LANDTAG MECKLENBURG-VORPOMMERN **Drucksache 8/4703**
8. Wahlperiode **17.03.2025**

UNTERRICHTUNG

durch den Landesrechnungshof

Sonderbericht gemäß § 99 der Landeshaushaltsordnung Mecklenburg-Vorpommern – Herausforderungen bei der Digitalisierung der Landesverwaltung

Zugeleitet mit Schreiben der Präsidentin des Landesrechnungshofes vom 11. März 2025

Inhaltsverzeichnis

Abbildungsverzeichnis

Tabellenverzeichnis

Abkürzungsverzeichnis

AfO	Ausschuss für Organisationsfragen
BeLVIS	Beauftragter der Landesverwaltung für Informationssicherheit
BSI	Bundesamt für die Sicherheit in der Informationstechnik
CERT	Cyber Emergency Response Team
CIO	Beauftragte der Landesregierung Mecklenburg-Vorpommern für Informationstechnologie und Digitalisierung (Chief Information Officer)
DSGVO	Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung)
DVC	Deutsche Verwaltungscloud
DVZ (M-V GmbH)	Datenverarbeitungszentrum Mecklenburg-Vorpommern GmbH
DVZG M-V	Gesetz über die Rechtsstellung des Datenverarbeitungszentrums Mecklenburg-Vorpommern (Datenverarbeitungszentrumsgesetz)
EGovG M-V	Gesetz zur Förderung der elektronischen Verwaltungstätigkeit in Mecklenburg-Vorpommern (E-Government-Gesetz Mecklenburg-Vorpommern - EGovG M-V)
EfA	Einer für Alle
eShop	Elektronisches Bestellsystem des LAiV, zentrales Einkaufsportal für die Landesverwaltung Mecklenburg-Vorpommern
EVB-IT	Ergänzende Vertragsbedingungen für die Beschaffung von IT-Leistungen
GGO I	Gemeinsame Geschäftsordnung I der Ministerien des Landes Mecklenburg-Vorpommern bzw. Gemeinsame Geschäftsordnung I der Ministerien und der Staatskanzlei des Landes Mecklenburg-Vorpommern
GGO II	Gemeinsame Geschäftsordnung II der Landesregierung
GmbH	Gesellschaft mit beschränkter Haftung
GPO	Geschäftsprozessoptimierung
GWB	Gesetz gegen Wettbewerbsbeschränkungen
ISB	Informationssicherheitsbeauftragter
IQMV	Institut für Qualitätsentwicklung
KofIS	Kommission für Informationssicherheit in der Landesverwaltung
kw	künftig wegfallend
LAGuS	Landesamt für Gesundheit und Soziales
LAF	Landesamt für Finanzen Mecklenburg-Vorpommern
LAiV	Landesamt für innere Verwaltung
LHO	Landeshaushaltsordnung Mecklenburg-Vorpommern
LUNG	Landesamt für Umwelt, Naturschutz und Geologie Mecklenburg-Vorpommern
MG	Maßnahmegruppe
NIS-2-Richtlinie	Richtlinie (EU) 2022/2555 des Europäischen Parlaments und des Rates vom 14. Dezember 2022 über Maßnahmen für ein hohes gemeinsames

	Cybersicherheitsniveau in der Union
OZG	Onlinezugangsgesetz
RIT	Rat der IT-Verantwortlichen
Tz(n).	Textzahl(en)
VgV	Verordnung über die Vergabe öffentlicher Aufträge (Vergabeverordnung)
VV	Verwaltungsvorschrift
VZÄ	Vollzeitäquivalente
Zendis	Zentrum für Digitale Souveränität
ZDMV	Zentrum für Digitalisierung Mecklenburg-Vorpommern
ZDMVG	Gesetz zur Errichtung des Landesamtes Zentrum für Digitalisierung Mecklenburg-Vorpommern

Abkürzung und Bezeichnung der Ressorts

STK	Staatskanzlei
IM	Innenministerium
JM	Justizministerium
FM	Finanzministerium
WM	Wirtschaftsministerium
LM	Landwirtschaftsministerium
BM	Bildungsministerium
WKM	Wissenschaftsministerium
SM	Sozialministerium

Lesehinweis

Fachbegriffe werden im Glossar erläutert. Dies soll die Lesbarkeit des Textes verbessern. Erläuterte Fachbegriffe sind durch einfache Unterstreichung kenntlich gemacht.

I Wesentliche Handlungsempfehlungen

(1) Die Landesverwaltung ist organisatorisch derzeit nicht so aufgestellt, dass sie die Herausforderungen der Digitalisierung bewältigen kann. Die Abteilung „Digitale Verwaltung; digitale Infrastruktur und Geoinformation“ (Digitalisierungsabteilung) im Innenministerium lässt in ihrer Aufbauorganisation eine strategische Schwerpunktsetzung nicht ausreichend erkennen. Dem Landesamt Zentrum für Digitalisierung Mecklenburg-Vorpommern (ZDMV) ist es bis Ende 2024 nicht gelungen, die ihm zugewiesenen operativen Aufgaben zufriedenstellend wahrzunehmen. Es konnte seine Arbeitsfähigkeit noch nicht herstellen. Es bestehen Defizite bei der Zusammenarbeit des für Digitalisierung zuständigen Innenministeriums mit den anderen obersten Landesbehörden im Rat der IT-Verantwortlichen (RIT).

Das Innenministerium sollte unverzüglich die Handlungsfähigkeit der für Digitalisierung zuständigen Abteilung im Innenministerium und im ZDMV organisatorisch und personell sicherstellen. Die Zusammenarbeit des Innenministeriums mit den anderen obersten Landesbehörden im RIT muss verbessert werden (vgl. Tzn. 99 bis 116).

(2) IT-Sicherheitstests haben kritische Schwachstellen in der Informationssicherheit des Landes offengelegt. Diese bestehen weiterhin. Das Innenministerium erstellt keine regelmäßigen IT-Sicherheitslageberichte für die Landesverwaltung. Der Beauftragte der Landesverwaltung für Informationssicherheit (BeLVIS) verfügt nicht über ausreichende Weisungs- und Durchgriffsrechte. Die personelle Ausstattung in der Informationssicherheitsorganisation ist unzureichend.

Das Innenministerium hat die erkannten Schwachstellen in der Informationssicherheit unverzüglich zu beseitigen. Es hat außerdem unverzüglich die Voraussetzung für regelmäßige IT-Sicherheitslageberichte zu schaffen. Die Stellung des BeLVIS ist zeitnah zu stärken. Die personelle Ausstattung in der Informationssicherheitsorganisation ist zu verbessern (vgl. Tzn. 241 bis 275).

(3) Die Aufgaben- und Zuständigkeitsverteilung ist komplex. Mit Digitalisierungsaufgaben sind die Digitale Verwaltung, digitale Infrastruktur und Geoinformation (Digitalisierungsabteilung) im Innenministerium, das Landesamt Zentrum für Digitalisierung Mecklenburg-Vorpommern (ZDMV), die DVZ M-V GmbH sowie Organisationseinheiten in den Fachressorts befasst.

Die Landesregierung sollte unverzüglich die Zuständigkeiten für Digitalisierungsaufgaben prüfen und optimieren. Insbesondere sollte die Landesregierung prüfen, welche Aufgaben in welcher Rechtsform die DVZ M-V GmbH zukünftig wahrnehmen soll (vgl. Tzn. 147 bis 173).

(4) Es fehlen wesentliche regulatorische Voraussetzungen für die Digitalisierung und den IT-Einsatz. Bereits vorhandene Regelungen sind veraltet und genügen nicht mehr den aktuellen Rahmenbedingungen. Insbesondere bedarf es einer Anpassung an den übergeordneten Rechtsrahmen (Bundes- und Europarecht). Landesrechtliche Regelungen sind häufig so ausgestaltet, dass sie eine Digitalisierung der Verwaltungsleistung erschweren (Digitalisierungshemmnisse).

Das Innenministerium sollte unverzüglich den Entwurf eines Informationssicherheitsgesetzes in den Gesetzgebungsprozess einbringen. Es sollte zeitnah den Anpassungsbedarf vorhandener Regelungen prüfen. Die Landesregierung sollte alle landesrechtlichen Regelungen hinsichtlich ihrer Digitalisierungsfähigkeit prüfen, um Digitalisierungshemmnisse zu beseitigen. Eine Verpflichtung dazu sollte in die GGO II aufgenommen werden (vgl. Tzn. 51 bis 97).

(5) Die Landesregierung hat bisher nur in Ansätzen Strategien zur Digitalisierung der Verwaltung erarbeitet. Es fehlen grundlegende Aussagen und Festlegungen, welchen Beitrag die Digitalisierung leisten soll, um die Funktionsfähigkeit der Landesverwaltung zu gewährleisten, die Aufgabenwahrnehmung zu verbessern und einen Mehrwert für Bürgerinnen und Bürger sowie Unternehmen zu schaffen. Demzufolge fehlen auch messbare Ziele und der strategische Überbau für abgeleitete Digitalisierungsstrategien der Ressorts und ihrer Geschäftsbereiche. Operatives und strategisches IT-Controlling werden nicht ausreichend wahrgenommen.

Die Landesregierung sollte zeitnah eine Digitalisierungsstrategie erarbeiten, in der sie verbindlich messbare strategische Ziele festschreibt. Mit dem zeitnahen Aufbau eines strategischen und eines operativen IT-Controllings einschließlich eines IT-Risikomanagements wären die Fortschritte zur Zielerreichung transparent (vgl. Tzn. 29 bis 50).

(6) Es fehlen Vorgaben für IT-Architekturen in der Landesverwaltung und eine Betriebsstrategie für Fachverfahren. Die Abhängigkeit der Landesverwaltung von bestimmten Herstellern und Produkten ist hoch.

Das Innenministerium sollte Vorgaben zur IT-Architektur in der IT-Richtlinie festlegen und eine Betriebsstrategie für Fachverfahren erarbeiten. Die Architektur sollte vorrangig auf bundesweit geltenden Standards beruhen. Das Innenministerium sollte die Nutzung von Open Source prüfen. Insbesondere sollte es prüfen, ob die vom Zentrum für digitale Souveränität (Zendis) entwickelten Lösungen in der Landesverwaltung eingesetzt werden können (vgl. Tzn. 224 bis 240).

(7) Ein zentrales Vertragsmanagement und -controlling in der Landesverwaltung fehlt bis heute.

Das Innenministerium sollte ein einheitliches Vertragsmanagement und -controlling als Basisdienst zentral zur Verfügung zu stellen (vgl. Tzn. 211 bis 218).

(8) Es besteht weiterhin ein hoher Bedarf an Haushaltsmitteln für die Finanzierung der Digitalisierung der Landesverwaltung. Die Landesverwaltung schiebt eine hohe „Bugwelle“ an Haushaltsresten bei den IT-Ausgaben vor sich her. In der Landesverwaltung werden Fachverfahren eingesetzt, bei denen sich aufgrund der Nutzungsdauer Ablösebedarfe abzeichnen. Ein umfassender Überblick über die Ablösebedarfe und die daraus folgenden Finanzierungsbedarfe für Nachfolgelösungen existiert nicht.

Die Behörden haben die Ablösebedarfe systematisch zu ermitteln und dem ZDMV rechtzeitig anzuzeigen. Das ZDMV sollte für alle Fachverfahren eine Pla-

nung zum voraussichtlichen Ablösezeitpunkt vorlegen. Die voraussichtlichen Finanzierungsbedarfe sind in der mittelfristigen Finanzplanung zu berücksichtigen (vgl. Tzn. 201 bis 210).

II Prüfungsfeststellungen im Einzelnen

1 Vorbemerkungen

1.1 Anlass für den Bericht

(9) Rechtliche Vorgaben zwingen die Verwaltung zum einen dazu, digitaler zu werden (z. B. Onlinezugangsgesetz, Registermodernisierungsgesetz, Single Digital Gateway Verordnung). Dies korrespondiert mit den Erwartungen der Bürgerinnen und Bürger sowie der Unternehmen nach einfachen und sicheren digitalen Zugängen zu Verwaltungsleistungen.

Zum anderen steigen kontinuierlich die rechtlichen und technischen Anforderungen an einen sicheren und ordnungsgemäßen Einsatz von Informationstechnik (IT). Hierzu zählen z. B. Regelungen zur Informationssicherheit (noch umzusetzende NIS-2-Richtlinie[1]) und zum Datenschutz (DSGVO).

(10) Nicht zuletzt zwingen die Vorgaben des Haushaltsrechts sowie die begrenzten finanziellen Ressourcen die Verwaltung zum wirtschaftlichen Handeln.

(11) Die Handlungs- und Funktionsfähigkeit der Verwaltung ist hochgradig abhängig davon, dass resiliente und sichere digitale Lösungen zur Verfügung stehen. Erfolgreiche Cyberangriffe in jüngster Vergangenheit haben diese Abhängigkeit deutlich und schmerzhaft vor Augen geführt.[2]

(12) Die Digitalisierung der Verwaltung bewegt sich in einem Spannungsfeld aus Ordnungsmäßigkeit (Rechtmäßigkeit einschließlich Datenschutz und Schutz des Dienstgeheimnisses, Informationssicherheit), Wirtschaftlichkeit (effiziente Lösungen, Finanzierbarkeit) und Funktionsfähigkeit der Verwaltung (effektive, pragmatische, bürgerorientierte Lösungen). Diese Anforderungen müssen so berücksichtigt werden, dass die Digitalisierung der Verwaltung einen möglichst großen Beitrag zu einer effektiven und effizienten Verwaltung leistet.

(13) Der Digitalisierung kommt daher eine besondere Bedeutung für die Handlungs- und Funktionsfähigkeit einer modernen und bürgerorientierten Verwaltung zu. Dieser Bedeutung ist die Landesregierung in den letzten Jahren nicht gerecht geworden. Dies belegt eine Vielzahl von Prüfungsfeststellungen des Landesrechnungshofes.

(14) Der Landesrechnungshof hat deshalb seine Feststellungen der letzten Jahre und daraus abgeleitete Handlungsempfehlungen in diesem Bericht zusammengefasst. Dies auch vor dem Hintergrund, dass die Funktionsfähigkeit der Verwaltung durch das sinkende Erwerbspersonenpotenzial immer stärker an ihre Grenzen stößt.

---

[1] Zum Anwendungsbereich der Richtlinie für die Bundesländer siehe Art. Art. 3 Abs. 1 lit. d i.V.m. Art. 2 Abs. 2 Buchstabe f Ziffer i und Art. 2 Abs. 1 S. 1 NIS-2-RL sowie die Erläuterungen dazu von Hornung/Schallbruch, IT-Sicherheitsrecht (2024), § 25 Öffentliche Verwaltung, Rz. 21.

[2] Z. B. im Landkreis Ludwigslust-Parchim und in der Landeshauptstadt Schwerin sowie im Landkreis Vorpommern-Rügen.

Der Bericht soll aufzeigen, mit welchen Maßnahmen in einzelnen Handlungsfeldern der derzeitige Stillstand beendet und Defizite beseitigt werden können. Der Landesrechnungshof wird diese Empfehlungen auch als Maßstab für künftige Prüfungen heranziehen.

1.2 Struktur des Berichts

(15) Der Bericht gliedert sich in die Handlungsfelder Strategie, Ziele und Controlling, regulative Voraussetzungen, organisatorische Voraussetzungen, Finanzierung und Informationssicherheit. Der Landesrechnungshof hat seine Empfehlungen und Forderungen diesen Handlungsfeldern zugeordnet. Mit der Zuordnung zu Handlungsfeldern will er die Landesregierung dabei unterstützen, die Probleme systematisch, strukturiert und priorisiert zu lösen.

(16) Soweit nichts anderes angegeben, beziehen sich die Ausführungen auf den Informationsstand des Landesrechnungshofes bis zum 30. September 2024.

(17) Das Ministerium für Inneres, Bau und Digitalisierung (Innenministerium) hat am 10. Februar 2025 nach Abstimmung mit der Staatskanzlei und dem Finanzministerium Stellung genommen.

2 Umsetzungen der Entschließungen des Landtages und der Empfehlungen des Landesrechnungshofes

(18) Der Landesrechnungshof hat auf Basis seiner zahlreichen Prüfungsfeststellungen 35 Empfehlungen zum Einsatz von IT und zur Digitalisierung der Landesverwaltung erarbeitet. Diese führten zu 14 Entschließungen des Landtages.

(19) Der Landesrechnungshof hat deutliche Unterschiede bei der Umsetzung seiner Empfehlungen zwischen den Ressorts festgestellt. Umgesetzt wurden Empfehlungen vor allem im Geschäftsbereich des Finanzministeriums. Die teilweise bzw. nicht umgesetzten Empfehlungen und Entschließungen richteten sich überwiegend an das für Digitalisierung zuständige Ministerium (zunächst das Energie- und dann das Innenministerium).

Die fehlende bzw. unzureichende Umsetzung durch das für Digitalisierung zuständige Ministerium hat zu einem deutlichen Handlungsstau geführt. Dieser hat – bereits heute – Auswirkungen auf die uneingeschränkte Funktionsfähigkeit der Landesverwaltung.

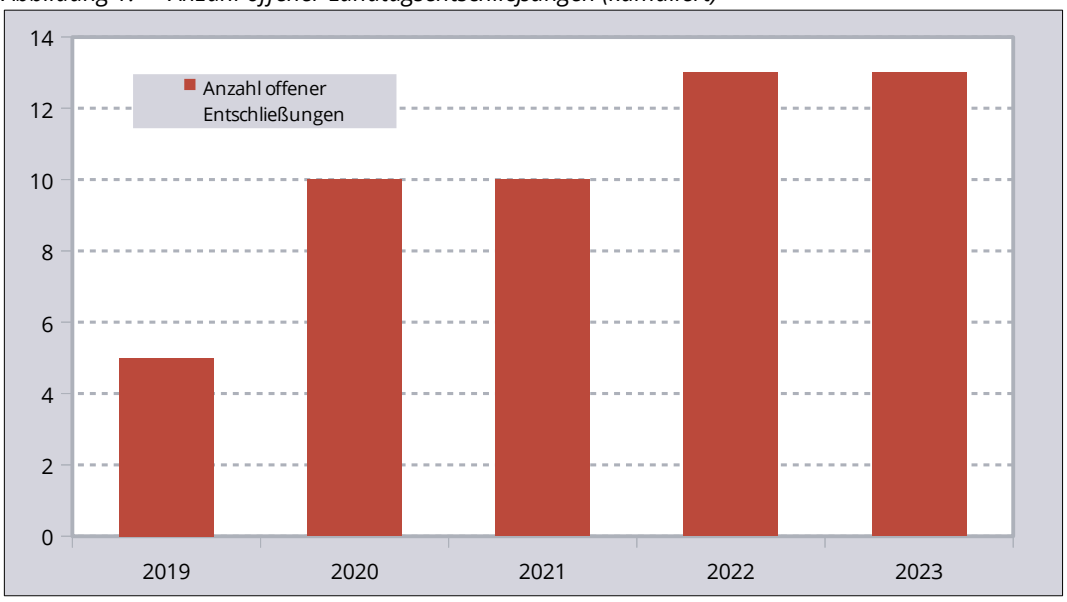
2.1 Entschließungen des Landtages umsetzen

(20) Von den 14 Entschließungen des Landtages wurde lediglich eine (!) vollumfänglich umgesetzt. 11 Entschließungen wurden nicht bzw. nicht fristgemäß und zwei Entschließungen nur teilweise umgesetzt. Einige Entschließungen wurden lediglich formal erledigt. So wurden beispielsweise IT-Standards festgelegt. Diese erfüllen jedoch nicht die inhaltlichen Anforderungen an solche Standards (vgl. Tzn. 72 ff). Da das Innenministerium einige Entschließungen nicht fristgemäß oder zeitnah umgesetzt hat, hat der Landtag einige Entschließungen mehrfach getroffen. So hat er z. B. Entschlie-

ßungen zum IT-Sicherheitsgesetz 2019 beschlossen und diese 2022 sowie 2023 erneuert.

(21) In Abbildung 1 ist die Entwicklung der Anzahl offener Entschließungen des Landtags von 2019 bis 2023 dargestellt. 2023 waren noch 13 Entschließungen offen.

Abbildung 1: Anzahl offener Landtagsentschließungen (kumuliert)



Quelle: eigene Darstellung.

