idw/idw-aktuell/idw-ps-860-fuer-die-it-pruefung-ausserhalb-der-abschlusspruefung/109206

URL.: https://www.ibs-schreiber.de/sap-sicherheit/casap/

URL.: https://www.isaca.de/sites/pf7360fd2c1.dev.team-wd.de/files/attachements/isaca_leitfaden_ii_2016_gesamt_screen.pdf

URL.: https://m.isaca.org/Knowledge-Center/Research/Documents/ITAF-3rd-Edition_fmk_Ger_0916.pdf

URL.: https://www.mhkbg.nrw/kommunales/Kommunale-Finanzen/Kommunale-Haushalte/Haushaltsrecht-_-NKF/index.php

Abbildungsverzeichnis

Abb.1: Prüfungsrelevante IT-Architekturkomponenten 7
Abb. 2: Kernelemente eines Unternehmens/einer Behörde 26
Abb. 3: Beschreibung der Abhängigkeiten zwischen Ablauf- und Aufbauorganisation, Produktion und Ressourcen/Informationstechnologie in ADONIS 26
Abb. 4: Auslieferungsstandard Vorlagenbäume von CheckAud® for SAP-Systems 31
Abb. 5: Certified Auditor for SAP Systems (CASAP) - Wissensdomänen 34
Abb. 6: Regelungsbereiche des internen Kontrollsystems nach IDW PS 261 37

Abkürzungsverzeichnis

.BAT-Datei	Dateinamenserweiterung für eine Stapelverarbeitungsdatei (engl. batch file)
.COM-Datei	Dateinamenserweiterung für eine ausführbare Datei (engl. command für Befehl)
.EXE-Datei	Dateinamenserweiterung für eine ausführbare Datei (engl. executable für ausführbar)
ABAP	Advanced Business Application Programming (proprietäre Programmiersprache der SAP SE)
ACL	Name einer Datenanalyse-Software
ADONIS	Produktbezeichnung für eine GPM-Software
AK	Arbeitskreis
AO	Abgabenordnung
APP	Application software (Anwendung)
BSI	Bundesamt für Sicherheit in der Informationstechnik
BPMN	Business Process Model and Notation
BPMS	Business Process Management System
CASAP	Certified Auditor for SAP Systems
CheckAud®	CheckAud® for SAP Systems ist eine eingetragene Marke der IBS Schreiber GmbH, Hamburg
CISA	Certified Information Systems Auditor
DIN	Deutsches Institut für Normung
DOS	Disk Operating System (Bezeichnung für ein Betriebssystem)
DSAG	Deutschsprachige SAP-Anwendergruppe e. V. mit Sitz in Walldorf
DS-GVO	Datenschutz-Grundverordnung
DV	Datenverarbeitung
GemHVO	Gemeindehaushaltsverordnung
GG	Grundgesetz für die Bundesrepublik Deutschland
GPM	Geschäftsprozessmanagement
GO NRW	Gemeindeordnung für das Land Nordrhein-Westfalen
GoB	Grundsätze ordnungsmäßiger Buchführung

GoBD	Grundsätze zur ordnungsmäßigen Führung und Aufbewahrung von Büchern, Aufzeichnungen und Unterlagen in elektronischer Form sowie zum Datenzugriff
GRC	Governance, Risk & Compliance (Unternehmensführung, Risikomanagement sowie Einhaltung der internen und externen Normen)
HGB	Handelsgesetzbuch
HPI	Hasso Plattner Institut
ICS	Industrial Control Systems (Oberbegriff für industrielle Steuerungssysteme)
IDEA	Interactive Data Extraction and Analysis (Bezeichnung für eine Datenanalyse-Software)
IDR	Institut der Rechnungsprüfer und Rechnungsprüferinnen in Deutschland e. V.
IDW	Institut der Wirtschaftsprüfer in Deutschland e. V.
IKS	Internes Kontrollsystem
IEC	International Electrotechnical Commission
ISACA	Information Systems Audit and Control Association
ISAE	International Standard on Assurance Engagements
ISMS	Managementsystem für Informationssicherheit
ISO	International Organization for Standardization (Internationale Organisation für Normung)
IT	Informationstechnologie
ITAF	Information Technology Assurance Framework
ITU	International Telecommunication Union (Internationale Fernmeldeunion)
JAVA	Name einer objektorientierten Programmiersprache
KomHVO NRW	Kommunalhaushaltsverordnung Nordrhein-Westfalen
KrO	Kreisordnung für das Land Nordrhein-Westfalen
LVerbO	Landschaftsverbandsordnung für das Land Nordrhein-Westfalen
LWL	Landschaftsverband Westfalen-Lippe
LWL-RPA	Rechnungsprüfungsamt des Landschaftsverbandes Westfalen-Lippe