(22) Die Entschließungen des Landtages und deren Umsetzungsstand sind in Anlage 1 im Einzelnen dargestellt.

(23) Das Innenministerium teilt nicht die Auffassung des Landesrechnungshofes, dass es von den Entschließungen des Landtages nur eine umgesetzt habe. Soweit inhaltlich identische oder teilidentische Beschlüsse mehrfach gezählt würden, sei diese Zählweise irreführend.

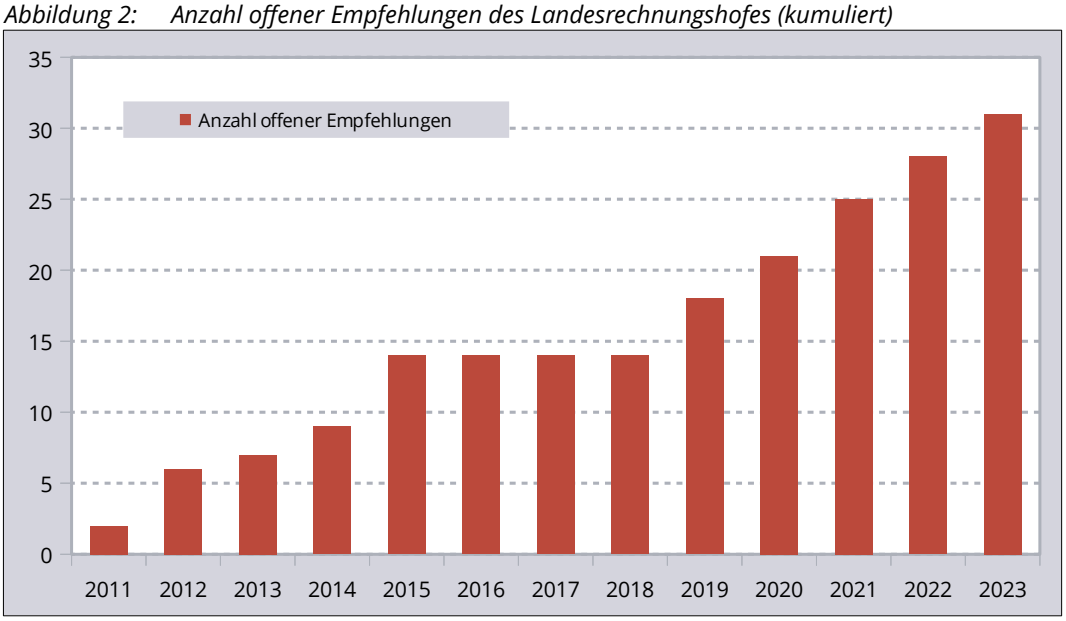
(24) Richtig ist, dass einige der aufgenommenen Entschließungen (z. B. zur IT- und Digitalisierungsstrategie, zur IT-Richtlinie und zu den IT-Landesstandards) tatsächlich inhaltlich (teil)identisch sind. Der Landtag hat wiederkehrend (teil)identische Entschließungen gefasst, weil die jeweils vorausgegangene Entschließung nicht oder nicht vollständig umgesetzt wurde. Der Landesrechnungshof hat den Umsetzungsstand kumuliert dargestellt. Dies ist nicht irreführend.

2.2 Empfehlungen des Landesrechnungshofes umsetzen

(25) Auf der Basis der Prüfungsergebnisse hat der Landesrechnungshof in seinen Landesfinanzberichten seit 2011 insgesamt 35 Empfehlungen ausgesprochen. Dabei handelt es sich um Empfehlungen mit unterschiedlicher Reichweite. Sie reichen von grundlegenden Empfehlungen z. B. im Bereich Regulierung für das gesamte Land bis zu Einzelmaßnahmen in einer Behörde. Davon wurden 17 nicht, 14 teilweise und vier vollständig umgesetzt. Infolge der fehlenden Umsetzung hat der Landesrechnungshof zu einigen Themen mehrfach Empfehlungen ausgesprochen.

(26) In Abbildung 2 ist die Entwicklung der Anzahl offener Empfehlungen des Landesrechnungshofes von 2011 bis 2023 dargestellt. 2023 waren noch 31 Empfehlungen offen.

Abbildung 2: Anzahl offener Empfehlungen des Landesrechnungshofes (kumuliert)



Quelle: eigene Darstellung.

(27) Die Anzahl der offenen Empfehlungen hat sich zunächst bis 2015 und noch einmal deutlich ab 2019 erhöht. Der Landesrechnungshof hat seit 2018 seine Prüfungen im Themenfeld Organisation und IT intensiviert.

(28) Das Innenministerium teilt nicht die Bewertung der Umsetzungsstände der angeführten 35 Empfehlungen des Landesrechnungshofes. Soweit inhaltlich identische oder teilidentische Empfehlungen mehrfach gezählt würden, sei dies irreführend. Bei einigen Empfehlungen handele es sich um Daueraufgaben, die ihrer Natur gemäß einen fortlaufenden Charakter hätten und mithin nicht als final „umgesetzt“ bewertet werden könnten.

(29) Richtig ist, dass einige Empfehlungen des Landesrechnungshofes (z. B. zu den IT-Landesstandards) inhaltlich (teil)identisch sind. Der Landesrechnungshof hat (teil)identische Empfehlungen erneut ausgesprochen, weil vorausgegangene Empfehlungen nicht oder nicht vollständig umgesetzt wurden. Seine Darstellung ist kumuliert und zählt nichts mehrfach. Dies ist gerade nicht irreführend.

Der in diesem Abschnitt und in den Anlagen 1 und 2 dargestellte Umsetzungsstand der Entschließungen des Landtages und der Empfehlungen des Landesrechnungshofes zeigt, dass die jeweiligen Landesregierungen den wachsenden Herausforderungen der Digitalisierung über die letzten Wahlperioden hinweg nicht zeitgerecht und nur unvollständig begegnet sind.

3 Strategie, Ziele und Controlling

3.1 IT- und Digitalisierungsstrategie erarbeiten

(30) Der Landesrechnungshof hatte in mehreren Landesfinanzberichten kritisiert, dass die Landesregierung weder über eine aktuelle IT-Strategie noch über eine Digitalisierungsstrategie verfügt. In Ermangelung festgelegter strategischer Ziele fehlt die Basis für operative Entscheidungen. Ohne strategische Grundsatzentscheidungen der Landesregierung können die Ressorts und die nachgeordneten Behörden beim Einsatz der IT nur Einzellösungen anstreben, die nicht zwingend in eine konsistente und widerspruchsfreie Landesstrategie münden.

(31) Der Landtag hatte bereits 2019[3] und erneut 2020[4] das seinerzeit zuständige Energieministerium bzw. die Landesregierung aufgefordert, Strategien zur Digitalisierung und zum IT-Einsatz zu erarbeiten.

(32) Strategien sollen die übergeordneten Ziele enthalten, aus denen konkrete operative Ziele abgeleitet und in einer Zielstruktur dargestellt werden. Operative Ziele müssen anhand qualitativer und quantitativer Kennzahlen messbar sein. Nachgeordnete Verwaltungsebenen müssen ihre Strategien an den übergeordneten Strategien ausrichten.[5]

(33) Eine IT-Strategie umfasst die übergeordneten Aussagen zu Prinzipien und Leitlinien des IT-Einsatzes, den Beitrag der IT zur Erreichung strategischer Ziele, Organisation und Steuerung, Finanzierung des IT-Einsatzes, IT-Architekturen und IT-Infrastruktur sowie zur Konsolidierung und Vereinheitlichung der eingesetzten IT.[6] Teilelemente der IT-Strategie sind auch die Digitalisierung von Verwaltungsprozessen sowie die Konsolidierung der Fachverfahrenslandschaft.[7]

(34) Eine Digitalisierungsstrategie betrifft auch Themenfelder außerhalb der Verwaltung (z. B. Digitalisierung der Wirtschaft, Schulen, Hochschulen). Bezüge zur IT-Strategie ergeben sich insbesondere, wenn die digitalen Schnittstellen zwischen staatlichen Stellen untereinander und zu anderen Stellen, z. B. kommunalen Stellen, der Wirtschaft und den Bürgern angesprochen werden.

(35) Die strategischen Ziele sind mit abrechenbaren bzw. messbaren Kennzahlen zu versehen, an denen die Zielerreichung zu messen ist. Die Strategien sind regelmäßig fortzuschreiben.

---

3 Vgl. Drs. 7/4162, Ziff. I 1 mit Bezug auf LFB 2019 Tzn. 106, 107.

4 Vgl. Drs. 7/5579, Ziff. I 5 mit Bezug auf LFB 2020 Tzn. 152 – 206.

5 Vgl. Rechnungshöfe des Bundes und der Länder (2024): Grundsätze der Verwaltungsorganisation, S. 3., www.lrh-mv.de/Veröffentlichungen/Gemeinsame-Dokumente-der-Rechnungshöfe/.

6 Vgl. Rechnungshöfe des Bundes und der Länder (2020): Mindestanforderungen zum Einsatz der Informationstechnik, S. 8 f. www.lrh-mv.de/Veröffentlichungen/Gemeinsame-Dokumente-der-Rechnungshöfe/.

7 Vgl. Landesrechnungshof Mecklenburg-Vorpommern (2023): Jahresbericht 2023 (Teil 1) Landesfinanzbericht 2023, S. 48f.

(36) Aus den Strategien sind IT-Maßnahmen abzuleiten, zu priorisieren und mit operationalen Kennzahlen zu versehen.

(37) Die Landesregierung hat bisher keine aktuellen Strategien mit diesen Mindestinhalten beschlossen.

(38) Lediglich für den Teilbereich der Informationssicherheit hat das Innenministerium die Informations- und Datenschutzstrategie 2023 erarbeitet.

(39) Der Landesrechnungshof begrüßt, dass für diesen Teilbereich einer IT-Strategie strategische Überlegungen vorgenommen wurden. Die dort dargestellten Handlungsfelder und Maßnahmen sind für die Informationssicherheit und den technischen Datenschutz erforderlich.

Die im Intranet der Landesverwaltung veröffentlichte Fassung lässt jedoch offen, wer die Informations- und Datensicherheitsstrategie beschlossen hat. Es ist auch nicht zu erkennen, wer Adressat der Ziele ist und mit welchem rechtlichen Verbindlichkeitsgrad die Adressaten diese Ziele umzusetzen haben.

Im Wesentlichen enthält das Papier einen Problemaufriss und beschreibt die Handlungsfelder. Abrechenbare Ziele fehlen.

(40) Die Beauftragte der Landesregierung für Informationstechnologie und Digitalisierung (CIO) hat gemäß § 16 Abs. 3 EGovG M-V die IT-Politik des Landes strategisch auszurichten und Beschlüsse zu E-Government und IT-Strategie herbeizuführen. Daraus ergibt sich neben den oben aufgeführten Entschließungen des Landtages unmittelbar auch ein gesetzlicher Auftrag, eine IT- und E-Government-Strategie zu erarbeiten und weiterzuentwickeln.

(41) Das Innenministerium hat gemäß § 16 Abs. 3 Nrn. 2, 3 EGovG M-V im Einvernehmen mit der Staatskanzlei und den anderen Ressorts zeitnah eine IT- und eine Digitalisierungsstrategie zu erarbeiten. Es sollte dabei auch einen Prozess einführen, der sicherstellt, dass

- überwacht wird, ob die strategischen Ziele erreicht werden,
- auf eine erkannte Zielabweichung reagiert wird und
- die Strategie fortentwickelt wird.

(42) Das Innenministerium teilt mit, dass es die Informations- und Datensicherheitsstrategie in 2025 fortschreiben werde. Die Hinweise des Landesrechnungshofes werde es berücksichtigen. Die Empfehlung zur Weiterentwicklung der IT- und E-Government-Strategie werde es umsetzen.

Zur Zeit entwickle der IT-Planungsrat eine föderale Digitalstrategie. Die Kommunen erarbeiteten derzeit ihre Strategie mit dem Schwerpunkt intensiverer Zusammenarbeit. Die Landesverwaltung werde ihre Strategie ab Mitte 2025 ausgehend von der föderalen Digitalstrategie und unter Berücksichtigung der kommunalen Digitalstrategie fortschreiben.

(43) Der Landesrechnungshof begrüßt dies. Die ebenenübergreifende Zusammenarbeit bei der Digitalisierung (Bund, Land, Kommune) erfordert aufeinander abge-

stimmte Strategien. Insbesondere für das Zusammenwirken der Landesverwaltung mit den kommunalen Verwaltungen bedarf es strategischer Zielvorgaben des Landes.

Die Landesregierung ist verantwortlich dafür, eine Strategie für die Landesverwaltung zu erarbeiten. Ein abgestimmtes Vorgehen entbindet das Land nicht von seiner Verantwortung. Das Innenministerium ist zuständig und verantwortlich, einen rechtmäßigen, wirtschaftlichen und nachhaltig finanzierbaren Einsatz der IT in der Landesverwaltung sicherzustellen. Diese Verantwortung kann nicht auf andere Ebenen abgeschoben werden. Die Landesstrategie ist regelmäßig anhand der föderalen Strategievorgaben zu überprüfen und ggf. anzupassen.

Die obersten Landesbehörden haben für sich und ihre Geschäftsbereiche in den Modernisierungs- und Optimierungskonzepten Ziele und Maßnahmen festgelegt, die u. a. auch die Digitalisierung betreffen. Für diese Ziele fehlt der übergeordnete Rahmen einer Landesstrategie.

Das Innenministerium sollte die Strategie zeitnah überarbeiten.

(44) Das Innenministerium teilt die Auffassung des Landesrechnungshofes nicht vollumfänglich.

Grundsätzlich existierten einheitliche Vorgaben für die Digitalisierung mit der Strategie der Landes-IT und auch Vorgaben zum zentralen Arbeitsplatz.

Überdies seien rechtliche Rahmenbedingungen wie die E-Government-Basisdienste-Landesverordnung, die IT–Richtlinie oder auch Vorgaben aus dem E-Government-Gesetz M-V ressortübergreifend abgestimmt, geeint und verbindlich.

(45) Das Innenministerium hat eine Strategie mit verbindlich formulierten widerspruchsfreien Zielen zu erarbeiten. Um die Zielerreichung überprüfen zu können, hat es verbindliche und messbare Kennzahlen festzulegen.

Einzelne Rechtsetzungsakte des Innenministeriums bzw. der Landesregierung sowie Gesetzgebungsinitiativen der Landesregierung können keine Strategie ersetzen. Diese muss als erstes entwickelt werden. Aus den Zielen der Strategie muss die Landesregierung den notwendigen regulatorische Handlungsbedarf ab- und die jeweils erforderlichen Rechtsetzungsverfahren einleiten.

3.2 IT-Controlling aufbauen

(46) Der Landesrechnungshof hat bereits im Jahresbericht 2011 kritisiert, dass ein IT-Controlling nicht mehr durchgeführt wird. Er forderte, im damals zuständigen Innenministerium eine ressortübergreifende IT-Steuerung und Koordinierung in einer eigenen Organisationseinheit zu bündeln.[8]

(47) In dem 2011 überarbeiteten Masterplan eGovernment war geplant, das IT-Controlling wieder aufzunehmen.

[8] Vgl. Landesrechnungshof Mecklenburg-Vorpommern (2011): Jahresbericht 2011 (Teil 2) Landesfinanzbericht 2011, S. 73f.

(48) Dies ist bisher nicht geschehen.

(49) Das zuständige Innenministerium sollte

- eine Organisationseinheit für operatives IT-Controlling für den Betrieb der IT im ZDMV und für strategisches IT-Controlling im Innenministerium aufbauen,
- im ZDMV ein IT-Risikomanagementsystem einführen und die Risiken fortlaufend überwachen,
- ein Monitoring und Reportingsystem aufbauen.

(50) Das Innenministerium teilt die Auffassung, dass es eines zentralen IT-Controllings mit den entsprechenden Befugnissen bedürfe. Das Referat 230 im Innenministerium verantworte die Steuerung der Digitalstrategie und führe die Fachaufsicht über das ZDMV (strategisches IT-Controlling). Ein zentrales operatives IT-Controlling für die ressortübergreifenden IT-Services fände bereits zum Teil im ZDMV statt. Dieses solle weiter ausgebaut werden und auch das Risikomonitoring übernehmen. Mit der Übertragung der Aufgaben aus den Ressorts würden weitere Bereiche in das Controlling übernommen. Der zentrale Einzelplan 15 sei die Grundlage der finanziellen Steuerung.

(51) Der Landesrechnungshof begrüßt die Aktivitäten des Innenministeriums.

Das operative IT-Controlling beschränkt sich jedoch nicht nur auf die Überwachung der IT-Ausgaben und die Budgeteinhaltung. Von größerer Bedeutung sind Fragen der Wirtschaftlichkeit, die Leistungsbewertung (Effizienz und Effektivität) und eine zielgerichtete Berichterstattung

Das erforderliche strategische IT-Controlling wird mit der Ausübung der Fachaufsicht über das ZDMV nicht erreicht. Wesentlicher Bestandteil des strategischen IT-Controlling ist die langfristige Planung und Steuerung des Einsatzes von IT. Hierzu sind relevante Informationen zu erheben und zu analysieren. Die Steuerung der Digitalstrategie erfordert operationalisierbare Ziele.

Sowohl beim operativen als auch beim strategischen IT-Controlling besteht noch erhebliches Verbesserungspotenzial, da nicht bei allen durchgeführten Projekten die angestrebten Ziele erreicht wurden. Eine systematische Leistungsbewertung der IT-Systeme und IT-Prozesse findet anscheinend nicht statt. Defizite bestehen auch bei der Planung.

4 Regulative Voraussetzungen für die Digitalisierung der Landesverwaltung und den Einsatz von Informationstechnik

4.1 Rolle der Digitalisierungsabteilung im Innenministerium stärken

(52) Es bedarf einer übergreifenden IT-Steuerung durch eine zentrale Stelle, wie z. B. die Abteilung „Digitale Verwaltung, digitale Infrastruktur und Geoinformation“ im In-

nenministerium. Diese hat darüber hinaus Standards für IT-Architekturen (IT-Systemkomponenten, Datenaustausch und Benutzerschnittstellen) sowie IT-Projektmanagement, IT-Betrieb und IT-Beschaffungen festzulegen.

Die zentrale Stelle muss mit den zur Bewältigung der Aufgaben benötigten Befugnissen ausgestattet sein.

(53) Die bislang vorherrschende Ressortperspektive führt nicht zu aufeinander abgestimmten und wirtschaftlichen IT-Lösungen.

Das Ressortprinzip steht entsprechenden IT-Lösungen nicht entgegen, da es sich lediglich um unterstützende Aufgaben handelt. Die Fachkompetenz der Ressorts wird durch zentrale, fachaufgabenneutrale Vorgaben zum Einsatz von Informationstechnik in der Regel nicht berührt.

Konzepte einer digitalen Verwaltung mit einer einzigen behördlichen Anlaufstelle begegnen keinen grundsätzlichen rechtlichen Bedenken. Entscheidend sind der konzeptionelle Aufbau der Plattform und die Einbindung der jeweils beteiligten Verwaltungsträger.[9]

(54) Die Digitalisierungsabteilung im Innenministerium sollte deutlich stärker zentral steuern. Dabei sollte sie den Rat der IT-Verantwortlichen (RIT) einbeziehen. Zentrale Vorgaben sollten möglichst im Benehmen mit dem oder zumindest nach Beratung durch den RIT erlassen werden. Darüber hinaus muss die Verantwortlichkeit der Fachressorts für ihre Fachaufgaben gewahrt bleiben.

(55) Das Innenministerium sollte prüfen, ob die Kompetenzen für eine zentrale Steuerung im E-Government-Gesetz Mecklenburg-Vorpommern (EGovG M-V) und in den dazu erlassenen Rechtsverordnungen und Verwaltungsvorschriften des Landes ausreichen. Es sollte prüfen, ob und inwieweit der CIO gesetzliche Durchgriffsrechte eingeräumt werden sollten, soweit sich diese nicht auf die Fachaufgaben der Ressorts auswirken.

(56) Das Innenministerium teilte mit, dass es die Empfehlung prüfen werde.

(57) Der Landesrechnungshof begrüßt dies. Das Innenministerium hat keinen Zeitrahmen mitgeteilt. Der Landesrechnungshof geht davon aus, dass das Innenministerium zeitnah prüfen und unmittelbar im Anschluss daran beginnen wird, die Ergebnisse seiner Prüfung umzusetzen.

[9] Heckmann/Paschke, jurisPK-Internetrecht (2025), Rz. 191.

4.2 Gesetzliche Verpflichtung zur Informationssicherheit schaffen

(58) Der Landesrechnungshof hatte im Landesfinanzbericht 2019[10] empfohlen, wesentliche Vorgaben zur Informationssicherheit in einem Informationssicherheitsgesetz zu regeln.

(59) Zudem ist die Richtlinie des Europäischen Parlaments und des Europäischen Rates über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Union (NIS-Richtlinien)[11] aus 2016, geändert 2022 (NIS-2-Richtlinien)[12], bis Oktober 2024 bezüglich der ggf. betroffenen Einrichtungen in Landesrecht umzusetzen. Dies sollte bei der Erarbeitung eines Informationssicherheitsgesetzes im Blick behalten werden.

(60) Die Sicherheitslage in Deutschland wird durch das Bundesamt für die Sicherheit in der Informationstechnik (BSI) als „angespannt bis kritisch" eingeschätzt.[13] Mehrere erfolgreiche Cyberangriffe in jüngster Zeit haben die Handlungsfähigkeit der öffentlichen Verwaltung stark eingeschränkt.[14] Sind von dem Angriff kritische Infrastrukturen betroffen, kann dies Leben und Gesundheit der Bürgerinnen und Bürger gefährden.

(61) Das Energieministerium hatte 2020 mitgeteilt, dass ein Gesetzgebungsverfahren in der 7. Legislaturperiode geplant sei. Das Gesetz sollte Ende 2020 in Kraft treten. Das Innenministerium teilte 2021 mit, dass der Gesetzesentwurf nicht mehr so rechtzeitig in den Landtag eingebracht worden konnte, dass dieser bis zum Ende der Legislaturperiode das Gesetz hätte beschließen können. Ein Gesetzgebungsverfahren sei nunmehr für die 8. Legislaturperiode geplant.[15]

(62) Der Entwurf eines Informationssicherheitsgesetzes liegt noch immer nicht vor.

(63) Damit fehlt eine gesetzliche Regelung der Befugnisse des Beauftragten der Landesverwaltung für Informationssicherheit (BeLVIS) sowie der Kompetenzen des Computer Emergency Response Teams (CERT).

(64) Weiterhin fehlt eine gesetzliche Verpflichtung für die Landesverwaltung, die kommunalen Verwaltungen sowie die sonstigen der Aufsicht des Landes unterstehenden Rechtspersonen des öffentlichen Rechts und die IT-Dienstleister (DVZ M-V GmbH sowie kommunale IT-Dienstleister), Informationssicherheit systematisch und

---

[10] Landesrechnungshof Mecklenburg-Vorpommern (2019): Jahresbericht 2019 (Teil 1) – Landesfinanzbericht 2019, S. 46 ff..

[11] Richtlinie (EU) 2016/1148 des Europäischen Rates und des Europäischen Parlaments vom 6. Juli 2016 über Maßnahmen zur Gewährleistung eines hohen gemeinsamen Sicherheitsniveaus von Netz- und Informationssystemen in der Union.

[12] Richtlinie (EU) 2022/2555 des europäischen Parlaments und des europäischen Rates vom 14. Dezember 2022 über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Union (NIS-2-Richtlinie).

[13] Vgl. Bundesamt für Sicherheit in der Informationstechnik (2023): Die Lage der IT-Sicherheit in Deutschland 2023, S. 9.

[14] Z. B.: Deutscher Bundestag, Kommunalservice Mecklenburg KSM (u. a. Landeshauptstadt Schwerin), Landkreis Anhalt-Bitterfeld, Südwest-IT (72 Kommunen).

[15] Vgl. Landesrechnungshof Mecklenburg-Vorpommern (2022): Jahresbericht 2022 (Teil 1) – Landesfinanzbericht 2022, S. 209.

standardisiert auf der Basis eines anerkannten Informationssicherheitsmanagements umzusetzen. Hierfür bietet sich der in der Landesverwaltung bereits verpflichtende IT-Grundschutz des Bundesamtes für Sicherheit in der Informationstechnik an. Zudem sind ggf. Anforderungen der NIS-2-Richtlinien in der Gesetzgebungszuständigkeit des Landes als Standard für ein hohes Cybersicherheitsniveau zu berücksichtigen.

(65) Für die Landesverwaltung muss die Stellung des BeLVIS im Innenministerium gestärkt werden. Hierzu zählen Kontroll- und Prüfbefugnisse und Weisungsrechte gegenüber dem ZDMV, den Fachbehörden und der DVZ M-V GmbH. Das ZDMV und die anderen Behörden der Landesverwaltung sind zu verpflichten, bei anderen IT-Dienstleistern Kontroll- und Prüfrechte des BeLVIS in den Verträgen zu regeln.

(66) Die Kommunen sollten verpflichtet werden, Beauftragte für die Informationssicherheit zu ernennen. Diese sind mit vergleichbaren Befugnissen auszustatten.

(67) Aufgaben, Rechte und Befugnisse des CERT M-V[16] für die Planung und die Umsetzung von vorbeugenden, reaktiven und nachhaltigen Maßnahmen im Rahmen des Informationssicherheitsmanagements des Landes sollten gesetzlich definiert werden. Es sind datenschutzrechtliche Regelungen zu schaffen, damit das CERT M-V Ursachenanalysen unabhängig von der Einwilligung der von einer möglichen Verarbeitung personenbezogener Daten Betroffenen betreiben kann.

(68) Die Landesverwaltung, die kommunalen Verwaltungen sowie die sonstigen der Aufsicht des Landes unterstehenden Rechtspersonen des öffentlichen Rechts und die IT-Dienstleister im Land (DVZ M-V GmbH, KSM Kommunalservice Mecklenburg AöR, IKT-Ost AöR) sind gesetzlich zu verpflichten, alle Sicherheitsvorfälle an das CERT M-V zu melden.

(69) Das Innenministerium sollte unverzüglich den Entwurf eines Informationssicherheitsgesetzes erarbeiten und ein Gesetzgebungsverfahren einleiten.

(70) Das Innenministerium teilt mit, dass es derzeit den Entwurf eines Informationssicherheitsgesetzes erarbeite. Im März werde die Ressortanhörung durchgeführt. Die Zuleitung an den Landtag sei im September 2025 geplant.

Die Empfehlungen des Landesrechnungshofes werde es überwiegend umsetzen.

Befugnisse des BeLVIS würden im Gesetz geregelt. Im Rahmen der Fachaufsicht verfüge dieser gegenüber dem ZDMV bereits jetzt über Prüfbefugnisse und Weisungsrechte.

Über die Anschlussbedingungen des Landesnetzes (CN LAVINE) bestünden bereits Meldepflichten bei schweren Sicherheitsvorfällen. Die Meldung sämtlicher – d. h. auch geringfügiger – Vorfälle sehe das Innenministerium kritisch.

(71) Der Landesrechnungshof begrüßt die für dieses Jahr geplanten Gesetzgebungsaktivitäten.

[16] Leitlinie zur Gewährleistung der Informationssicherheit in der Landesverwaltung von Mecklenburg-Vorpommern.

Die Verpflichtung zur Meldung von Sicherheitsvorfällen an das CERT sollte gesetzlich normiert werden, auch wenn eine solche Pflicht über die Anschlussbedingungen bereits besteht. Durch die Meldung auch geringfügiger Sicherheitsvorfälle kann das CERT ein übergreifendes Lagebild erstellen. Die Häufung und Verteilung geringfügiger Sicherheitsvorfälle kann auf schwerwiegendere Sicherheitsprobleme hinweisen. Mithilfe automatisierter Meldewege und Analysen kann der Verwaltungsaufwand gering gehalten werden.

4.3 Standardisierung verbessern

4.3.1 IT-Landesstandards offen und produktneutral formulieren

(72) Bereits im Jahresbericht 2011 hatte der Landesrechnungshof kritisiert, dass es an aktuellen Standards und Normen fehlt. Die Standardisierungsrichtlinie hatte das seinerzeit zuständige Innenministerium bereits 2007 außer Kraft gesetzt.[17] Es hatte beabsichtigt, zeitnah neue IT-Landesstandards festzulegen.

Der Landesrechnungshof hatte im Jahresbericht 2019 gefordert, dass das Energieministerium in der IT-Richtlinie verbindliche IT-Landesstandards festlegt.[18]

(73) Das Innenministerium hat im August 2022 IT-Landesstandards erlassen, in denen konkrete Produkte bzw. herstellerspezifische Formate benannt werden.

(74) Dies verstößt gegen die Grundsätze der Offenheit von Standards sowie der Hersteller- und Produktneutralität. Zudem bestehen vergaberechtliche Bedenken. Im Vergaberecht gilt der Grundsatz der Produktneutralität.[19] Die derzeit geltenden IT-Landesstandards können daher nicht als Grundlage für Leistungsbeschreibungen bei öffentlichen Auftragsvergaben herangezogen werden.[20]

Ein Standard setzt voraus, dass die grundlegende Technik durch eine Standardisierungsorganisation als Standard empfohlen wird und sich die Nutzer auf deren Anwendung verbindlich einigen bzw. seine Anwendung verbindlich vorgegeben wird (z. B. durch Beschlüsse des IT-Planungsrats). Ein herstellerspezifisches Format wird allein durch seine verbreitete Nutzung nicht zum Standard.

(75) Anstelle konkreter Produkte sollten die IT-Landesstandards grundsätzlich offene Protokolle, Schnittstellen und Datenformate festlegen. Dies ist unabdingbare Voraussetzung für die Digitalisierung der Landesverwaltung.

---

17 Vgl. Landesrechnungshof Mecklenburg-Vorpommern (2011): Jahresbericht 2011 (Teil 2) – Landesfinanzbericht 2011, S. 70 f.

18 Vgl. Landesrechnungshof Mecklenburg-Vorpommern (2019): Jahresbericht 2019 (Teil 1) – Landesfinanzbericht 2019, S. 49 f.

19 Vgl. § 31 Abs. 2 Vergabeordnung: Leistungsbeschreibung in Form von Leistungs- und Funktionsanforderungen mit Bezug auf Normen und technische Spezifikationen, § 23 Abs. 1 Unterschwellenvergabeordnung: Leistungsbeschreibung durch Funktions- und Leistungsanforderungen.

20 Landesrechnungshof Mecklenburg-Vorpommern 2020: Jahresbericht 2020 (Teil 1) – Landesfinanzbericht 2020, S. 72.

Das gilt insbesondere für die anstehende Erneuerung der Fachverfahren und deren reibungslose Einbindung in vollständig digitale und automatisierte Geschäftsprozesse. Hierzu ist es notwendig, dass Daten und Dokumente mit der aufgrund des Onlinezugangsgesetzes zu schaffenden IT-Infrastruktur (Portal, Bürgerkonto), der elektronischen Akte und anderen Fachverfahren bzw. Registern automatisiert ausgetauscht werden können.

Besonders die Nutzung von Fachlösungen (Einer-für-Alle-Prinzip)[21] erfordert offene Standards.

Die Entwicklung eines standardisierten IT-Arbeitsplatzes und die modulare Einbindung verschiedener Dienste (z. B. E-Mail, Videokonferenz) sowie der Zugriff auf Fachverfahren über diesen Arbeitsplatz erfordern offene Protokolle und Schnittstellen.

(76) Das Innenministerium sollte zeitnah die IT-Landesstandards überarbeiten.

(77) Das Innenministerium teilt mit, dass die IT-Richtlinie unter Berücksichtigung der vom IT-Planungsrat für verbindlich erklärten IT-Standards überarbeitet werde.

Es stimme der Forderung des Landesrechnungshofes grundsätzlich zu, offene Protokolle, Schnittstellen und Datenformate festzulegen. Bestimmte Fachanwendungen nutzten aber proprietäre Datenaustauschformate. Teilweise gäbe es keine Branchen-Standards.

(78) Der Landesrechnungshof begrüßt, dass das Innenministerium die IT-Landesstandards überarbeiten wird. Das Innenministerium sollte die IT-Landesstandards zeitnah überarbeiten.

Grundsätzlich sind öffentliche Aufträge produkt- und herstellerneutral auszuschreiben (vgl. Tz. 74). Wenn das Innenministerium Standards so formuliert, dass dadurch bestimmte Unternehmen oder bestimmte Produkte begünstigt oder ausgeschlossen werden (§ 31 Abs. 6 Vergabeverordnung), muss es im Vorfeld prüfen, ob dies vergaberechtlich zulässig ist.

Das Innenministerium sollte durch die IT-Landesstandards sicherstellen, dass zukünftig bei Vergabeentscheidungen Fachanwendungen, Betriebssysteme und Hardware ausgewählt werden, die möglichst nicht-proprietäre Protokolle, Schnittstellen oder Formate nutzen. Proprietäre Protokolle, Schnittstellen und Datenformate dürfen nicht allein deshalb dauerhaft als Standard festgeschrieben werden, weil aktuell genutzte Fachanwendungen derzeit proprietäre Dateiaustauschformate nutzen.

4.3.2 Landesverordnung über Datenaustauschstandards überarbeiten

(79) Die Landesregierung hat am 7. Januar 2020 die Landesverordnung über Datenaustauschstandards erlassen. Sie ist mit Wirkung vom 16. Januar 2020 in Kraft getreten.

[21] Vgl. IT-Planungsrat: Beschluss Nr. 2022/29 vom 22. August 2022.

(80) In der Rechtsverordnung sollen Datenaustauschformate festgelegt und allgemeine technisch-organisatorische Regelungen zur Kompatibilität der verschiedenen Verfahren geregelt werden, um eine landesweite Weiterverwendbarkeit durch Behörden und Gerichte sicherzustellen.

Die gemäß § 11 Abs. 2 und § 15 Abs. 1 EGovG M-V festzulegenden Standards sollen offen, hersteller- und produktneutral sein[22] und müssen sicherstellen, dass die allgemeinen Grundsätze für IT-Standards (insbesondere Wirtschaftlichkeit, Offenheit, Interoperabilität, Sicherheit) sowie die Grundsätze der Aktenführung (insbesondere Authentizität, Integrität, Vertraulichkeit, Verfügbarkeit, Lesbarkeit, Verkehrsfähigkeit, Revisionssicherheit) eingehalten werden.

(81) Der Landesrechnungshof hatte im Landesfinanzbericht 2020[23] kritisiert, dass Dateiformate aufgenommen wurden, die nicht oder nicht uneingeschränkt offen sowie hersteller- und produktneutral waren. Weiterhin hat der Landesrechnungshof kritisiert, dass nicht alle Standards verpflichtend vorgegeben waren. Zudem werden nicht alle Datenaustauschstandards für die Kommunalverwaltung zur verpflichtenden Anwendung festgeschrieben.

Der BeLVIS hat die Nutzung einiger der vorgegebenen Dateiformate untersagt.

(82) Diese Defizite bestehen weiterhin.

(83) Das Innenministerium sollte zeitnah die Landesverordnung über Datenaustauschstandards überarbeiten.

(84) Das Innenministerium teilt mit, dass es Handlungsbedarfe hinsichtlich der Landesverordnung prüfen werde. Vorgaben des IT-Planungsrats werde es dabei berücksichtigen.

(85) Der Landesrechnungshof begrüßt dies. Das Innenministerium sollte zeitnah prüfen.

Bei der Ausgestaltung der Vorgaben des IT-Planungsrats sollte das Innenministerium grundsätzlich offene Protokolle, Schnittstellen und Formate festlegen.

4.4 Rechtliche Grundlagen für den Landesdienstleister überprüfen

(86) Der Landesrechnungshof hat wiederholt darauf hingewiesen, dass die Regelungen des DVZ-Gesetzes veraltet sind bzw. der geänderten Rechtslage auf Bundesebene nicht entsprechen.[24]

(87) In der damaligen Ermangelung eines Freistellungstatbestandes im Gesetz gegen Wettbewerbsbeschränkungen (GWB) diente das DVZG M-V zum Zeitpunkt seiner Entstehung (2000) u. a. dazu, eine Beauftragung der DVZ M-V GmbH ohne öffentliche

[22] Vgl. Entwurf eines Gesetzes zur Förderung der elektronischen Verwaltungstätigkeit in Mecklenburg-Vorpommern und zur Änderung des Landesverwaltungsverfahrensgesetzes, Drs. 6/4636, S. 49.

[23] Landesrechnungshof Mecklenburg-Vorpommern 2020: Jahresbericht 2020 (Teil 1) – Landesfinanzbericht 2020, S. 70 ff..

[24] Landesrechnungshof Mecklenburg-Vorpommern 2019: Jahresbericht 2019 (Teil 1) – Landesfinanzbericht 2019, S. 51, Jahresbericht 2023 (Teil 1) – Landesfinanzbericht 2023, S. 139 f.

Vergabeverfahren zu ermöglichen. Neuregelungen im GWB in 2016 führten dazu, dass Aufträge im Oberschwellenbereich auch ohne DVZG M-V von der Anwendung des öffentlichen Vergaberechts freigestellt werden können.

(88) Gemäß Anlage A des DVZG M-V beschafft die DVZ M-V GmbH zentral „IuK-Technik" nach dem IT-Strukturrahmen für die Landesverwaltung Mecklenburg-Vorpommern. Der vorliegende IT-Strukturrahmen aus 2005 ist technologisch veraltet. Damit sind bedarfsgerechte Beschaffungen durch die DVZ M-V GmbH derzeit rechtlich nicht abgesichert.

Auch die in Anlage 1 des DVZG aufgeführten Verfahren entsprechen nicht mehr dem tatsächlichen Stand.

(89) Der Landesrechnungshof hatte bereits im Landesfinanzbericht 2019 empfohlen, die DVZ M-V GmbH gesetzlich zur Einhaltung des BSI-Grundschutzes zu verpflichten. Außerdem hatte er empfohlen, Regelungen zur Auftragsverarbeitung in das DVZG M-V aufzunehmen.[25] Im Verwaltungsvollzug könnte dann auf den Abschluss einzelner Auftragsverarbeitungsverträge verzichtet werden. Aufgrund einer Entschließung des Landtages sicherte das damals zuständige Energieministerium zu, dies prüfen zu wollen.[26] Ergebnisse liegen dem Landesrechnungshof nicht vor.

(90) Das Innenministerium sollte das DVZG M-V prüfen und überarbeiten. Das DVZG M-V sollte

- die rechtliche Grundlage für die Beauftragung der DVZ M-V GmbH unter Berücksichtigung der Regelungen des GWB regeln,
- Regelungen aufnehmen, die eine bedarfsgerechte und standardkonforme Beschaffung ermöglichen,
- eine Generalermächtigung und vorrangige Beauftragung der DVZ M-V GmbH für die Verarbeitung personenbezogener und sonstiger zu schützender Daten im landeseigenen Rechenzentrum und Regelungen zur Auftragsverarbeitung enthalten sowie
- die DVZ M-V GmbH gesetzlich auf die Einhaltung des BSI-Grundschutzes verpflichten.

(91) Das Innenministerium teilt mit, dass es die Hinweise bei der Überarbeitung des DVZG M-V berücksichtigen werde.

(92) Der Landesrechnungshof begrüßt dies. Das Innenministerium sollte das DVZG M-V zeitnah überarbeiten und in der Gesetzesbegründung dokumentieren, dass es die Hinweise berücksichtigt hat.

[25] Landesrechnungshof Mecklenburg-Vorpommern 2019: Jahresbericht 2019 (Teil 1) – Landesfinanzbericht 2019, S. 53.

[26] Landesrechnungshof Mecklenburg-Vorpommern 2020: Jahresbericht 2020 (Teil 1) – Landesfinanzbericht 2020, S. 253 ff.

4.5 Landesrechtliche Hemmnisse für die Digitalisierung beseitigen

(93) Gesetzentwürfe der Landesregierung werden nur unzureichend auf ihre Digitalisierungsfähigkeit überprüft. Bei untergesetzlichen Normen spielt die Digitalisierungsfähigkeit bisher gar keine Rolle. Rechtliche Regelungen sind häufig so gestaltet, dass komplexe Verwaltungsprozesse eine Digitalisierung hemmen (Digitalisierungshemmnisse).