LWL-RPO	Rechnungsprüfungsordnung für den Landschaftsverband Westfalen-Lippe
MHKBG NRW	Ministerium für Heimat, Kommunales, Bau und Gleichstellung des Landes Nordrhein-Westfalen
MS-Office	Bezeichnung für ein Office-Paket der Fa. Microsoft (Bürosoftware-Anwendungen)
NKF	Neues Kommunales Finanzmanagement
NKFWG NRW	Gesetz zur Weiterentwicklung des Neuen Kommunalen Finanzmanagements für Gemeinden und Gemeindeverbände im Land Nordrhein-Westfalen und weiterer kommunalrechtlicher Vorschriften
Nr./Nrn.	Nummer/Nummern
NRW	Nordrhein-Westfalen
O2C-Prozess	Order-to-Cash-Prozess (Prozess von der Bestellung bis zum Zahlungseingang)
OPS	Operation per Second/Betrieb
OZG	Gesetz zur Verbesserung des Onlinezugangs zu Verwaltungsleistungen
P2P-Prozess	Purchase to Pay–Prozess (Einkauf bis Bezahlung-Prozess)
PC	Personal Computer
S.	Satz
SAN	Storage-Area-Network
SAP	Ist eine Marke der SAP SE
SAP ERP	SAP ERP ist ein Produkt der SAP SE; ERP steht für Enterprise-Resource-Planning oder Unternehmens-Informationssystem
SAP HANA	Bezeichnung für die In-Memory-Computing-Plattform der SAP SE
SAP SE	Firmenname eines deutschen Softwareherstellers mit Sitz in Walldorf
Strg	Steuerung
WSC	World Standards Cooperation (Arbeitsgemeinschaft dreier weltweit tätiger Organisationen der Normung – IEC, ISO, ITU)

1. Einleitung

Die Digitalisierung in den Behörden schreitet nicht nur aufgrund der gesetzlichen Anforderungen – u. a. mit dem Gesetz zur Verbesserung des Onlinezugangs zu Verwaltungsleistungen (OZG), das die Rahmenbedingungen für die Digitalisierung in der öffentlichen Verwaltung festlegt – stetig voran.[1] Infolgedessen wächst das Aufgabenfeld der örtlichen Rechnungsprüfung insbesondere im Bereich der IT-Prüfung gleichermaßen. In den Handreichungen zum NKF heißt es dazu: „Die Digitalisierung der Geschäftsabläufe in der Gemeinde führt auch zu einer Veränderung der Prüfungskonzepte und verlangt mehr IT-Kenntnisse von den Prüfern. Sie müssen vielfach über Spezialkenntnisse verfügen, um die gemeindlichen Geschäftsabläufe und den Umgang mit der Vielzahl von Daten der Gemeinde sachgerecht beurteilen zu können. Die Digitalisierung beeinflusst daher die Prüfungsarbeit gravierend, denn ohne Verständnis für die Funktionsweise sind automatisierte Buchungen sowie das Zusammenspiel und die Wechselwirkungen von Systemen nur schwer nachvollziehbar."[2]

Das vorliegende Skript soll eine Einführung in die IT-Prüfung der örtlichen Rechnungsprüfung geben.

2. Grundlagen der IT-Prüfung

In diesem Kapitel werden zunächst die Grundlagen der IT-Prüfung betrachtet. Hierzu werden im Einzelnen die Aspekte

- Prüfungsauftrag
- Prüfungsgegenstände
- Prüfungsmaßstäbe
- Informationssicherheit
- Prüfhilfen

in den Fokus genommen.

[1] Das Onlinezugangsgesetz verpflichtet die Behörden dazu, bis zum Jahr 2022 sämtliche Leistungen der Verwaltung auch digital anzubieten.

[2] Siehe Neues Kommunales Finanzmanagement in Nordrhein-Westfalen, Handreichung für Kommunen, 7. Auflage, Seite 1469

2.1. Prüfungsauftrag

Gemäß § 23 Abs. 2 S. 1 Landschaftsverbandsordnung (LVerbO) gelten die Vorschriften der Gemeindeordnung NRW (GO NRW) und ihrer Durchführungsverordnungen sowie § 55 der Kreisordnung sinngemäß. Die GO NRW definiert dann die Aufgaben der örtlichen Rechnungsprüfung in seinen §§ 102 bis 104. § 6 Abs. 1 LVerbO ermächtigt die Landschaftsverbände, ihre Angelegenheiten durch Satzungen zu regeln, soweit die Gesetze nicht etwas Anderes bestimmen. Mit dem Erlass einer Rechnungsprüfungsordnung (LWL-RPO) hat der Landschaftsverband Westfalen-Lippe in Bezug auf die örtliche Rechnungsprüfung davon Gebrauch gemacht. Von Bedeutung für Umfang und Gegenstand der IT-Prüfung ist insbesondere § 5 LWL-RPO (Aufgaben des LWL-Rechnungsprüfungsamtes). Weitere Hinweise hierzu ergeben sich aus § 8 LWL-RPO (Mitteilungspflichten).

Bezogen auf die IT-Prüfung lässt sich aus §§ 102 und 104 GO NRW und den v. g. Bestimmungen der LWL-RPO grundsätzlich folgendes Aufgabenspektrum ableiten:

2.1.1. Gesetzliche Pflichtprüfungen

Prüfung der Programme vor ihrer Anwendung – ex-ante-Prüfung

- Bei Durchführung der Finanzbuchhaltung mit Hilfe automatisierter Datenverarbeitung (IT-gestützte Buchführung) des Landschaftsverbandes und seiner Sondervermögen die Prüfung der Programme vor ihrer Anwendung (§ 104 Abs. 1 Nr. 3 GO NRW i. V. m. § 5 Abs. 1 Buchstabe f LWL-RPO)

Anmerkungen: Das Prüfungsgebot betrifft auch die Änderung dieser Programme sowie Programme für die Erzeugung des Jahresabschlusses und des Gesamtabschlusses.
Die Einführung solcher Systeme wird meistens als Projekt organisiert. Um dem v. g. gesetzlichen Auftrag rechtzeitig nachkommen zu können, ist es angezeigt, diese Projekte begleitend zu prüfen.

Prüfung der Programme zur IT-gestützten Buchführung im laufenden Einsatz – ex-post- Prüfung

- Die laufende Prüfung der Vorgänge in der Finanzbuchhaltung zur Vorbereitung der Prüfung des Jahresabschlusses (§ 102 Abs. 1 S. 1 und § 104 Abs. 1 Nr. 1 GO NRW i. V. m. § 5 Abs. 1 Buchstaben a und d LWL-RPO)

Prüfung der produktiven Programme des Gesamtabschlusses – ex-post-Prüfung

- Die Prüfung des Gesamtabschlusses (§ 102 Abs. 11 GO NRW i. V. m. § 5 Abs. 1 Buchstabe c LWL-RPO sowie § 102 Abs. 3 GO NRW)