(94) Gesetzentwürfe sind auf ihre digitale Vollziehbarkeit, Machbarkeit und digitale Sinnhaftigkeit zu prüfen (Digital-Check).[27] Das Gleiche gilt auch für untergesetzliche Normen. Verwaltungsvorschriften und Richtlinien gestalten wesentlich die Verwaltungsverfahren und die Aufgabenwahrnehmung.

(95) Um die Digitalisierungsfähigkeit landesrechtlicher Regelungen sicherzustellen, sollten insbesondere

- Schriftformerfordernisse vermieden bzw. – wenn nicht gänzlich vermeidbar – die Möglichkeit vorgesehen werden, die Schriftform durch elektronische Alternativen zu ersetzen,
- elektronische Kommunikation und elektronischer Datenaustausch ermöglicht werden, idealerweise über bestehende Plattformen (z. B. MV-Serviceportal),
- Regeln und Prozesse vereinfacht sowie klar und eindeutig formuliert und die Notwendigkeit von Ermessensregeln geprüft werden (automatisierbare Entscheidungsstrukturen),
- Entscheidungsregeln visualisiert werden (Rule Mapping),
- Rechtsbegriffe möglichst vereinheitlicht und maschinentauglich anhand prüfbarer Kriterien und Beziehungen zu anderen Begriffen verwendet werden,
- vorrangig automatisierte Datenabrufe aus Registern und Fachverfahren (once-only- Prinzip) vorgesehen werden,
- Prozesse, Schnittstellen und Datenmodelle bereits bei der Normsetzung entworfen und möglichst hinsichtlich (teil)automatisierter Verarbeitung optimiert werden,
- Voraussetzungen für Dunkelverarbeitung einschließlich risikobasierter Stichprobenprüfungen geschaffen werden.

(96) Die Entwürfe landesrechtlicher Regelungen sind durch die jeweils zuständige oberste Landesbehörde auf ihre Digitalisierungsfähigkeit zu prüfen. Bei Gesetzen und Verordnungen sollte das Ergebnis der Prüfung in die Begründung aufgenommen werden. Die Regelungen in der GGO II sollten entsprechend angepasst werden.

(97) Bestehende landesrechtliche Regelungen sollten durch die jeweils zuständige oberste Landesbehörde auf bestehende Digitalisierungshemmnisse geprüft werden. Erkannte Defizite sollten umgehend beseitigt werden.

[27] Vgl. Nationales E-Government Kompetenzzentrum e. V.: Digitalscheck im Gesetzgebungsverfahren. NEGZ Kurzstudie Nr. 26, 2022.

(98) Das Innenministerium teilt mit, dass es aktuell einen Formulierungsvorschlag für die Einführung eines Digital-Checks in der GGO II erarbeite. Dabei werde es die Hinweise des Landesrechnungshofes berücksichtigen.

(99) Der Landesrechnungshof begrüßt dies. Die Landesregierung sollte zeitnah eine entsprechende Regelung in die GGO II aufnehmen.

5 Organisatorische Voraussetzungen für die Digitalisierung der Landesverwaltung und den Einsatz von Informationstechnik

5.1 Defizite in der Aufbauorganisation der Digitalisierungsabteilung des Innenministeriums abbauen

(100) Mit der Abteilung „Digitale Verwaltung; digitale Infrastruktur und Geoinformation“ wurde innerhalb des Ministerium eine eigene Organisationseinheit geschaffen, die überwiegend für die Digitalisierung zuständig ist. Neben den mit Digitalisierungsaufgaben beauftragten Referaten sind zusätzlich die dem Minister zugeordneten „*Stabsstelle Digitaler Wandel*“ und „*CIO Stabsstelle E-Government*“ für Digitalisierungsfragen zuständig.

(101) Der Landesrechnungshof hatte 2019 die Organisation der Digitalisierungsabteilung im damaligen Energieministerium geprüft. Er kritisierte, dass das Ministerium organisatorische Pflichtaufgaben wie Aufgabenkritik, Geschäftsprozessoptimierung und Personalbedarfsermittlung nicht wahrgenommen hat.[28]

(102) Die Digitalisierungsabteilung des ehemaligen Energieministeriums wurde 2022 in das Innenministerium überführt. Dort wurde sie ohne organisatorische Prüfung in bereits bestehende Strukturen eingebettet.

(103) Das Innenministerium sollte eine Aufgabenkritik, Geschäftsprozessoptimierungen und Personalbedarfsermittlungen für die übernommenen Aufgaben durchführen.

(104) Das Innenministerium teilt mit, dass die Aufgaben im Bereich Digitalisierung ganz bewusst in verschiedenen Einheiten organisiert worden seien. Explizit sei entschieden worden, dass die Digitalisierung der Verwaltung vor allem mit dem Bereich des allgemeinen Verwaltungsrechts in einer Abteilung zusammengeführt werden sollte. Es sollte die Illusion aufgelöst werden, es gäbe eine digitale Verwaltung neben einer „analogen“ Verwaltung.

Die Stabsstelle Digitaler Wandel sei mit von diesen Bereichen unabhängigen Aufgaben betraut (digitale Transformation der Gesellschaft). Die CIO-Stabsstelle diene der Staatssekretärin als Unterstützung bei der Steuerung, der Vorbereitung von Terminen und der Unterstützung bei der strategischen Ausrichtung.

[28] Landesrechnungshof Mecklenburg-Vorpommern 2021: Jahresbericht 2021 (Teil 1) – Landesfinanzbericht 2021, S. 130 f.

Aufgabenkritik, Geschäftsprozessoptimierung und Personalbedarfsermittlung würden als kontinuierliche Aufgaben regelmäßig von den Führungskräften erledigt. So hätten diese beispielsweise Vorschläge für die Organisation des ZDMV erarbeitet, um das Ministerium von operativen Aufgaben zu entlasten.

(105) Der Landesrechnungshof weist darauf hin, dass die Digitalisierung lediglich Werkzeuge für das Verwaltungshandeln bereitstellt.

Die Landesregierung sollte die Organisation der Digitalisierungsabteilung überprüfen. Die Aufgaben und Zuständigkeiten für die Digitalisierung der Verwaltung sollten soweit als möglich gebündelt werden.

Für die dafür erforderlichen Arbeitsschritte wie Aufgabenkritik, Geschäftsprozessoptimierung und Personalbedarfsberechnungen ist ist das Organisationsreferat des Innenministeriums verantwortlich. Diese Aufgabe lässt sich nicht auf IT-Führungskräfte in der Digitalisierungsabteilung delegieren.

5.2 Rat der IT-Verantwortlichen stärken

(106) Der RIT ist ein Gremium der obersten Landesbehörden. Er stimmt die informationstechnischen Vorhaben der Geschäftsbereiche mit der für ressortübergreifende IT-Angelegenheiten zuständigen obersten Landesbehörde ab.[29] Außerdem berät er das Innenministerium

- zu IT-Standards sowie Regelungen zur Nutzung von IT,
- bei der Überwachung von Kennzahlen zur Umsetzung der Standards,
- bei der einheitlichen Weiterentwicklung der E-Government- und IT-Strategie des Landes,
- über Anforderungen an die landesweite Weiterentwicklung der IT-Infrastruktur und der Servicelevel
- sowie bei der Weiterentwicklung der Leistungsangebote der DVZ M-V GmbH für die Landesverwaltung. [30]

Es können demnach nur Vertreterinnen und Vertreter der obersten Landesbehörden miteinander interagieren. Da das EGovG M-V der Staatssekretärin des Innenministeriums in ihrer Funktion als CIO die ressortübergreifende Koordinierung zuweist, handelt es sich auch um eine ausdrückliche Fachaufgabe des Innenministeriums.[31]

(107) Das Innenministerium hat die ihm als oberste Landesbehörde zugewiesenen Aufgaben wahrzunehmen. Dazu gehört der Vorsitz im RIT. Das ZDMV kann beratend an den Sitzungen des RIT teilnehmen, sofern die IT-Richtlinie dahingehend angepasst wird. Es kann das Innenministerium bei seiner Aufgabenwahrnehmung unterstützen.

(108) 2023 tagte der RIT nur sehr unregelmäßig. Die Sitzungen wurden kurzfristig, teilweise erst am Sitzungstag und ohne Begründung abgesagt. Die Protokolle zu den

[29] Vgl. § 16 Abs. 4 EGovG M-V.

[30] Vgl. Nr. 3.4 IT-Richtlinie der Behörden der Landesverwaltung Mecklenburg-Vorpommern (IT-Richtlinie – ITRL M-V) vom 1. September 2021.

[31] Vgl. § 16 Abs. 3 EGovG M-V.

Sitzungen werden seit August 2022 nicht mehr im Intranet der Landesverwaltung veröffentlicht. Inzwischen ist im Intranet der Landesverwaltung kein eigenes Informationsangebot des RIT mehr vorhanden. Die IT-Richtlinie ist nicht mehr veröffentlicht. Regelungen zur Geschäftsordnung sind ebenfalls nicht veröffentlicht.

(109) Der RIT sollte unter Vorsitz des Innenministeriums wieder regelmäßig tagen und die Protokolle im Intranet der Landesverwaltung veröffentlichen. Ebenso sollten die IT-Richtlinie sowie Regelungen zur Geschäftsordnung des RIT im Intranet veröffentlicht werden. Auch weitere Informationen zum ressortübergreifenden Einsatz von IT und zur Digitalisierung der Landesverwaltung sollten über das Intranet der Landesverwaltung zur Verfügung gestellt werden.

(110) Im Zeichen der Digitalisierung der Verwaltung sind IT und Organisation zwei Seiten derselben Medaille. Es bedarf einer engen Abstimmung der Zuständigen für IT und Organisation. Die Arbeit des RIT sollte daher stärker mit dem Ausschuss für Organisationsfragen (AfO) verzahnt werden. Der Vorsitzende des AfO sollte mit Rederecht regelmäßig an den Sitzungen des RIT teilnehmen und der Vorsitzende des RIT umgekehrt an denen des AfO.

(111) Das Innenministerium verweist darauf, dass der RIT seine Grundlage in der IT-Richtlinie und nicht im EGovG M-V habe. Nach der IT-Richtlinie gehörten nicht nur IT-Verantwortliche der obersten Landesbehörden, sondern auch IT-Verantwortliche anderer Behörden dem RIT an. Der RIT habe eine beratende Funktion.

(112) Der Landesrechnungshof teilt diese Sichtweise nur zum Teil. Der RIT als solcher ist durch die IT-Richtlinie eingerichtet und näher ausgestaltet. Seine Einrichtung beruht aber auf dem gesetzlich normierten Abstimmungsgebot gem. § 16 Abs. 4 EGovG M-V. Demnach stimmen die obersten Landesbehörden die informationstechnischen Vorgaben ihrer Geschäftsbereiche mit der für ressortübergreifende IT-Angelegenheiten zuständigen obersten Landesbehörde (Innenministerium) ab. Demzufolge können auch nur die Vertreter der obersten Landesbehörden stimmberechtigte Mitglieder im RIT sein.

Obere und untere Landesbehörden unterstehen gem. § 15 Abs. 1 LOG M-V der Dienst- und Fachaufsicht. Daraus folgt, dass nachgeordnete Behörden kein von ihrer obersten Landesbehörde abweichendes Votum abgeben können. Es spricht aber nichts gegen eine beratende Teilnahme der Vertreter nachgeordneter Behörden, insbesondere wenn diese z. B. bei Fachverfahren ihre Expertise einbringen.

Gem. § 16 Abs. 4 EGovG M-V besteht eine Abstimmungspflicht. Eine gegenseitige Abstimmung in Form einer Konsensfindung geht entgegen der Auffassung des Innenministeriums über eine Beratungsfunktion hinaus.

(113) Das Innenministerium teilt die Auffassung des Landesrechnungshofes, dass der Vorsitz des RIT beim Innenministerium liege und das ZDMV den Vorsitz unterstützen könne. Es werde das ZDMV in der IT-Richtlinie als Mitglied benennen.

(114) Der Landesrechnungshof begrüßt, dass das Innenministerium seinen Ausführungen zum Vorsitz folgt. Er begrüßt weiterhin, dass das ZDMV formal als Mitglied in

der IT-Richtlinie benannt werden soll. Aufgrund der umfassenden Zuständigkeit des ZDMV ist eine beratende Teilnahme zweckmäßig.

Das ZDMV kann aber nicht die Belange des Innenministeriums als oberste Landesbehörde als stimmberechtigtes Mitglied im RIT vertreten (vgl. Tz. 112).

(115) Weiterhin teilt das Innenministerium mit, dass es die IT-Richtlinie und die Geschäftsordnung des RIT überarbeiten werde. Die Funktion und Arbeitsweise des RIT sowie dessen Verzahnung mit dem AfO werde es anhand der Vorgaben und Ziele des ZDMVG überprüfen.

Eine geeignete Form der Veröffentlichung der Ergebnisprotokolle werde geprüft. Die Veröffentlichung sei abhängig von der Klassifizierung gemäß Traffic Light Protocol (TLP).

(116) Der Landesrechnungshof begrüßt, dass das Innenministerium die IT-Richtlinie und die Geschäftsordnung des RIT überarbeiten wird.

Das TLP ist zwar in IT-Kreisen gebräuchlich, jedoch in der Landesverwaltung nicht normiert. Über das normale Dienstgeheimnis hinausgehende Schutzbedarfe werden als Verschlusssache gewährleistet. Hierzu existieren normierte Verfahrensweisen und Verhaltensregeln (§ 32 GGO I, Verschlusssachenanweisung für das Land Mecklenburg-Vorpommern). Wenn eine Beschränkung auf „*Kenntnis nur wenn nötig*“ (TLP:Amber) notwendig ist, empfiehlt der Landesrechnungshof eine Klassifikation als „*VS - Nur für den Dienstgebrauch*“. Eine Veröffentlichung z. B. im Intranet ist dadurch ausgeschlossen. Im Übrigen ist es auch nicht zweckmäßig, zwei unterschiedliche Systeme zur Klassifikation vertraulicher Informationen in der Landesverwaltung anzuwenden.

5.3 Defizite beim Aufbau des Landesamts „Zentrum für Digitalisierung Mecklenburg-Vorpommern – ZDMV“ beseitigen

5.3.1 Gesetzliche Aufgaben zwischen ZDMV und Fachbehörden abgrenzen

(117) Das Gesetzgebungsverfahren zum Errichtungsgesetz des ZDMV[32] (ZDMVG) hat der Landesrechnungshof umfangreich mit Stellungnahmen begleitet.

(118) Insbesondere kritisierte der Landesrechnungshof eine unzureichende Abgrenzung bei der Aufgabe „Entwicklung und Pflege der fachbezogenen IT-Services“. Die Verantwortung für die sich aus dem Fachgesetz ergebenden Anforderungen an das Fachverfahren, die Fachprozesse und die Strukturen, innerhalb derer die Fachaufgaben wahrgenommen werden, sollte beim Fachministerium verbleiben.

Das ZDMVG sieht eine geteilte Fachaufsicht vor.[33] Die Fachaufsicht der fachlich zuständigen obersten Landesbehörde soll erst greifen, wenn das ZDMV fachbezogene

[32] Vgl. Drs. 8/1346 vom 21. September 2022.

[33] Vgl. § 4 Abs. 2 ZDMVG.

IT-Services bereitgestellt bzw. entwickelt hat. Auch die Pflege der fachlichen IT-Services soll nicht der Fachaufsicht der fachlich zuständigen obersten Landesbehörde unterliegen. Damit entfällt ein wesentlicher Bereich der Verantwortung aus der Zuständigkeit der Fachaufsicht der fachlich zuständigen obersten Landesbehörde und geht in die Zuständigkeit des ZDMV über.

(119) Dies verstößt gegen das verfassungsrechtlich verankerte Ressortprinzip. Dazu zählt auch die Verantwortung des Fachministers, dafür Sorge zu tragen, dass die eingesetzten Fachverfahren eine ordnungsgemäße und rechtmäßige Aufgabenerfüllung ermöglichen.

Die Aufgaben des ZDMV sind darauf zu konzentrieren, einheitliche Vorgaben für Fachverfahrensarchitekturen festzulegen und auf eine technologische Konsolidierung der Fachverfahren hinzuwirken. Weiterhin sollte es dafür zuständig sein, die für den Betrieb von Fachverfahren notwendigen Infrastrukturen zu betreiben und interoperable Standards festzulegen. Dies verstößt nicht gegen das Ressortprinzip, da dadurch die Wahrnehmung der Fachaufgaben nicht beeinflusst wird.

(120) Darüber hinaus hält der Landesrechnungshof die Begriffsdefinitionen im ZDMVG nicht für geeignet, die Aufgaben zwischen ZDMV und Fachbehörde eindeutig abzugrenzen. So lässt sich z. B. aus der Definition des Begriffs „IT-Portfoliomanagement“ als das „Ziel, innerhalb der Landesverwaltung eine optimale Mischung aus IT-Projekten und IT-Services zur Erreichung der Ziele zu schaffen“ nicht herleiten, welche Aufgaben das ZDMV in Abgrenzung zur Fachbehörde konkret wahrnehmen soll.

(121) Die diesbezüglichen Stellungnahmen des Landesrechnungshofes im Gesetzgebungsverfahren hat das Innenministerium weitgehend nicht berücksichtigt.

(122) Das Innenministerium sollte die Aufgaben des ZDMV bei einer Modifikation des ZDMVG deutlicher definieren und abgrenzen.

(123) Das Innenministerium teilt mit, dass der Prozess zur Aufnahme neuer Anforderungen im Anforderungsmanagement im ZDMV standardisiert sei. Die Verantwortung für die Formulierung von Anforderungen obliege weiterhin dem Fachressort als Bedarfsträger. Das ZDMV werde auf Anforderung des Fachressorts tätig. Die Verantwortung für die Umsetzung der durch die Bedarfsträger formulierten Anforderungen obliege dem ZDMV.

Die geteilte Fachaufsicht verstoße nicht gegen das Ressortprinzip. Die Wahrung des Ressortprinzips sei bereits im Gesetzgebungsverfahren geprüft worden.

(124) Der Landesrechnungshof begrüßt, dass die Formulierung von Anforderungen weiterhin dem Fachressort als Bedarfsträger obliegt.

Probleme treten dann auf, wenn das ZDMV bei der Umsetzung der vom Bedarfsträger formulierten fachlichen Anforderungen von diesen abweichen will. Zwar kann die fachlich zuständige oberste Landesbehörde gem. § 4 Abs. 2 ZDMVG fachaufsichtlich gegen das ZDMV vorgehen, z. B. durch Weisung. Jedoch kann sie dies nur im Einvernehmen mit der CIO und der für die Digitalisierung in der Verwaltung zuständigen obersten Landesbehörde tun. Dies beschränkt sie in ihrer Fachaufgabenwahrnehmung und damit in ihrer Ressorthoheit.

Der Landesrechnungshof hatte bereits in den Ressort- und Verbandsanhörungen zum Entwurf des ZDMVG auf Probleme bei der Abgrenzung der Verantwortlichkeit im Bereich Fachverfahren hingewiesen.

5.3.2 Stellenplan für ZDMV einrichten

(125) Voraussetzung für den Stellenplan einer Behörde ist der Nachweis der Notwendigkeit der Stellen nach Anzahl und Wertigkeit. Dies setzt voraus, dass auf der Basis eines Aufgabenkatalogs und einer optimierten Aufbau- und Ablauforganisation der Stellenbedarf analytisch festgestellt wird.[34]

(126) Dies ist bisher nicht geschehen.

(127) Im Einzelplan 15 des Haushaltsplans 2024/2025 existiert ein Abschnitt mit der Bezeichnung „Stellenplan und Stellenübersichten“[35], jedoch fehlen in diesem Abschnitt alle Planansätze (Anzahl, Wertigkeit). Stellen und Stellenanteile sollen gemäß § 50 LHO umgesetzt werden. 15 Stellen im Kapitel des Ministeriums (0401) können zugunsten des ZDMV doppelt besetzt werden (§ 8 Abs. 6 Nr. 16 HHG 2024/25).

(128) Das ZDMV hat ein internes Dokument zur Personalplanung erstellt. Dieses stellt die Struktur der Behörde samt der Wertigkeit fast aller dargestellten Stellen mit Stand 5. Januar 2024 dar. Einen vollständigen Überblick gibt es jedoch nicht, da dieses Dokument die zwischenzeitlichen organisatorischen Veränderungen im ZDMV nicht berücksichtigt.

(129) Seit der Errichtung des ZDMV zum 1. Januar 2023 wurden keine Stellenbedarfe für die neue Behörde ausgewiesen. Die eingeräumten Doppelbesetzungsmöglichkeiten können nicht nachvollzogen werden. Sie verstoßen gegen die Haushaltsgrundsätze der Wahrheit und Klarheit.

(130) Bereits in der Stellungnahme zu den Beratungen des Entwurfs des Haushaltsgesetzes 2024/2025 und des Haushaltsbegleitgesetzes 2024/2025 hatte der Landesrechnungshof kritisiert, dass der Stellenplan des ZDMV nicht im Einzelplan des Ministeriums ausgewiesen ist.

(131) Die Gliederung des Haushaltsplans in Einzelpläne folgt gem. Nr. 3.1 Haushaltstechnische Richtlinien grundsätzlich dem Ressortprinzip (institutionelle Gliederung). Ausnahmsweise können Einnahmen und Ausgaben, die fachlich einem einzelnen Verwaltungszweig nicht zuzurechnen sind, in einem Einzelplan zusammengefasst werden (funktionelle Gliederung). Demzufolge können die Ausgaben für Informationstechnik zentral im Einzelplan 15 veranschlagt werden. Die Einnahmen und Ausgaben des ZDMV als nachgeordnete Behörde des Innenministeriums sind hingegen im Epl. 04 zu veranschlagen. Andernfalls wird das Ressortprinzip durchbrochen. Demzufolge ist auch der Stellenplan des ZDMV im Einzelplan 04 zu veranschlagen.

(132) Der Haushalt und der Stellenplan des ZDMV sind ab dem Doppelhaushalt 2026/2027 als Kapitel im Einzelplan des Innenministeriums (Epl. 04) auszubringen.

[34] Vgl. Landesrechnungshof Mecklenburg-Vorpommern 2022: Jahresbericht 2022 (Teil 1) – Landesfinanzbericht 2022, S. 196 ff.

[35] Vgl. Haushaltsplan Mecklenburg-Vorpommern, Haushaltsjahr 2024/2025, Einzelplan 15, S. 151 ff.

Der Stellenbedarf des ZDMV ist analytisch auf der Basis eines Aufgabenkatalogs (Aufgabenkritik) und optimierter Geschäftsprozesse zu ermitteln. Planstellen und andere als Planstellen sind im notwendigen und begründeten Umfang im kommenden Haushaltsaufstellungsverfahren zu beantragen.

(133) Das Innenministerium führt aus, dass es vom Haushaltsgesetz ermächtigt sei, bis zu 15 Doppelbesetzungen in Anspruch zu nehmen, um den Aufbau der Behörde zu unterstützen.

(134) Der Landesrechnungshof hat die Ausgestaltung der Doppelbesetzungsmöglichkeiten bereits im Landesfinanzbericht 2024 kritisiert:

- die Regelung ist zu pauschal,
- Doppelbesetzungsmöglichkeiten sollten in ihrer Wertigkeit definiert werden,
- der anvisierte Zeitraum erscheint zu lang,
- die Anzahl der Doppelbesetzungsmöglichkeiten sollte sich um den Anteil an Stellen vermindern, der mit dem Aufgabenübergang übertragen wird – einschließlich Leitung und allgemeine Verwaltung.[36]

(135) Der Landesrechnungshof hält für erforderlich, die Personalbedarfe des ZDMV analytisch zu ermitteln, die Stellen und Dienstposten zu bewerten und den Stellenbedarf in einem Stellenplan auszuweisen.

(136) Das Innenministerium vertritt die Auffassung, dass Einnahmen und Ausgaben, die keinem konkreten Verwaltungszweig zuzuordnen seien, in einem eigenen Einzelplan zusammengeführt werden können (Ziffer 3.1 Haushaltstechnische Richtlinien). Der Einzelplan 15 sei analog zum Einzelplan 12 eingeführt worden, um eine Gesamtsteuerung aller Einnahmen und Ausgaben nebst Personalbedarfen in Verbindung mit der Digitalisierung der Landesverwaltung zu ermöglichen. Dies sei auch notwendig für das von Landtag und Landesrechnungshof erwartete Controlling.

(137) Der Landesrechnungshof bleibt bei seiner Auffassung, dass die Veranschlagung des Sach- und Personalhaushalts der Behörde ZDMV im funktionalen Einzelplan dem Ressortprinzip nicht entspricht.

Ziffer 3.1 Haushaltstechnische Richtlinien lässt nur eine Zusammenfassung fachlich bedingter Ausgaben zu. Der Verweis auf Einzelplan 12 geht fehl, da dort gerade keine Sach- und Personalausgaben der Bauverwaltung veranschlagt sind.

Das Controlling wird nicht innerhalb des Haushaltsplans oder der Haushaltsrechnung durchgeführt. Eine Anwendung zum Controlling kann ihre Daten aus dem Behördenkapitel ZDMV im Einzelplan des Innenministeriums und dem funktionalen Einzelplan 15 beziehen.

[36] Vgl. Landesrechnungshof Mecklenburg-Vorpommern (2024): Jahresbericht 2024 (Teil 1) – Landesfinanzbericht 2024, S. 29.

5.3.3 ZDMV mit notwendigem Personal ausstatten

(138) Das ZDMV wurde am 1. Januar 2023 gegründet.[37] Der Geschäftsverteilungsplan des ZDMV vom 1. März 2024 umfasste insgesamt 139 Dienstposten mit ihrer organisatorischen Zuordnung. 82 % aller im ZDMV ausgewiesenen Dienstposten waren unbesetzt.

(139) Das Innenministerium führt aus, dass sich der Personalbedarf nur auf den bis dahin verantworteten Aufgabenumfang beziehen könne. Der in Bezug gesetzte Geschäftsverteilungsplan des ZDMV entspreche weder einem Stellenplan noch den bisher umgesetzten Stellen nach § 50 LHO. Es handele sich vielmehr um ein Zielbild des ZDMV. Die dort genannten Aufgaben seien noch nicht vollständig an das ZDMV übertragen worden.

(140) Der Landesrechnungshof erkennt an, dass der personelle Aufwuchs im ZDMV verbunden ist mit der schrittweisen Übertragung von Aufgaben und Stellen.

Es fehlt jedoch ein verbindlicher Stellenplan und ein damit korrespondierender Geschäftsverteilungsplan. Das „*Zielbild des ZDMV*" kann den auf einen haushaltsrechtlich genehmigten Stellenplan basierenden Geschäftsverteilungsplan nicht ersetzen.

Aber auch als *„Zielbild"* ist das vorgelegte Dokument nicht geeignet. Als solches müsste es ausweisen, welche Besetzungsgrade mit welcher Ausbaustufe das ZDMV zu bestimmten Zeitpunkten erreicht hat bzw. erreichen soll. Andernfalls kann das ZDMV im Rahmen der Organisationssteuerung nicht feststellen, ob seine Handlungsfähigkeit erreicht ist.

(141) Auf Bitten des Landesrechnungshofes im Abschlussgespräch am 27. Januar 2025 hat das Innenministerium aktualisierte Zahlen mit Stand vom 28. Februar 2025 vorgelegt. Statt der im März 2024 ausgewiesenen 139 Dienstposten weist das ZDMV nun 55 Dienstposten aus. Hierbei handele es sich um die haushaltsrechtlich möglichen Besetzungen der Dienstposten (z. B. aufgrund von Doppelbesetzungsmöglichkeiten und Umsetzungen gem. § 50 LHO). Für die 55 Dienstposten wesit das ZDMV nut eine Besetzung von rechnerisch rd. 84 % aus.

(142) In Ermangelung eines Stellenplans kann der Landesrechnungshof die haushaltsrechtliche Ermächtigung für das zum Stand 28. Februar 2025 ausgewiesene Soll von 55 Dienstposten nicht nachvollziehen. Damit kann auch nicht nachgewiesen werden, ob und inwieweit die Ist-Besetzung auf einer haushaltsrechtlichen Ermächtigung beruht.

(143) Das ZDMV hat die haushaltsrechtliche Ermächtigung für die Besetzung der Dienstposten transparent nachzuweisen.

(144) Wird von einem haushaltsrechtlich zulässigen Stellenplan von 55 Stellen ausgegangen, bestünde eine personelle Deckungslücke von rd. 16 %. Zum ZDMV gehört das CERT. Im für die IT-Sicherheit wichtigen CERT sind sogar drei von vier Stellen (75 %) nicht besetzt.

[37] Vgl. Ministerium für Inneres, Bau und Digitalisierung (2022): Pressemitteilung vom 7. Dezember 2022: Landtag gibt grünes Licht: Zentrum für Digitalisierung kann kommen, www.regierung-mv.de/Landesregierung/im/Aktuell/?id=186503&processor=processor.sa.pressemitteilung.

(145) Die personelle Unterbesetzung gefährdet die Arbeitsfähigkeit des ZDMV und hat damit unmittelbare Auswirkungen auf den Einsatz von Informationstechnik in der Landesverwaltung. Die bestehende Unterbesetzung im CERT gefährdet darüber hinaus die Informationssicherheit und damit die Arbeitsfähigkeit der gesamten Landesverwaltung.

(146) Das ZDMV hat die personelle Deckungslücke zeitnah zu schließen. Es hat die Stellen im CERT unverzüglich zu besetzen.

5.4 Aufgabenverteilung prüfen und Komplexität reduzieren

5.4.1 Komplexe Organisationsstruktur

(147) Im Innenministerium übernimmt die CIO übergreifende Aufgaben beim Einsatz von IT in der Landesverwaltung.

Die Abteilung „Digitale Verwaltung, digitale Infrastruktur und Geoinformation“ befasst sich u. a. mit der Digitalisierung der Landesverwaltung.

(148) Die DVZ M-V GmbH wurde 2000 mit dem Datenverarbeitungszentrumsgesetz (DVZG M-V) als eine vom Land Mecklenburg-Vorpommern beherrschte juristische Person des Privatrechts errichtet. Sie dient der Unterstützung öffentlicher Aufgaben der Landesverwaltung.[38] Hierzu gehören insbesondere der Betrieb des Landesrechenzentrums, der Betrieb von Fachverfahren, die Beschaffung von Standardhard- und -software. Weiterhin bietet die DVZ M-V GmbH verschiedene Dienstleistungen an, wie z. B. das Erstellen von Sicherheitskonzeptionen, Fortbildung und Beratung. Sie bietet auch Geschäftsprozessoptimierung in den Behörden der Landesverwaltung an.

(149) Zum 1. Januar 2023 wurde das ZDMV als nachgeordnete Behörde des Innenministeriums gegründet u. a. mit der Aufgabe, zentrale und fachbezogene IT-Services bereitzustellen sowie IT-Dienstleister zu beauftragen.

(150) Fachministerien und Fachbehörden beschäftigten sichweiterhin mit Fragen des IT-Einsatzes, weil diese Aufgabe bisher nicht an das ZDMV übergegangen ist bzw. weil sie vom ZDMVG ausgenommen sind (z. B. Justizministerium). Auch nach dem Übergang von Aufgaben an das ZDMV bleiben sie zuständig, indem sie die fachlichen Anforderungen an den IT-Einsatz definieren und Informationssicherheit und Datenschutz sicherstellen müssen.

(151) Das Landesamt für innere Verwaltung (LAiV) ist zuständig für zentrale Beschaffungen. Dazu zählen auch Hard- und Software, die nicht als Standardprodukte über die DVZ M-V GmbH beschafft werden.

(152) Damit ist im Aufgabengebiet der IT mit der Digitalisierungsabteilung, der DVZ M-V GmbH, dem ZDMV, bestimmten Aufgabenbereichen des LAiV sowie den

[38] Vgl. Landtag Mecklenburg-Vorpommern (2000), Drs 3/1381, S. 9.

IT-Stellen der Fachministerien eine komplexe und nicht überschneidungsfreie Organisationsstruktur mit entsprechend komplexen Prozessen entstanden.

5.4.2 Aufgabenverteilung zwischen ZDMV und DVZ M-V GmbH prüfen

(153) Derzeit verursacht das System aus Fachressorts (fachliche Instanz), ZDMV (vermittelnde Instanz) und DVZ M-V GmbH (ausführende Instanz) hohe Transaktionskosten.

So müssen sowohl das ZDMV als auch die DVZ M-V GmbH ein Vertragsmanagement und -controlling betreiben. Beide beschäftigen Vertragsmanager.

Das ZDMV schließt mit der DVZ M-V GmbH Verträge. In bestimmten Fällen, lässt die DVZ M-V GmbH Leistungen vollständig durch Dritte erbringen. In diesen Fällen schließt sie mit dem Dritten einen Vertrag über die selbe Leistung.

(154) Auf die Leistungen der DVZ M-V GmbH wird wegen der gewählten Rechtsform Umsatzsteuer fällig. Die DVZ M-V GmbH kalkuliert außerdem bei den Selbstkostenpreisen für selbst erbrachte Leistungen einen kalkulatorischen Gewinn von 5 %. Zudem erhebt die DVZ M-V GmbH eine Beschaffungspauschale von 5 %. Damit ergeben sich um bis zu 10 % höhere Nettopreise zzgl. Umsatzsteuer im Vergleich zu den Ausgaben die entstehen würden, wenn eine Behörde diese Leistungen erbrächte anstelle der DVZ M-V GmbH.

(155) Die DVZ M-V GmbH ist nicht Teil der Landesverwaltung. Im Hinblick auf Datenschutz und Informationssicherheit ist sie als externer Dritter zu betrachten. Die Funktion des Landes als alleiniger Gesellschafter spielt für die Anforderungen des Datenschutzes und der Informationssicherheit keine Rolle.

Dies bedeutet, dass für alle Leistungen der DVZ M-V GmbH, bei denen personenbezogene Daten verarbeitet werden, datenschutzrechtliche Auftragsverarbeitungsverträge geschlossen werden müssen.

Bezüglich des Informationssicherheitsmanagements müssen die Behörden und Gerichte den Baustein OPS 2.3 „Nutzung von Outsourcing“ des BSI-Grundschutzkompendiums bearbeiten und die Ergebnisse dokumentieren. Umgekehrt muss die DVZ M-V GmbH den Baustein OPS 3.2 „Anbieten von Outsourcing“ bearbeiten und die Ergebnisse dokumentieren.

(156) Würden diese Leistungen innerhalb der Landesverwaltung erbracht, könnte dieser Mehraufwand entfallen.

(157) Mit dem ZDMV existiert bereits eine nachgeordnete Behörde des Innenministeriums. Der Betrieb von Fachverfahren und des Landesrechenzentrums könnte in das ZDMV verlagert oder als Landesbetrieb dem ZDMV angeschlossen werden.

(158) Für alle in der Landesverwaltung ausgeführten Leistungen würden sich damit der Verwaltungsaufwand und die Transaktionskosten reduzieren. Die Behörden der Landesverwaltung würden ihre Anforderungen an das ZDMV adressieren und die Leistungen direkt von dort beziehen.

(159) Das Innenministerium sollte prüfen, ob der Betrieb von Fachverfahren und des Landesrechenzentrums sowie die eigene Softwareentwicklung und Beratungsleistungen für die Landesverwaltung und Kommunen als Landesbehörde dem ZDMV übertragen bzw. als Landesbetrieb dem ZDMV zugeordnet werden können (Rechtmäßigkeit, Zweckmäßigkeit, Wirtschaftlichkeit).

(160) Das Innenministerium teilt mit, dass die vom Landesrechnungshof dargestellte Aufgabenzusammenführung einer eingehenden Prüfung (u. a. Rechtmäßigkeit, Zweckmäßigkeit, Wirtschaftlichkeit) bedürfe. Insbesondere bei Fachverfahren sei das für eine Beurteilung erforderliche Wissen nur dezentral in den Behörden der Landesverwaltung vorhanden. Es sei zweckmäßig, zunächst den mit dem ZDMVG begonnenen Konsolidierungsprozess abzuschließen. Eine erste Analyse sei nach der Datenerhebung für den Rollout des verwalteten IT-Arbeitsplatzes 4 (vITA 4) möglich.

(161) Der Landesrechnungshof begrüßt, dass das Innenministerium die Vorschläge des Landesrechnungshofes prüfen wird.

5.4.3 Überschneidende Zuständigkeiten bei der Beschaffung von Hard- und Software beseitigen

(162) Die zentrale Beschaffung durch die DVZ M-V GmbH überschneidet sich teilweise inhaltlich mit den Aufgaben des LAiV. Dieses ist zentrale Vergabestelle u. a. für Software, die nicht Standard ist und Fachanwendungen, soweit nicht die DVZ M-V GmbH gesetzlich zuständig ist.

(163) Der Landesrechnungshof hatte dem Innenministerium 2021 empfohlen, diese Doppelstrukturen zu prüfen. Das LAiV wäre in der Lage, bei entsprechender Ressourcenausstattung auch Standardhard- und software zu beschaffen.[39]

(164) Das Innenministerium hat mitgeteilt, es werde die Aufgabenabgrenzung zwischen LAiV und DVZ M-V GmbH prüfen und optimieren.

(165) Ein Ergebnis liegt noch nicht vor.

(166) Der Landesrechnungshof erneuert seine Prüfbitte an das Innenministerium, ob die Beschaffung von Standardhard- und software auf das LAiV übertragen werden kann.

(167) Die Beschaffung von Standardhard- und -software durch das LAiV sei nach Auffassung des Innenministeriums nicht zweckmäßig. Ziel sei es, die IT- und IuK-Beschaffungen möglichst im Wege der Inhouse-Vergabe über die DVZ M-V GmbH abzuwickeln. Diese verfüge über das nötige Fachwissen für die Beschaffung von IT. Sie könne ihre Ressourcen flexibler an den Bedarf der Ressorts anpassen. Dieser Grundsatz sei daher auch bereits seit längerem in den Bewirtschaftungserlassen des Finanzministeriums festgehalten.

[39] Vgl. Landesrechnungshof Mecklenburg-Vorpommern 2021: Jahresbericht 2021 (Teil 1) – Landesfinanzbericht 2021, S. 104 ff., Vgl. Landesrechnungshof Mecklenburg-Vorpommern 2022: Jahresbericht 2022 (Teil 1) – Landesfinanzbericht 2022, S. 185 ff.

(168) Der Landesrechnungshof bleibt bei seiner Empfehlung, die Beschaffung im LAiV durchführen zu lassen, da dieses auf die Anwendung des Vergaberechts spezialisiert ist. Die fachlichen und funktionellen Anforderungen müssten ohnehin – wie bei allen Beschaffungen – vom Bedarfsträger definiert werden. Für die Leistungen der DVZ M-V GmbH fallen zusätzliche Ausgaben einschließlich der Umsatzsteuer an. In der Vergangenheit war die DVZ M-V GmbH oftmals personell nicht in der Lage, alle Beschaffungsvorhaben mit eigenem Personal abzuwickeln. Sie hat dann Rechtsanwaltskanzleien beauftragt, so z. B. bei der Verlängerung der DOMEA-Lizenzen. Dies hat die Beschaffungen zusätzlich verteuert, weil neben den Honoraren für die Rechtsanwaltskanzlei auch Ausgaben für die DVZ M-V GmbH als Vermittlerin entstanden.

Das Innenministerium hat nicht nachgewiesen, dass die Beschaffungen durch die DVZ M-V GmbH wirtschaftlicher sind als die durch das LAiV. Es sollte auf der Basis einer Wirtschaftlichkeitsbetrachtung und den vorstehenden Ausführungen prüfen, ob die Beschaffung auf das LAiV übertragen werden soll.

Unter Berücksichtigung der Prüfungsergebnisse zu den Empfehlungen in den Tzn. 153 bis 161 sollte das Innenministerium im Benehmen mit dem Finanzministerium eine Gesamtkonzeption erarbeiten, in der auch die zukünftige Rolle der DVZ M-V GmbH betrachtet wird.

5.5 Aufgaben zwischen Digitalisierungsabteilung und ZDMV abgrenzen

(169) In obersten Behörden sollen grundsätzlich nur ministerielle Aufgaben wahrgenommen werden. Um ministerielle Aufgaben handelt es sich, wenn die Aufgaben inhaltlich davon geprägt sind, dass sie strategischer, politischer, rechtsetzender/ normativer, konzeptioneller oder koordinierender Art sind.