2.1.2. Übertragene Aufgaben

Prüfung der sonstigen Informationstechnologie

- Die Prüfung der Verwaltung und der Sondervermögen auf Rechtmäßigkeit, Zweckmäßigkeit und Wirtschaftlichkeit sowie die Aufklärung von Unregelmäßigkeiten (§ 5 Abs. 2 Buchstabe b LWL-RPO)

Anmerkung: Hierunter sind zunächst im Bereich der Sondervermögen die produktiven Programme der IT-gestützten Buchführung einschl. der Jahresabschlussprogramme zu subsumieren – ex-post Prüfung. Im Übrigen fallen hierunter alle Bereiche der Informationstechnologie ohne Finanzbezug; das gilt sowohl für die Zentralverwaltung als auch für die Sondervermögen des LWL (§ 104 Abs. 3 GO NRW i. V. m. § 5 Abs. 2 Buchstabe b LWL-RPO).

Im Bereich Informationstechnologie

- Die Beratung der Verwaltung und Mitwirkung in Projekten (§ 104 Abs. 3 GO NRW i. V. m. § 5 Abs. 2 Buchstabe g LWL-RPO)

Hinweis: Die projektbegleitende Prüfung der Programme zur IT-gestützten Buchführung erfolgt im Rahmen der ex-ante-Prüfung.

2.1.3. Einzelprüfungsaufträge

Einzelaufträge im Bereich Informationstechnologie

Die Landschaftsversammlung, der Landschaftsausschuss und der Rechnungsprüfungsausschuss können dem LWL-Rechnungsprüfungsamt Prüfungsaufträge erteilen. Die Direktorin/der Direktor des Landschaftsverbandes kann Aufträge zur Prüfung unter Mitteilung an die Vorsitzende/den Vorsitzenden des Rechnungsprüfungsausschusses und deren Stellvertreterin/Stellvertreter bzw. dessen Stellvertreterin/Stellvertreter erteilen (§ 104 Abs. 3 und 4 GO NRW i. V. m. § 6 LWL-RPO).

2.1.4. Abgeleitete Prüfungsaufträge

Aus den nachstehend aufgeführten Mitteilungspflichten der Verwaltung lassen sich weitere Aufgaben der IT-Prüfung im LWL-RPA ableiten:

Gutachtliche Stellungnahmen

Das LWL-Rechnungsprüfungsamt ist über alle beabsichtigten, wichtigen organisatorischen Änderungen in der Verwaltung, insbesondere, wenn sie die Haushaltswirtschaft betreffen oder wenn Umstellungen auf Informationsverarbeitung sowie Änderungen in diesem Bereich damit verbunden sind, so rechtzeitig in Kenntnis zu setzen, dass es sich vor der Entscheidung

dazu gutachtlich äußern kann (§ 8 Abs. 1 LWL-RPO).

Besondere Vorkommnisse im Bereich Informationstechnologie
Das LWL-Rechnungsprüfungsamt ist unverzüglich über Betriebsstörungen in der Datenverarbeitung zu unterrichten, wenn dadurch Verwaltungsabläufe wesentlich beeinflusst werden (§ 8 Abs. 3 LWL-RPO).

Mitwirkung bei Prüfungen aufgrund von Mitteilungen nach § 8 Abs. 5 LWL-RPO
Das LWL-Rechnungsprüfungsamt ist von der zuständigen Dienststelle unter Darlegung des Sachverhaltes unmittelbar und unverzüglich zu unterrichten, wenn sich ein begründeter Verdacht auf Verfehlungen oder Unregelmäßigkeiten ergibt, durch die ein Vermögensschaden für den Landschaftsverband entstanden oder zu vermuten ist. Das Gleiche gilt bei Vermögensdelikten, Sachbeschädigungen und Brandstiftungen zum Nachteil des Landschaftsverbandes sowie bei Hinweisen auf Korruption. Hinweis: Dies gilt auch, soweit die Informationstechnologie betroffen ist.