Zu den nichtministeriellen Aufgaben gehören solche mit überwiegend operativem, rechtanwendendem und ausführendem Charakter, die routinemäßig erfüllt werden.

(170) Dem ZDMV sind ausschließlich operative Aufgaben zuzuweisen. Hierzu zählt insbesondere der Betrieb der Basisdienste und -infrastrukturen, das Vertragsmanagement, die Bewirtschaftung des Epl. 15 und das operative Controlling.

Der Digitalisierungsabteilung des Innenministeriums sind die strategischen und steuernden Aufgaben zuzuweisen. Hierzu zählen die Strategie, die Rechtsetzung, die Vertretung Mecklenburg-Vorpommerns in den föderalen Gremien, die Haushaltsverhandlungen zum Epl. 15 sowie das strategische Controlling.

(171) Das Innenministerium sollte einen Aufgabenkatalog für die Digitalisierungsabteilung und für das ZDMV erarbeiten, der vollständig den jeweiligen Aufgabenbestand abbildet.[40] Zuständigkeiten und Verantwortlichkeiten sind überschneidungsfrei von einander abzugrenzen. Ein solcher Aufgabenkatalog ist zudem Grundvoraussetzung für die Personalbedarfsermittlung.

[40] Vgl. Rechnungshöfe des Bundes und der Länder (2024): Grundsätze für die Verwaltungsorganisation, Nr. 2.5, a. a. O.

(172) Die Aufgaben des Innenministeriums und des ZDMV seien hinreichend konkret abgegrenzt und in den jeweiligen Geschäftsverteilungsplänen dargestellt. Die Aufteilung folge dabei auch der Abgrenzung zwischen strategisch-steuernden und operativ-vollziehenden Aufgaben.

(173) Der Landesrechnungshof begrüßt die Bemühungen des Innenministeriums, die Aufgaben abzugrenzen. Das ZDMV unterstützt derzeit das Innenministerium stark bei dessen strategischen Aufgaben zu Lasten der Erledigung seiner eigenen operativen Aufgaben. Das könnte den Betrieb der Basisdienste und -infrastrukturen gefährden.

5.6 Große IT-Projekte personell absichern

(174) Ein hohes Risiko für das Scheitern, Verzögern oder Verteuern von IT-Projekten liegt u. a. in fehlenden personellen Ressourcen besonders während der Umsetzungsphase.

(175) Es ist daher sicherzustellen, dass während der Umsetzungsphase ausreichend qualifizierte Beschäftigte zur Verfügung stehen. Da Projekte eine endliche Laufzeit haben, sollte der Personalbedarf nur vorübergehend bestehen. Um Personal vorübergehend zu beschäftigen, können Stellen mit dem Zusatz „künftig wegfallend“ ausgebracht werden. Die Notwendigkeit für die Veranschlagung dieser Stellen ist zu begründen.

(176) Die bisher häufig genutzten Doppelbesetzungsmöglichkeiten sieht der Landesrechnungshof grundsätzlich kritisch.[41] Gleichwohl könnten auch sie genutzt werden, wenn folgende Voraussetzungen gegeben sind:

- Ausgabeermächtigungen für das Projekt sind in den Haushaltsjahren veranschlagt, in denen die Doppelbesetzungsmöglichkeiten geschaffen werden,
- Planungsunterlagen gem. VV Nr. 2 zu § 24 LHO liegen vor, dies betrifft insbesondere eine Zeit- und Ressourcenplanung,
- die Notwendigkeit für die Zahl und die Wertigkeit der Stellen ist nachgewiesen,
- Qualifikationsanforderungen wurden festgelegt,
- die Doppelbesetzungsmöglichkeiten sind zeitlich befristet und nach Anzahl und Wertigkeit bestimmt.

(177) Das Finanzministerium sollte prüfen, wie befristet benötigtes Personal für die Umsetzung von IT-Projekten beschäftigt werden kann. Dafür kämen kw-Stellen oder Doppelbesetzungsmöglichkeiten in Betracht.

(178) Das Innenministerium teilt grundsätzlich die Einschätzung des Landesrechnungshofes. In vielen Fällen stehe geeignetes Personal nicht oder nur eingeschränkt am Arbeitsmarkt zur Verfügung. Neben dem allgemein bestehenden Fachkräftemangel bestehe insbesondere im Bereich IT und Digitalisierung eine ganz erhebliche Kon-

[41] Vgl. Landesrechnungshof Mecklenburg-Vorpommern 2024: Jahresbericht 2022 (Teil 1) – Landesfinanzbericht 2022, S. 27 ff.

kurrenz zu anderen öffentlichen und privaten Arbeitgebern. Gerade die vom Landesrechnungshof angeführten befristeten Stellen ließen zunehmend kaum oder keine geeigneten Bewerberinnen bzw. Bewerber erwarten und erschwerten es zudem, das einmal gewonnene Personal für die gesamte Projektdauer zu halten.

Abhilfe könnte hier ggf. ein „Pool" von unbefristet beschäftigten Projektmitarbeitern schaffen, die dem Land dauerhaft für wechselnde Digitalisierungsprojekte zur Verfügung stünden. Auf diesem Wege könnten insbesondere auch die bei der Projektumsetzung gesammelten Praxiserfahrungen dem Land langfristig erhalten bleiben und so institutionelles Wissen und Können innerhalb der Verwaltung aufgebaut werden.

Die haushaltsrechtliche Abbildung einer solchen Lösung stelle das Land indes vor erhebliche Herausforderungen.

(179) Der Landesrechnungshof begrüßt, dass Innen- und Finanzministerium das Risiko fehlender Personalressourcen für den Erfolg von IT-Projekten erkannt haben und Lösungsmöglichkeiten entwickeln.

5.7 Geschäftsprozesse als Voraussetzung für die Digitalisierung optimieren

(180) Vor der Digitalisierung von Verwaltungsprozessen ist zwingend eine Geschäftsprozessoptimierung durchzuführen.[42] Das Land hat in der Vergangenheit erhebliche Mittel für Geschäftsprozessoptimierungen ausgegeben. Es hat eigens für diesen Zweck im Januar 2020 die MV-Beratung gegründet, die seit dem 1. September 2024 in der neu gegründeten Abteilung 5 „Beteiligungen und Verwaltungsmodernisierung" im Finanzministerium angesiedelt ist.

(181) Der Landesrechnungshof hat im Landesfinanzbericht 2020 empfohlen, vorrangig IT-Projekte umzusetzen, bei denen eine digitale Rendite durch eine höhere Effizienz zu erwarten ist.[43] Auf diese Weise kann die Digitalisierung ihren Beitrag leisten, die Funktionsfähigkeit der Verwaltung zu sichern und zu verbessern. Kurzfristig können bereits freiwerdende Kapazitäten dafür genutzt werden, die Digitalisierung der Landesverwaltung zu beschleunigen.

(182) Aktuelle Prüfungsfeststellungen zeigen, dass Geschäftsprozessoptimierungen zwar durchgeführt werden, aber nicht unbedingt mit dem Ziel, die Digitalisierung vorzubereiten. In den geprüften Geschäftsprozessoptimierungen ging es z. B. um die Verkürzung der Durchlaufzeiten oder die Verbesserung der Prozessqualität. Notwendige Dokumente für die Auswahl eines geeigneten informationstechnischen Systems wurden nicht erstellt.

(183) Angesichts der Anzahl laufender Digitalisierungsprojekte in der Landesverwaltung wäre eine größere Anzahl an Geschäftsprozessoptimierungen im Zusammenhang mit diesen zu erwarten gewesen. Notwendige Geschäftsprozessoptimierungen vor Einführung oder Änderung von informationstechnischen Systemen sind jedoch

[42] Vgl. § 14 Abs. 2 EGovG M-V.

[43] Vgl. Landesrechnungshof Mecklenburg-Vorpommern 2020: Jahresbericht 2020 (Teil 1) – Landesfinanzbericht 2020, S. 81 ff.

(teilweise) unterblieben. Dies birgt das Risiko, dass nicht optimierte analoge Prozesse einfach nur digital abgebildet werden. Die Chancen der Digitalisierung im Zusammenspiel mit den erforderlichen Geschäftsprozessoptimierungen können so nicht genutzt werden.

(184) Ziel der Digitalisierung der Landesverwaltung sollte u. a. sein, die Aufgaben mit geringerem oder höchstens gleich bleibendem Personalaufwand wahrzunehmen. Durch einen stärkeren IT-Einsatz sollte eine digitale Rendite erzielt werden. Voraussetzung dafür ist die Digitalisierung der Geschäftsprozesse. Vorhandene Stellen können dann zur Erledigung anderer Aufgaben genutzt werden.

Dabei sind die Möglichkeiten digitaler Assistenzsysteme (digitale Prozessabfolgen und Regelwerke, Bereitstellung aktueller verwaltungsspezifischer Informationen, Einbindung automatisierter Datenbankabfragen) sowie von Teil- oder Vollautomatisierung (z. B. automatisierter Erlass eines Verwaltungsaktes, Dunkelverarbeitung) zu berücksichtigen.[44]

(185) Die Landesverwaltung sollte Geschäftsprozessoptimierungen vorrangig zum Zweck der Digitalisierung von Geschäftsprozessen durchführen. Dabei sind Geschäftsprozesse auszuwählen, bei denen die Digitalisierung die Wirtschaftlichkeit des Verwaltungshandelns verbessert.

(186) Die Landesregierung sollte sicherstellen, dass Verwaltungsabläufe optimiert werden, bevor informationstechnische Systeme eingeführt bzw. wesentlich geändert werden. [45]

Bei der Optimierung sollten folgende Fragen berücksichtigt werden:

- Wird eine adäquate digitale Rendite erzielt?
- Werden neue potenzielle Kunden, Partner, Produkte und Dienstleistungen berücksichtigt?
- Fügt sich das Digitalisierungsvorhaben in die Gesamtarchitektur ein?
- Ermöglichen die rechtlichen Rahmenbedingungen, insbesondere auch die untergesetzliche Regelungen (vgl. Tzn. 93 bis 97) und die vorhandenen Technologien die Zielerreichung?[46]

(187) Im Ergebnis der Geschäftsprozessoptimierung[47] müssen alle Erkenntnisse vorliegen und dokumentiert sein, die unmittelbar für die Digitalisierung des Prozesses notwendig sind. Hierzu gehören insbesondere eine Workflowdarstellung, Schnittstellenbeschreibungen und Datenmodelle.

---

[44] Vgl. Landesrechnungshof Mecklenburg-Vorpommern 2022: Jahresbericht 2022 (Teil 1) – Landesfinanzbericht 2022, S. 49.

[45] Vgl. § 14 Abs. 2 EGovG M-V.

[46] Vgl. Eidgenössische Finanzkontrolle: Modell zur Prüfung digitaler Transformation, www.efk.admin.ch/wp-content/uploads/publikationen/vorgehen-und-methoden/pruefungsmodell-der-digitalen-transformation-d.pdf.

[47] Vgl. § 14 Abs. 2 EGovG M-V.

Hierzu könnte in §§ 24 oder 54 LHO bzw. den VV zu §§ 24 oder 54 LHO verbindlich geregelt werden, dass das Ergebnis der Optimierung vorzulegen ist, bevor Haushaltsmittel für informationstechnische Systeme veranschlagt bzw. in Anspruch genommen werden.

(188) Das Innenministerium teilt die Einschätzung, dass vor der Digitalisierung von Verwaltungsprozessen eine Geschäftsprozessoptimierung durchzuführen sei. Die MV-Beratung sei mit Kabinettsbeschluss nicht ausschließlich mit der Durchführung von Geschäftsprozessoptimierungen (GPO) beauftragt worden. Die MV-Beratung wähle ihre Projekte nicht aktiv selbst aus. Sie werde durch die jeweiligen Behörden beauftragt. Die Praxiserfahrungen der MV-Beratung der letzten zwei Jahre zeigten, dass das tatsächliche Ausmaß der erforderlichen Geschäftsprozessoptimierungen in der Landesverwaltung die vorhandenen Kapazitäten der MV-Beratung deutlich übersteige. Auch in den Behörden fehlten die Kapazitäten und Fähigkeiten für die eigenständige Durchführung von GPO. Aus diesem Grund habe die MV-Beratung den Befähigungsansatz nach dem Prinzip „Hilfe zur Selbsthilfe“ eingeführt.

(189) Der Landesrechnungshof sieht nicht die MV-Beratung in der alleinigen Verantwortung GPO-Projekte durchzuführen. Die MV-Beratung sollte die Landesverwaltung vielmehr mit aktuellem Methodenwissen und einheitlichen Standards zur Prozessoptimierung unterstützen. Sie sollte die Behörden befähigen, eigenständig GPO durchzuführen bzw. bei Beauftragung von Externen, diese hinreichend steuern zu können.

(190) Das Innenministerium folgt nicht umfänglich der Auffassung des Landesrechnungshofes, dass die Landesverwaltung Geschäftsprozessoptimierungen vorrangig zum Zweck der Digitalisierung von Geschäftsprozessen durchführen sollte. In der Priorisierung von Geschäftsprozessoptimierungen sollten die maximalen Effekte maßgebend sein. Überwiegend seien maximale Effekte zwar bei Geschäftsprozessen mit mangelndem oder fehlendem Digitalisierungsstand zu erwarten, dies lasse sich jedoch nicht als generelle Behauptung aufstellen.

Das Innenministerium stimmt der Empfehlung zu, dass Verwaltungsabläufe optimiert werden müssen, bevor informationstechnische Systeme eingeführt bzw. wesentlich geändert werden. Aus den Beratungsprojekten der MV-Beratung zeige sich, dass ein deutliches Potenzial durch die Einführung von informationstechnischen Systemen nutzbar gemacht werden könnte. Dabei konnte auch das in der Prüfungsfeststellung erwähnte potenzielle Risiko, dass nicht optimierte analoge Prozesse einfach nur digital abgebildet werden, erkannt werden.

(191) Der Landesrechnungshof weist darauf hin, dass die Digitalisierung die Anforderungen an Verwaltungsprozesse grundlegend ändert, z. B. durch die Nutzung elektronischer Akten, Dunkelverarbeitung und Automatisierung, elektronische Kommunikation und elektronischen Datenaustausch. Da nahezu jeder Verwaltungsprozess davon betroffen und vor einer Digitalisierung eine Geschäftsprozessoptimierung durchzuführen ist, besteht hierfür ein enormer Bedarf. Dies stellt die Verwaltung vor große Herausforderungen. Die begrenzten Ressourcen sollten daher – zumindest vorübergehend – auf GPO-Projekte in Zusammenhang mit der Digitalisierung konzentriert werden.

(192) Das Innenministerium teilt die Aussage, wonach den IT-Ausgaben eine „digitale Rendite“ gegenüberstehen solle. Es werde verkannt, dass durch die Einführung von IT-Lösungen bereits seit Jahren eine „digitale Rendite“ in Form von Produktivitätssteigerungen erwirtschaftet werde. Dass diese Produktivitätssteigerungen für die Erfüllung von Mehraufgaben aufgebraucht würden und sich somit im Saldo nicht in „Einsparungen“ niederschlügen, sei kein Defizit der Digitalisierung.

(193) Der Landesrechnungshof weist darauf hin, dass die Landesverwaltung den Nachweis über die angeführten Produktivitätssteigerungen noch nicht erbracht hat. Steigenden IT-Ausgaben stehen noch immer steigende Personalbedarfe gegenüber. Dies ist sicher auch zum Teil auf neue Aufgaben zurückzuführen. Insofern ist neben der Digitalisierung eine grundlegende Aufgabenkritik des Verwaltungshandelns und ein damit einhergehender Abbau der Regelungsdichte notwendig.

5.8 Voraussetzungen für die Fachrichtung Verwaltungsinformatik schaffen

(194) Beamtinnen und Beamte, die Aufgaben informationstechnischer Art wahrnehmen, sind laufbahnrechtlich der Fachrichtung Allgemeiner Dienst zugeordnet. Damit fehlt eine Möglichkeit, bei Vorliegen sachlicher Gründe Besonderheiten im Unterschied zu den übrigen Beamtinnen und Beamten dieser Fachrichtung zu regeln.

(195) Seitens der Landesregierung wurde wiederholt ausgeführt, dass es Probleme bei der Personalgewinnung von Fachkräften im IT-Bereich gibt. Wenn dies auch bisher nicht empirisch belegt wurde, bietet eine eigene Fachrichtung Verwaltungsinformatik im Laufbahnrecht die Möglichkeit, zukünftigen Probleme bei der Gewinnung von Fachkräften zu begegnen. So könnte, sofern durch die Arbeitsmarktlage nachgewiesen, z. B. ein höheres Eingangsamt festgelegt werden.

(196) Eine eigene Fachrichtung ermöglicht es dem Innenministerium, Anforderungen hinsichtlich Vor- und Ausbildung und zum Vorbereitungsdienst zu regeln. Dies ermöglicht anforderungsgerechte Ausschreibungen der Dienstposten.

(197) Verwaltungsinformatik existiert als eigene Fachrichtung, Laufbahn bzw. Schwerpunkt z. B. in Thüringen, Bayern und Baden-Württemberg.

(198) Das Innenministerium sollte die Einrichtung einer Fachrichtung Verwaltungsinformatik prüfen.

(199) Das Innenministerium teilt mit, dass im Konzept zur Weiterentwicklung der Fachhochschule für öffentliche Verwaltung, Polizei und Rechtspflege des Landes Mecklenburg-Vorpommern – u. a. auch auf Anregung des Landesrechnungshofes im Rahmen der Anhörung – ein ergänzender Vorbereitungsdienst für IT-Fachkräfte aufgenommen worden sei. Die Einführung einer Fachrichtung Verwaltungsinformatik könnte grundsätzlich geeignet sein, den bestehenden Fachkräftemangel zu mildern.

(200) Der Landesrechnungshof begrüßt dies.

6 Finanzierung der Digitalisierung der Landesverwaltung

6.1 Finanzierung der Digitalisierung sichern und Haushaltsreste abbauen

(201) Die Haushaltsansätze für die Digitalisierung steigen seit 2003 deutlich. Es gelingt der Landesverwaltung aber nicht, die zur Verfügung stehenden Mittel in Anspruch zu nehmen. Dies galt insbesondere auch für die umfangreichen im MV-Schutzfonds bereitgestellten Mittel für die Digitalisierung. Zudem schiebt die Landesverwaltung eine hohe „Bugwelle“ an Haushaltsresten bei den IT-Ausgaben vor sich her.[48]

Es besteht weiterhin ein hoher Bedarf an Haushaltsmitteln für die Finanzierung der Digitalisierung der Landesverwaltung. Dies betrifft u. a. die Ablösung alter Fachverfahren und die Einführung eines einheitlichen IT-Arbeitsplatzes.

(202) Das Innenministerium sollte im Benehmen mit dem Finanzministerium die mittelfristigen Finanzierungsbedarfe erheben und in der mittelfristigen Finanzplanung abbilden. Dabei ist zu berücksichtigen, welche Personalressourcen für die Umsetzung der Maßnahmen zur Verfügung stehen. Ziel sollte ein Maßnahmenplan sein, der eine Priorisierung der Maßnahmen und die Zeiträume für die Umsetzung berücksichtigt.

(203) Das Innenministerium verweist darauf, dass der Abbau von Ausgaberesten vom Finanzministerium im Rahmen des Resteverfahrens durch eine restriktive Restebildung offensiv vorangetrieben werde.

(204) Der Landesrechnungshof begrüßt die Bemühungen des Finanzministeriums.

Einen wesentlichen Beitrag zur Vermeidung einer übermäßigen Restebildung müssen die für die veranschlagten Maßnahmen und Projekte zuständigen Behörden, insbesondere Innenministerium und ZDMV leisten. Maßnahmen und Projekte sind erst zu veranschlagen, wenn die notwendige Veranschlagungsreife erreicht ist. Die Maßnahmen und Projekte sind zielorientiert und zügig umzusetzen, so dass der rechtzeitige Mittelabfluss gewährleistet ist.

(205) Das Innenministerium verweist auf die aktuellen Bestrebungen zwischen Innenministerium und Finanzministerium, einen rollierenden Planungs- und Forecastprozess zu etablieren. Ziel sei eine größtmögliche Transparenz und Planbarkeit der notwendigen IT-Ausgaben zu erreichen. Der Feststellung, dass dabei insbesondere auch die erforderlichen Personalressourcen zu berücksichtigen seien, werde ausdrücklich zugestimmt.