Prüfungen aufgrund von Mitteilungen nach § 8 Abs. 10 LWL-RPO
Dem LWL-Rechnungsprüfungsamt sind die Rollen und Berechtigungen aller Bediensteten mitzuteilen, die befugt sind, Buchungen zu veranlassen. Das Gleiche gilt für die Bediensteten, die befugt sind, Zahlungen zu veranlassen. Hierbei ist der Umfang der Befugnisse anzugeben. Hinweis: Das gilt insbesondere, soweit die Mitteilungen offensichtlich Anlass geben, dass die zugewiesenen Rollen und Berechtigungen die Ordnungsmäßigkeit und/oder Sicherheit der IT-gestützten Buchführung beeinträchtigen.

2.2. Prüfungsgegenstände

Im Kapitel Prüfungsauftrag werden häufig die Begriffe „IT“ und „Programm“ verwendet. Da die beiden Begriffe nicht immer einheitlich verwandt werden, ist es zur Vermeidung von Missverständnissen erforderlich, diese zu definieren.

Ein **Programm** im engeren Sinne ist eine den Regeln einer bestimmten Programmiersprache genügende Folge von Anweisungen (bestehend aus Deklarationen und Instruktionen), um bestimmte Funktionen bzw. Aufgaben oder Probleme mithilfe eines Computers zu bearbeiten

oder zu lösen[3].

Die Vorschrift des § 104 Abs. 1 Nr. 3 GO zur Programmprüfung geht aber historisch bedingt von einem wesentlich weiter gefassten Programmbegriff aus. Denn die Programmprüfung fand zu Zeiten der Großrechner Eingang in die GO. Seit dieser Zeit hat sich die Datenverarbeitung rasant hin zur Informationstechnologie weiterentwickelt. Der Fachausschuss für die Informationstechnologie des Institutes der Wirtschaftsprüfer (IDW) hat in seiner Stellungnahme zur Rechnungslegung: Grundsätze ordnungsmäßiger Buchführung bei Einsatz von Informationstechnologie (IDW RS FAIT 1) festgelegt, dass unter **Informationstechnologie (IT)** die Gesamtheit der im Unternehmen zur elektronischen Datenverarbeitung eingesetzten Hard- und Software verstanden wird. Die GO NRW verwendet aber nach wie vor den Begriff Programm. Daher ist der Begriff unter den heutigen Bedingungen zu interpretieren.

So wurde bereits in den NKF-Handreichungen[4] zu § 103 Abs. 1 S. 1 Nr. 6 GO a. F. darauf hingewiesen, dass die Programmprüfung darauf abzielt, die organisatorisch gesicherte Funktionsfähigkeit der Systeme der Buchführung, der Zahlungsabwicklung sowie der Zuliefersysteme unter Einbeziehung der örtlichen IT-Landschaft und Hardwarestruktur sicherzustellen. Die Prüfungspflicht besteht sowohl für selbsterstellte als auch für von Dritten bezogene IT-Produkte. Weitere Anhaltspunkte zur Interpretation des Programmbegriffs ergeben sich aus den Grundsätzen zur ordnungsmäßigen Führung und Aufbewahrung von Büchern, Aufzeichnungen und Unterlagen in elektronischer Form sowie zum Datenzugriff (GoBD). Diese wurden mit Schreiben des Bundesministers der Finanzen vom 14.11.2014 erlassen, ersetzen die Grundsätze ordnungsmäßiger DV-gestützter Buchführungssysteme (GoBS) und sind nach § 28 Absatz 5 Kommunalhaushaltsverordnung Nordrhein-Westfalen (KomHVO NRW) bei einer IT-gestützten Buchführung zu beachten.
Die GoBD nennen neben dem Haupt(buchführungs)system auch Vor- und Nebensysteme, z. B. explizit Anlagenbuchführung, Lohnbuchführungssystem, Kassensystem, Warenwirtschaftssystem, Zahlungsverkehrssystem, Materialwirtschaft, Fakturierung, Zeiterfassung, Archivsystem, Dokumenten-Management-System einschließlich der Schnittstellen zwischen den

[3] ISO/IEC 2382-1:1993 definiert „computer program": „A syntactic unit that conforms to the rules of a particular programming language and that is composed of declarations and statements or instructions needed to solve a certain function, task, or problem." Bis 2001 definierte die DIN 44300 „Informationsverarbeitung Begriffe" identisch.

[4] vgl. MHKBG, Neues Kommunales Finanzmanagement in Nordrhein-Westfalen – Handreichung für Kommunen (7. Auflage), Seite 1606, letzter Absatz

Systemen. Dabei kommt es aber nicht auf die Bezeichnung des Systems an, sondern auf die Frage, ob in einem System buchführungs- oder aufzeichnungspflichtige Daten erfasst, erzeugt, empfangen, übernommen, verarbeitet, gespeichert oder übermittelt werden.

Weiter müssen nach den GoBD Daten mit Einfluss auf Buchungen oder IT-gestützte Aufzeichnungen nachvollziehbar sein (z. B. durch Historisierung, Protokollierung, Verfahrensdokumentation). Dies betrifft daher auch die Basis-Services (z. B. Datensicherung und Virenschutz), die Basis-Architekturkomponenten (Storage-Area-Network (SAN), Datenbanken, Betriebssysteme, etc.) sowie die Netzwerkinfrastruktur. Wegen ihrer Bedeutung für die Informationssicherheit muss die Gebäudeinfrastruktur ebenfalls betrachtet werden.

Gestützt auf diesen umfassenden Programmbegriff betreffen die Prüfungsgegenstände in der IT-Prüfung die **Gesamtheit** der im LWL zur elektronischen Datenverarbeitung eingesetzten Hard- und Software sowie die dafür genutzten Netzwerke und Gebäude.

Die Fachanwendungen nutzen die Basis-Services, die für alle Fachanwendungen bereitgestellt werden. Beispielsweise werden mittels der Firewall und der Virenschutzprogramme Angriffe von außen, sogenannte Cyberangriffe, abgewehrt. Die Datensicherung erfolgt global für die Daten aller Fachanwendungen.

Die Benutzer, Gruppen und Computer aller Fachanwendungen werden in einem zentralen Active Directory, dem Verzeichnisdienst für Microsoft Windows Server, verwaltet.

Ebenso nutzen die Fachanwendungen Basis-Architekturkomponenten. Der Betrieb der Fachanwendungen ist abhängig von den Betriebssystemen, auf denen sie laufen. Die Daten der Fachanwendungen werden über Netzwerkverbindungen übertragen und auf IT-Systemen gespeichert, die wiederum in bestimmten Räumen stehen. Die ordnungsmäßige Funktionsweise der Fachanwendungen ist somit abhängig von den untergelagerten Ebenen.

In dem nachfolgenden Schaubild wird diese vertikale Ebene, neben der bisher primär horizontalen Betrachtungsweise der Fachanwendungen, deutlich.