Gleichwohl werde grundsätzlich an der Auffassung festgehalten, dass der Bereich IT und Digitalisierung aufgrund der ihm immanenten Eigenschaften (u. a. kurze Innova-

[48] Vgl. Landesrechnungshof Mecklenburg-Vorpommern 2020: Jahresbericht 2020 (Teil 1) – Landesfinanzbericht 2020, S. 79 ff., Vgl. Landesrechnungshof Mecklenburg-Vorpommern 2022: Jahresbericht 2022 (Teil 1) – Landesfinanzbericht 2022, S. 47 ff., Vgl. Landesrechnungshof Mecklenburg-Vorpommern 2023: Jahresbericht 2023 (Teil 1) – Landesfinanzbericht 2023, S. 26 ff., Vgl. Landesrechnungshof Mecklenburg-Vorpommern 2024: Jahresbericht 2024 (Teil 1) – Landesfinanzbericht 2024, S. 38 ff.

tionszyklen) einer präzisen, langfristigen Ausgabenplanung nur in eingeschränktem Maße zugänglich sei. Auch in Zukunft müssten haushaltsrechtlich zulässige Instrumente zur flexiblen Mittelplanung genutzt werden.

(206) Der LRH verweist auf § 6 LHO, der zur sorgfältigen Ermittlung und Schätzung der Ausgaben verpflichtet[49]. Dies setzt voraus, dass die Planung für eine Nachfolgelösung so weit fortgeschritten sein muss, dass belastbare Aussagen über die notwendigen Ausgaben getroffen werden können (Veranschlagungsreife). Der Lebenszyklus von Hardware, Betriebssystemen und Software ist im Allgemeinen bekannt. Die Hersteller kommunizieren das Ende der Produktunterstützung. Eine Ausgabenplanung ist dadurch möglich.

In der Vergangenheit scheiterte eine ordnungsgemäße und rechtzeitige Veranschlagung der Haushaltsmittel häufig daran, dass Innenministerium und ZDMV zu spät mit der Planung einer Ersatzbeschaffung begonnen haben. In einigen Fällen haben sie den Ablöseprozess erst nach Ablaufen der Herstellerunterstützung begonnen.[50]

Ein weiterer Grund für Verzögerungen und damit für Restebildungen war die aufwändige Erarbeitung der Anforderungen. Das Innenministerium und das ZDMV sollten einen effizienten Prozess etablieren, um Anforderungen zügig aufzunehmen und zu prüfen. Die Anzahl der beteiligten Akteure (Rollen) sollte auf das notwendige Maß begrenzt werden.

Aufgrund der Abhängigkeit von den kurzen Produktzyklen bestimmter Hersteller ist der Aufwand für Ersatzbeschaffungen groß. In einigen Fällen sind die Produktzyklen so kurz, dass bereits bei der Einführung die Planung für die Ablösung beginnen muss. Dies stellt die Verwaltung vor große Herausforderungen. Mittelfristig kann Abhilfe dadurch geschaffen werden, dass die Abhängigkeiten von diesen Herstellern, z. B. durch den Einsatz von Open Source-Lösungen, beseitigt oder zumindest verringert werden.

6.2 Ablösebedarfe von Fachverfahren analysieren

(207) Der Landesrechnungshof hat bei den Ressorts erfragt, welche Fachverfahren sie einsetzen. Die Ressorts haben angegeben, aktuell 774 Fachverfahren einzusetzen.

(208) Der Landesrechnungshof hat erhoben, wie lange die Fachverfahren eingesetzt werden und ob Ablösebedarf besteht. Die Ergebnisse sind in Abbildung 3 dargestellt. Für 634 von 774 Fachverfahren (rd. 82 %) waren Angaben zum Einsatzalter vorhanden.

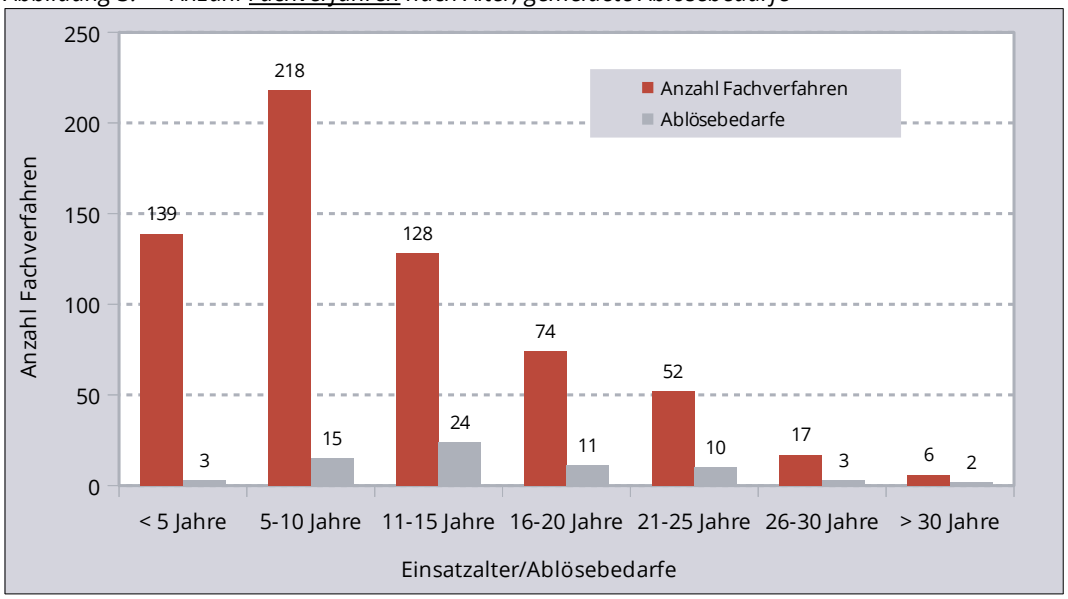
149 von 634 Verfahren (rd. 24 %) sind älter als 15 Jahre. Für 26 der 149 Fachverfahren (rd. 17 %) wurden Ablösebedarfe gemeldet. Es ist davon auszugehen, dass das Betriebsrisiko mit zunehmender Einsatzdauer zunimmt und der Ablösebedarf steigt. Bei den Verfahren die älter als 15 Jahre sind, ist daher davon auszugehen, dass we-

[49] Vgl. Heuer, Scheller: Kommentar zum Haushaltsrecht, Rnr. 7 zu § 6 Bundeshaushaltsordnung.

[50] Vgl. Landesrechnungshof Mecklenburg-Vorpommern (2020): Jahresbericht 2020 (Teil 1) – Landesfinanzbericht 2020, S. 223 ff.

sentlich mehr als die 26 mit Ablösebedarf gemeldeten Verfahren in den nächsten Jahren ablösebedürftig sein werden.

Abbildung 3: Anzahl Fachverfahren nach Alter, gemeldete Ablösebedarfe



Quelle: eigene Erhebung, Fachverfahren mit Angaben zum Einsatzalter und Ablösebedarfen.

(209) Es sind wenige Verfahren mit Ablösebedarf gemeldet worden. Belastbare Analysen und Zahlen zu den Ablösebedarfen liegen nicht vor. Es ist absehbar, dass in den nächsten Jahren ein erheblicher Investitionsbedarf besteht. Dies deutet darauf hin, dass die Behörden keine systematische Abwägung der Risiken vornehmen und Rechtmäßigkeit, Wirtschaftlichkeit und Zweckmäßigkeit der eingesetzten Verfahren nicht regelmäßig prüfen. Darin liegt ein finanzielles Risiko für die mittelfristige Planbarkeit des Landeshaushalts und für die Aufgabenwahrnehmung. Die Landesverwaltung steuert die Lebenszyklus-Risiken für einen sicheren und ordnungsgemäßen Betrieb nicht ausreichend.

(210) Die Behörden sollten regelmäßig die Betriebsrisiken von Fachverfahren analysieren und die Wirtschaftlichkeit feststellen. Der Ablösezeitpunkt eines Fachverfahrens muss bestimmt werden. Kriterien hierfür sind Betriebsrisiken, Rechtmäßigkeit, Wirtschaftlichkeit und Zweckmäßigkeit.[51] Ablösebedarfe sind systematisch zu ermitteln und rechtzeitig dem ZDMV anzuzeigen. Das ZDMV sollte für alle Fachverfahren eine Planung zum voraussichtlichen Ablösezeitpunkt vorlegen. Die Planungen für die Ablösung sind so rechtzeitig zu beginnen, dass die dafür notwendigen Haushaltsmittel im jeweiligen Haushaltsjahr veranschlagungsreif sind.

6.3 Vertragsmanagement und -controlling einrichten

(211) Prüfungsfeststellungen des Landesrechnungshofes zeigen, dass die Behörden der Landesverwaltung nur einen unzureichenden Überblick über ihre Verträge haben. Ein Vertragsmanagement und -controlling existierte nicht.[52]

[51] Vgl. Landesrechnungshof Mecklenburg-Vorpommern (2023): Jahresbericht 2023 (Teil 1) Landesfinanzbericht 2023, S. 45f.

[52] Vgl. Landesrechnungshof Mecklenburg-Vorpommern (2023): Jahresbericht 2023 (Teil 1) Landesfinanzbericht 2023, S. 140.

(212) Der Landesrechnungshof empfahl, ein Vertragsmanagement und -controlling einzurichten.

(213) Dieser Empfehlung kam die Landesverwaltung bislang nicht nach.

(214) Wenn die Landesbehörden keine vollständige Übersicht über ihre Verträge besitzen, können sie ihre Leistungsbeziehungen nicht aktiv steuern. Zudem fehlen wichtige Informationen für die Veranschlagung von Haushaltsmitteln. Im Rahmen der Haushaltsaufstellung des Einzelplans 15 erhebt das Finanzministerium zur Zeit grundlegende Informationen über Vertragsbeziehungen. Ein vollständiger Überblick über die Verträge ist u. a. Voraussetzung für einen ordnungsgemäßen Aufgabenübergang an das ZDMV.

(215) Das ZDMV sollte ein Vertragsmanagement und -controlling einführen. Bei der Aufgabenübernahme von den Ressorts sind die Angaben zu den existierenden Verträgen systematisch zu erfassen. Diese sind über ihren gesamten Lebenszyklus zu verwalten.

(216) Soweit Teile der Landesverwaltung nicht vom ZDMVG erfasst sind (wie z. B. der Geschäftsbereich des Justizministeriums), sollten sie ein eigenes Vertragsmanagement und -controlling einführen. Das ZDMV sollte prüfen, ob eine IT-Lösung für das Vertragsmanagement und -controlling als Basisdienst für die gesamte Landesverwaltung eingeführt werden kann.

(217) Das Innenministerium stimmt der Auffassung des Landesrechnungshofes im Ergebnis zu. Das ZDMV habe für seinen Zuständigkeitsbereich bereits ein Vertragsmanagement und -controlling eingesetzt. Die im Rahmen der Haushaltsplanung 2026/2027 ressortübergreifend erhobenen Vertragsdaten sollten von den Ressorts laufend fortgeschrieben werden und u. a. auch die ordnungsgemäße Übergabe der Aufgaben und Verträge an das ZDMV vorbereiten.

Das Innenministerium strebe die Einführung einer IT-Lösung für das Vertragsmanagement an. Das Finanzministerium und das Innenministerium bereiteten hierzu ein gemeinsames Projekt vor, um auch einen größtmöglichen (Mit-) Nutzen der Lösung für die Haushaltsplanung und -bewirtschaftung sicherzustellen.

(218) Der Landesrechnungshof begrüßt die Bemühungen von Innen- und Finanzministerium. Defizite beim Vertragsmanagement und -controlling bestehen bei allen Ressorts. Er empfiehlt, ein einheitliches Vertragsmanagement und -controlling als Basisdienst – nicht nur für IT-Verträge – zentral zur Verfügung zu stellen.

7 Technologie und Architektur

7.1 Architekturvorgaben festlegen

(219) Es fehlen Vorgaben für IT-Architekturen in der Landesverwaltung. Eine IT-Architektur legt die Grundstrukturen fest und definiert Regeln und Standards, die das dynamische Zusammenspiel der verschiedenen IT-Komponenten steuern (Anwendungen, Daten, Infrastruktur, Sicherheitsarchitektur).

(220) IT -Architekturen sind organisations- und ebenenübergreifend abzustimmen. Durch die Verwendung offener, interoperabler Standards wird sichergestellt , dass die Elemente der verschiedenen *IT-Architekturen* kompatibel und nachnutzbar sind.

Vorgaben für die IT-Architektur sind aus den jeweiligen strategischen Zielen abzuleiten.

(221) Das Innenministerium sollte Vorgaben zur IT-Architektur in der IT-Richtlinie festlegen. Föderale Vorgaben durch den IT-Planungsrat oder die Föderale IT-Kooperation[53] (FITKO) sind zu berücksichtigen. Das Innenministerium sollte die Grundprinzipien für die Gestaltung der Informationstechnik in der Landesverwaltung festschreiben. Insbesondere sollte es hierbei berücksichtigen

- Konsolidierung und Vereinheitlichung (Betrieb, informationstechnische Systeme, Dienste),
- digitale Souveränität,
- ebenenübergreifende Interoperabilität, insbesondere unter Berücksichtigung der Beschlüsse des IT-Planungsrates und der Vorgaben des Europäischen Interoperabilitätsrahmens,
- Anpassungsfähigkeit an den digitalen Wandel und Skalierbarkeit,
- Informationssicherheit und Datenschutz (security by design und privacy by design).

Das Innenministerium sollte prüfen, inwieweit auch die kommunale Ebene Architekturvorgaben verpflichtend anzuwenden hat.

(222) Das Innenministerium teilt mit, dass es die Hinweise des Landesrechnungshofes bei der Überarbeitung der IT-Richtlinie beachten werde.

(223) Der Landesrechnungshof begrüßt dies.

7.2 Betriebsstandards für Fachverfahren festlegen

(224) Der Landtag hat die Landesregierung gebeten, eine zukunftsfähige Betriebsstrategie für Fachverfahren zu entwickeln. Dabei sollte die Deutsche Verwaltungscloud (DVC) als mögliche Betriebsumgebung geprüft werden. Die sichere Migration der Fachverfahren ist bei der Einführung eines standardisierten IT-Arbeitsplatzes zu gewährleisten.[54]

(225) Bisher wird häufig für jede Fachaufgabe ein monolithisches Fachverfahren entwickelt. Dies ist sehr ressourcen- und zeitaufwändig. Häufig ist die Technologie schon wieder veraltet, wenn das Fachverfahren fertig entwickelt ist und regelmäßig betrieben wird.

[53] Vgl. § 5 Vertrag über die Errichtung des IT-Planungsrats und über die Grundlagen der Zusammenarbeit beim Einsatz der Informationstechnologie in den Verwaltungen von Bund und Ländern – Vertrag zur Ausführung von Artikel 91c GG (IT-Staatsvertrag).

[54] Vgl. Drs. 8/3408.

(226) Für die Entwicklung neuer Fachverfahren sollten zeitgemäße Technologien genutzt werden:

- Fachverfahren sollten modular aufgebaut sein, so dass einzelne Teile bei Bedarf erneuert werden können. Für Funktionen, die bei vielen Fachverfahren gleichermaßen benötigt werden, sollten dieselben Module (wieder)verwendet werden.
- Fachverfahren sollten auf einem einheitlichen Betriebsstandard beruhen. Dies reduziert den Entwicklungsaufwand und vereinfacht den Betrieb im Rechenzentrum. Zudem kann der Betrieb einfacher von einem Rechenzentrum auf ein anderes verlagert werden. Dies verbessert auch das Notfallmanagement.
- Soweit Fachaufgaben auf einem einfachen Verwaltungsprozess beruhen, können aus diesen Prozessen mittels Low-Code-Lösungen direkt Fachanwendungen erstellt werden.
- Bei einfachen Fachaufgaben können auch vorgegebene Strukturen und wiederverwendbare Bausteine die Entwicklung vereinfachen und verkürzen.

(227) Bei Fachverfahren sollte soweit wie möglich auf bereits bestehende IT-Lösungen anderer Länder gesetzt werden. Hierzu kann das Land Entwicklungs- oder Betriebsverbünden beitreten. Die mit einer Eigenentwicklung von IT-Fachverfahren verbundenen finanziellen und personellen Ressourcen sind per se nicht wirtschaftlich. Zusätzlich ist mit hohen Risiken zu rechnen. Diese bestehen in Überschreitungen der geplanten Kosten und Zeitziele sowie Betriebsrisiken.

(228) Die Freie und Hansestadt Hamburg hat mit MODUL-F eine Low-Code-Entwicklungsplattform bereitgestellt. Es handelt sich um eine „Einer-für-Alle“-Leistung. Sie kann auf dem EfA-Marktplatz „govdigital“ direkt und ohne Ausschreibung bezogen werden.

(229) Bevor neue Fachverfahren eingeführt bzw. alte Fachverfahren abgelöst werden, sollte die Landesverwaltung prüfen, ob

- der Beitritt zu einem Entwicklungs- oder Betriebsverbund bzw. die Nachnutzung einer vorhandenen Lösung zweckmäßig und wirtschaftlich ist,
- die Architektur auf bundesweit zur Verfügung stehenden Standards beruhen kann (DVC, SCS) oder
- eine Low-Code-Entwicklung ausreichend und wirtschaftlich ist.

Bevor Haushaltsmittel veranschlagt werden, müssen diese Fragen geprüft und in den gemäß VV Nr. 2 zu § 24 LHO zu erstellenden Planungsunterlagen beantwortet sein. Das Finanzministerium sollte die VV Nr. 2 zu § 24 LHO dahingehend konkretisieren.

(230) Das Innenministerium teilt mit, dass es die Hinweise des Landesrechnungshofes zur Migration von Fachverfahren bei der Einführung eines zentralen IT-Arbeitsplatzes berücksichtigen werde. In die Entwicklung der DVC sei das Land über den IT-Planungsrat und die Mitarbeit im DVC-Architekturboard eng eingebunden. Es werde die DVC bei der Ausrichtung der Fachverfahrensstrategie in der Landesverwaltung berücksichtigen.

(231) Der Landesrechnungshof begrüßt dies.

(232) Das Innenministerium führt aus, dass es eine verbindliche Regelung in VV Nr. 2 zu § 24 LHO für nicht notwendig erachte. Der Bewirtschaftungserlass sehe hierzu bereits ergänzende Regelungen vor.

(233) Der Landesrechnungshof hält es für erforderlich, dass die Prüffragen in Tz. 229 im Rahmen der gem. VV Nr. 2 zu § 24 LHO zu erstellenden Planungsunterlagen beantwortet werden müssen. Er bleibt daher bei seiner Empfehlung, VV Nr. 2 zu § 24 LHO dahingehend zu konkretisieren.

7.3 Digitale Souveränität gewährleisten

(234) Der Landesrechnungshof hatte untersucht, ob und wie Open Source einen Beitrag leisten kann, die digitale Souveränität der Landesverwaltung zu erhöhen. Er hatte empfohlen, dass das seinerzeit zuständige Energieministerium die Abhängigkeit der Landesverwaltung von Softwareanbietern analysieren und Risiken dieser Abhängigkeit bewerten sollte. Weiterhin hatte er dem Energieministerium empfohlen, die Einsatzmöglichkeiten von Open Source zu prüfen und zu erproben.[55]

Der Landtag hat beschlossen, dass das Energieministerium die Abhängigkeit der Landesverwaltung von Softwareanbietern untersuchen, daraus resultierende Risiken bewerten sowie die Möglichkeiten einer stärkeren Nutzung von Open Source prüfen sollte.[56]

(235) Der Aufwand für einen Wechsel zu Open Source ist unterschiedlich. Am anspruchsvollsten sind die Betriebssysteme für Endgeräte und für Server. Weniger aufwändig ist ein Wechsel in der Peripherie. Bei einem modularen Aufbau der IT-Arbeitsplätze können Komponenten für E-Mail, Chat und Videokonferenzen durch Open Source ersetzt werden.

(236) Das Innenministerium sollte zunächst die Nutzung von Open Source bei den Modulen des IT-Arbeitsplatzes prüfen, die eine geringe Integration in das Kernsystem benötigen.