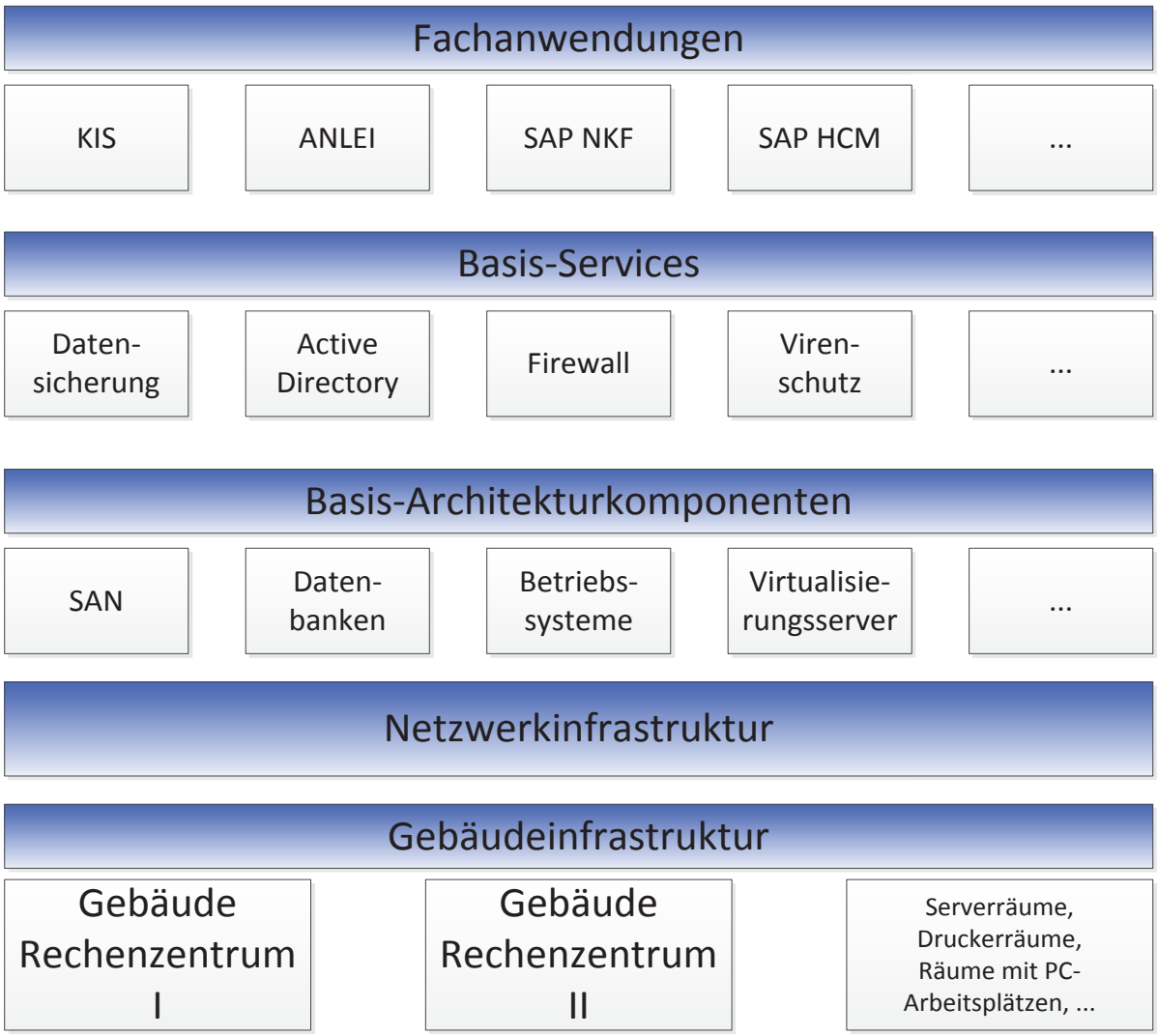

Abb.1: Prüfungsrelevante IT-Architekturkomponenten

2.3. Prüfungsmaßstäbe

Den Prüfungen des LWL-RPA liegen die Anforderungen zur Ordnungsmäßigkeit zugrunde. Der Ordnungsmäßigkeitsgrundsatz umfasst die Rechtmäßigkeit, Zweckmäßigkeit und Wirtschaftlichkeit. Bei der Durchführung jeder Prüfung gilt die Prüfungshierarchie Rechtmäßigkeit vor Zweckmäßigkeit sowie vor Wirtschaftlichkeit.

Der absolute Vorrang der Prüfung der Rechtmäßigkeit ergibt sich aus der verfassungsrechtlichen Verankerung des Legalitätsprinzips (Art. 20 Abs. 3 GG). Der relative Vorrang der Prüfung der Zweckmäßigkeit vor der Wirtschaftlichkeit leitet sich daraus ab, dass es nicht sinnvoll ist, falsche Maßnahmen wirtschaftlich durchzuführen.