(237) Zur Zeit verfolgt die Bundesregierung zwei unterschiedliche Ansätze, souveräne IT-Arbeitsplätze zur Verfügung zu stellen.

Der Bund hat das Zentrum für digitale Souveränität eingerichtet (ZENDIS). Dieses soll Projekte durchführen, um mehr Open Source in der Verwaltung zu nutzen. Hierzu zählt auch openDesk, ein auf Open Source basierender Arbeitsplatz.

OpenDesk vereint Open Source-Komponenten unter einer einheitlichen Oberfläche z. B. für Textverarbeitung, Tabellenkalkulation, E-Mail, Kontakte, Kalender, Chats, Videokonferenz und gemeinsames Arbeiten an Dokumenten.

---

[55] Landesrechnungshof Mecklenburg-Vorpommern (2020): Jahresbericht 2020 (Teil 1) – Landesfinanzbericht 2020, S. 61.

[56] Landesrechnungshof Mecklenburg-Vorpommern (2023): Jahresbericht 2023 (Teil 1) – Landesfinanzbericht 2023, S. 189 ff., Vgl. Drs 8/1533 mit Bezug auf LFB 2020 Tzn. 127 – 151.

Die Alternative ist eine souveräne Cloud-Plattform (Delos-Cloud). Sie ist Teil der Multicloudstrategie der Bundesregierung. Sie basiert auf einem Cloudangebot eines etablierten amerikanischen Cloudanbieters und ermöglicht die Nutzung der Bürosoftware dieses Anbieters. Drittanbieter können ebenfalls Lösungen über die Cloud anbieten, sofern diese die BSI-Anforderungen erfüllen.

(238) Das Innenministerium sollte beide Alternativen hinsichtlich Rechtmäßigkeit und Wirtschaftlichkeit prüfen. Aus Sicht der digitalen Souveränität ist die Variante openDesk vorzuziehen. Diese wird von einer Einrichtung des Bundes weiterentwickelt. Bei der Delos-Cloud bleibt es bei der Abhängigkeit von einem kommerziellen Anbieter, der bereits jetzt über erhebliche Marktmacht verfügt. Zudem bestehen Zweifel, ob die Delos-Cloud datenschutzkonform und den Anforderungen aus der Informationssicherheit entsprechend betrieben werden kann.

(239) Das Innenministerium teilt mit, dass es die Hinweise des Landesrechnungshofes in den Tzn. 236 und 238 bei der Prüfung von Open Source-Lösungen berücksichtigen werde.

(240) Der Landesrechnungshof begrüßt dies. Das Innenministerium sollte seine dahingehenden Prüfungen umfassend dokumentieren.

8 Informationssicherheit

(241) Für die gesamte Landesverwaltung gilt der IT-Grundschutz des Bundesamtes für Sicherheit in der Informationstechnik (BSI) als Mindestsicherheitsniveau.[57] Dementsprechend ist auch die dafür geltende Methodik anzuwenden. Die Einhaltung des IT-Grundschutzes ist wesentliche Voraussetzung für eine rechtmäßige Datenverarbeitung.

(242) Nach Einschätzung des Innenministeriums liegen die aktuellen Bedrohungen der Landes-IT in

- Ransomware,
- Spam-Emails,
- Sicherheitslücken in Hard- und Software und
- Distributed-Denial-of-Service (DDoS)-Angriffen.

2023 und im ersten Halbjahr 2024 traten 26 ressortübergreifende Sicherheitsvorfälle ein. Bei 19 Sicherheitsvorfällen konnten die genannten Bedrohungen als Ursache bzw. als Anlass zugeordnet werden.[58]

[57] Ministerium für Inneres und Sport Mecklenburg-Vorpommern (2012), Leitlinie zur Gewährung der Informationssicherheit in der Landesverwaltung von M-V, S. 3 f.

[58] Vgl. Schreiben des Innenministeriums vom 9. September 2024, Az.: II-252-02000-2021/014-004, S. 1 ff

8.1 Sicherheitsorganisation aufbauen

(243) Gemäß den BSI-Standards im IT-Grundschutz ist die oberste Managementebene jeder Behörde für das zielgerichtete und ordnungsgemäße Funktionieren der Institution verantwortlich.[59]

Die Informationssicherheitsbeauftragten (ISB) unterstützen die jeweilige Behördenleitung mit der Erledigung operativer Aufgaben bei der Gewährleistung der Informationssicherheit.[60] Sie spielen für die Aufrechterhaltung und Verbesserung der Informationssicherheit auch aufgrund ihrer Unabhängigkeit eine wichtige Rolle.

(244) Der Landesrechnungshof bat das Innenministerium um einen Überblick über die Einrichtung der ISB in den Ressorts. Die Ergebnisse sind in Tabelle 1 dargestellt.

Tabelle 1: Informationssicherheitsbeauftragte in den Ressorts des Landes

Ressort	SOLL (VZÄ)	IST (VZÄ)	Bemerkungen
BM	1	1	Zuständigkeit: Ministerium, Schulämter und IQMV
FM	3,1	2,9	
IM	3,4	1,1	Darunter ZDMV Soll 1,0, Ist 0, Begründung: keine Stelle vorhanden.
JM	0,5	0,5	Das Justizministerium wird durch eine private Firma aufgrund eines Vertrages mit dem DVZ zusätzlich beraten und unterstützt.
LM	0	0	Die Leistung des IT-Sicherheitsbeauftragten wird durch die DVZ GmbH im Rahmen eines Dienstleistungsvertrages erbracht.
SM	1,5	1,3	Die Funktion des Informationssicherheitsbeauftragten des Ressorts teilen sich die Informationssicherheitsbeauftragten des Sozialministeriums und des LAGuS
StK	0	0	*„Die Beauftragtenfunktionen sind grundsätzlich nicht mit Stellenanteilen im HH-Plan hinterlegt. Die Aufgabe des IT-SIBE wird im Rahmen der organisationsrechtlichen Erwägungen wahrgenommen und erfüllt. Die Beauftragtenfunktion kann laufbahnübergreifend wahrgenommen werden. Die Besetzung der Beauftragtenfunktion steht nicht in Abhängigkeit einer Stelle, sondern hängt von der Bereitschaft der KollegInnen dieses Amt zu übernehmen ab. Die Beauftragtenfunktion wird zusätzlich zur originären Fachaufgabe wahrgenommen.“*
WKM	1	1	
WM	Keine Meldung		
Summe	**10,5**	**7,8**	

Quelle: Erhebungen des Landesrechnungshofes.

(245) Der Stellenbedarf für die Aufgaben eines ISB ist abhängig von der Größe und den Aufgaben der Institution. Soweit die Ressorts Stellen bzw. Stellenanteile im Soll angegeben haben, geht der Landesrechnungshof davon aus, dass es sich um den notwendigen Bedarf handelt.

Insofern hält es der Landesrechnungshof für bedenklich, dass von den angegebenen 10,5 VZÄ im Soll nur 7,8 VZÄ im Ist besetzt sind. Insbesondere ist auffällig, dass im ZDMV keine Stelle für einen ISB vorhanden ist, obwohl das ZDMV für zentrale Basisdienste und -infrastrukturen verantwortlich ist. Dies stellt ein hohes Risiko für diese zentralen Basisdienste und -infrastrukturen und damit für die Funktionsfähigkeit der gesamten IT der Landesverwaltung dar.

[59] Vgl. Bundesamt für Sicherheit in der Informationstechnik (2017), BSI-Standard 200-1 – Managementsysteme für Informationssicherheit, S. 20.

[60] Vgl. Bundesamt für Sicherheit in der Informationstechnik (2017), BSI-Standard 200-2 – IT-Grundschutz-Methodik, S. 19.

(246) Die Ressorts haben dafür Sorge zu tragen, hinreichend qualifiziertes Personal im erforderlichen Umfang für diese Aufgabe vorzuhalten. Im ZDMV ist unverzüglich ein ISB einzusetzen.

(247) Innerhalb einer Organisation müssen alle relevanten Aufgaben und Funktionen klar definiert und voneinander abgegrenzt sein.[61] Dies gilt auch für die Funktion des ISB.

Deshalb ist es notwendig einen ISB eindeutig zu benennen.

Die Entscheidung der Staatskanzlei, die Aufgabe des ISB im Rahmen der organisationsrechtlichen Erwägungen wahrzunehmen, erfüllt die Anforderungen aus dem BSI-Grundschutz nicht. Die Aufgaben des ISB können parallel zu Fachaufgaben wahrgenommen werden, soweit diese nicht inkompatibel sind. Um zu gewährleisten, dass der ISB seine Aufgaben im notwendigen Umfang wahrnehmen kann, sind dafür separate Stellen bzw. Stellenanteile auszuweisen.

(248) Die Staatskanzlei hat einen ISB zu bestellen und für diese Aufgaben Stellen bzw. Stellenteile auszuweisen.

(249) Grundsätzlich ist eine Bestellung auch von Externen im Justiz- und Landwirtschaftsministerium als ISB zulässig. Um die Aufgaben eines ISB sachgerecht wahrnehmen zu können, ist allerdings umfangreiches Wissen über die eingesetzten IT-Verfahren und verarbeiteten Daten sowie die Verfahrensweisen in der jeweiligen Behörde notwendig. In großen, komplexen Organisationen, wie z. B. einem Ministerium als oberste Landesbehörde, sollte von einer externen Beauftragung abgesehen werden. Die Funktion des ISB sollte nur im Ausnahmefall von Externen ausgeübt werden.

(250) Das Justiz- und Landwirtschaftsministerium sollten das Outsourcing der Aufgaben des ISB überprüfen.

(251) Das Innenministerium teilt mit, dass die Aufgaben des ISB innerhalb des Geschäftsbereichs der Ministerpräsidentin einer Person übertragen worden seien. Bei der Auswahl des ISB habe die Staatskanzlei ein besonderes Augenmerk darauf gelegt, dass die Aufgaben des ISB mit den Fachaufgaben keinen Interessenkonflikt verursachten und die zu bestellende Person fachlich geeignet sei. Vor dem Hintergrund des anstehenden Übergangs der Aufgabe an das ZDMV sei eine Stellenausweisung nicht vorgenommen worden.

Weiterhin teilt das Innenministerium mit, dass es prüfen werde, ob die Bestellung von externem Personal als ISB bei den obersten Landesbehörden mit dem Informationssicherheitsgesetz näher geregelt oder untersagt werden sollte.

(252) Der Landesrechnungshof begrüßt, dass das Innenministerium prüfen wird, ob die Bestellung externen Personals als ISB gesetzlich geregelt oder untersagt werden müsse.

[61] Vgl. BSI-Grundschutzkompendium, Baustein ORP.1 Organisation, Anforderung ORP.1.A1 Festlegung von Verantwortlichkeiten und Regelungen.

8.2 Sicherheitslage in der Landesverwaltung beobachten

(253) Mit dem Konzept zum Aufbau und Betrieb eines Informationssicherheitsmanagements in der Landesverwaltung von Mecklenburg-Vorpommern wurden zusätzliche Berichtspflichten definiert. So haben die ISB der Ressorts quartalsweise Sicherheitslageberichte zu erstellen.

Das CERT soll die Meldungen der Ressorts anonymisieren, zusammenfassen und an den BeLVIS weiterleiten. Dieser soll daraus den quartalsweisen IT-Sicherheitslagebericht für die gesamte Landesverwaltung erstellen.

(254) Der Landesrechnungshof bat das Innenministerium um Übersendung der Sicherheitslageberichte für 2022 bis 2024.

(255) Das Innenministerium teilte mit, dass das Informationssicherheitsmanagement in der Landesverwaltung bislang nicht den Reifegrad erreicht habe, regelmäßig landesspezifische Sicherheitslageberichte zu erstellen. Es sollten jedoch anlassbezogene Sicherheitslageberichte erstellt werden. Das Innenministerium hat dem Landesrechnungshof keine Sicherheitslageberichte übersandt.

(256) Es fehlt damit ein zentraler und umfassender Überblick über die Sicherheitslage in der Landesverwaltung.

(257) Das Innenministerium hat dafür Sorge zu tragen, dass die IT-Sicherheitslageberichte erstellt werden. Dies sollte im IT-Sicherheitsgesetz gesetzlich verankert werden.

8.3 Informations- und Datensicherheitsstrategie 2023 umsetzen

(258) Im Dezember 2020 veröffentlichte das Innenministerium die „Informations- und Datensicherheitsstrategie 2023“.[62] Die Strategie sah u. a. eine Stärkung der Stellung des BeLVIS und eine bessere Ressourcenausstattung der Informationssicherheitsorganisation in der Landesverwaltung vor.

(259) Die Aufgaben und Kompetenzen des BeLVIS blieben unverändert. Die personelle Ausstattung in der Informationssicherheitsorganisation ist unzureichend. Als ressortübergreifendes Regelwerk bestehen weiterhin nur die Anschluss- und Benutzungsbedingungen für das Verwaltungsnetz des Landes, CN LAVINE.

Die mit der Strategie verbundenen Ziele hat das Innenministerium bisher nicht erreicht.

(260) Das Innenministerium hat einen Prozess aufzusetzen, der gewährleistet, dass die Informationssicherheits- und Datensicherheitsstrategie regelmäßig geprüft, fortgeschrieben und deren Zielerreichung überwacht wird. Die in der Strategie definierten Ziele sind zeitnah umzusetzen.

[62] Vgl. https://wir.m-v.de/dokumentation-und-wissen/informationssicherheit/Leitlinien-und-Sicherheitsstandards/.

(261) Das Innenministerium teilt mit, dass es den Hinweis bei der Erarbeitung des Entwurfs für ein Informationssicherheitsgesetz berücksichtigen werde. Ein Prozess existiere bereits. Die Informations- und Datensicherheitsstrategie 2028 werde derzeit fortgeschrieben. Mit der Fortschreibung würden auch mess- und prüfbare Kennzahlen aufgenommen werden.

(262) Der Landesrechnungshof begrüßt dies.

8.4 Informationssicherheit regelmäßig überprüfen

(263) In regelmäßigen Abständen sollte die Umsetzung der Sicherheitsmaßnahmen mit Hilfe von Audits ausgewertet werden.[63]

(264) Mit dem „Auditprogramm“ hat sich die Landesverwaltung eine eigene Richtlinie zur Vorbereitung und Durchführung von Audits geschaffen. Danach muss bis zum 15. Januar des jeweiligen Kalenderjahres festgelegt werden, welche einzelnen Audits mit festgelegten Beteiligten durchgeführt werden sollen.[64]

(265) Der Landesrechnungshof hatte die Audits und den Stand der Durchführung für 2022 bis 2024 beim Innenministerium erfragt. Die für die jeweiligen Jahre geplanten und abgeschlossenen Audits sind in Tabelle 2 dargestellt.

Tabelle 2: Durchführungsstand der Audits der Jahre 2022 bis 2024

Jahr	Geplante Audits	Abgeschlossene Audits
2022	11	4
2023	9	0
2024	7	0

Quelle: Erhebungen des Landesrechnungshofes.

(266) Dem Innenministerium gelang es nicht, seine eigenen Auditplanungen einzuhalten.

(267) In der Landesverwaltung werden 774 Fachverfahren sowie verschiedene E-Government-Basisdienste und zentrale IT-Standardverfahren eingesetzt. Aktuell ist eine dem Risiko angemessene Kontrolldichte zur Gewährleistung des Sicherheitsniveaus nicht gegeben.

(268) Zur Gewährleistung der Informationssicherheit und des Datenschutzes haben die Ressorts sowie die CIO geeignete Audits zu planen und durchzuführen.

(269) Neben den Audits, in denen umfassende Betrachtungen zu den jeweiligen Verfahren durchgeführt werden, finden in der Landesverwaltung noch weitere Prüfmethoden der Erfolgskontrolle Anwendung. Zu diesen zählen IS-Penetrationstests, Schwachstellenanalysen und der IS-Webcheck.

(270) Der Landesrechnungshof hat die Sicherheitsprüfungen 2022 bis 2024 beim Innenministerium angefragt. Dieses hat zwei Schwachstellenanalysen, drei IS-Webchecks und zwei Penetrationstests durchgeführt.

[63] Vgl. Bundesamt für Sicherheit in der Informationstechnik (2017), BSI-Standard 200-1 – Managementsysteme für Informationssicherheit, S. 30.

[64] Vgl. Ministerium für Inneres, Bau und Digitalisierung (2023), Auditprogramm, S. 9 f.

(271) In den Überprüfungen hat der BeLVIS zum Teil erhebliche Mängel und Defizite festgestellt.

Zum Beispiel hat ein Penetrationstest bei einer zentralen Komponente 18 Schwachstellen ergeben, deren klassifiziertes Schadenspotenzial „mittel“ bis „hoch“ eingeschätzt wurde.[65] Zu fünf kritischen Schwachstellen empfahl der BeLVIS, Maßnahmen dringend und umgehend umzusetzen.

Die Digitalisierungsabteilung des Innenministeriums bzw. das ZDMV haben auf die durch den BeLVIS aufgezeigten Schwachstellen nicht reagiert. Abschließende Vermerke mit den abgeleiteten bzw. umzusetzenden Maßnahmen lagen nicht vor.

(272) Die kritischen Schwachstellen bestehen noch immer, obwohl sie den verantwortlichen Stellen bekannt sind. Die Informationssicherheit des gesamten Informationsverbundes ist damit gefährdet. Es besteht dringender Handlungsbedarf.

(273) Das Innenministerium hat unverzüglich alle Maßnahmen zu treffen, die notwendig sind und vom BeLVIS empfohlen wurden, um bestehende Schwachstellen zu beseitigen. Es hat organisatorische Vorkehrungen zu treffen, um zukünftig unverzüglich auf Ergebnisse durchgeführter Prüfungen reagieren zu können.

(274) Das Innenministerium teilt mit, dass die Stellung des BeLVIS mit dem Informationssicherheitsgesetz gestärkt werden solle.

Seit der Abfrage des Landesrechnungshofes seien zwei weitere, d. h. insgesamt fünf IS-Webchecks durchgeführt worden.

Die durch den BeLVIS identifizierten Maßnahmen zur Schließung von Schwachstellen seien kontinuierliche Aufgaben im Servicemanagement. Die Maßnahmen würden derzeit bearbeitet bzw. seien teilweise bereits durch den/die IT-Dienstleister umgesetzt worden.

(275) Der Landesrechnungshof begrüßt, dass die Stellung des BelVIS gestärkt werden soll.

Die vom BeLVIS aufgezeigten Sicherheitslücken sind unverzüglich zu schließen. Angesichts der Defizite im Informationssicherheitsmanagement und der aktuellen Bedrohungslage müssen Innenministerium und ZDMV ihre Aktivitäten zur Verbesserung der Informationssicherheit verstärken.

Vom Senat des Landesrechnungshofes beschlossen am 5. März 2025.

[65] Aus Sicherheitsgründen verzichtet der Landesrechnungshof auf eine detaillierte Darstellung.

Anlagen

Anlage 1: Entschließungen des Landtages und Umsetzungsstand

Jahr	Themenfeld	Entschließung	Quelle	Umsetzung
2019	E-Government	Das Energieministerium wird gebeten, zeitnah eine **aktualisierte E-Government- und IT-Strategie** zu erarbeiten.	Drs. 7/4162, Ziff. I 1 mit Bezug auf **LFB 2019** Tzn. 106 – 107	nicht umgesetzt
	Regulierung	Das Energieministerium wird gebeten, eine **IT-Richtlinie** zu erlassen und **IT-Standards** landesweit verbindlich festzulegen.	Drs. 7/4162, Ziff. I 1 mit Bezug auf **LFB 2019** Tzn. 106 – 107	nicht umgesetzt
	Regulierung	Das Energieministerium wird gebeten, das **E-Government-Gesetz** zu überarbeiten und die Notwendigkeit eines **Informationssicherheitsgesetzes** zu prüfen.	Drs. 7/4162, Ziff. I 1 mit Bezug auf **LFB 2019** Tzn. 106 – 107	nicht umgesetzt
	Technologie und Architektur	Das Energieministerium wird gebeten, funktionale und wirtschaftliche Anforderungen für IT-Arbeitsplätze in der Landesverwaltung festzulegen und einen standardisierten IT-Arbeitsplatz (MV-PC) einschließlich der für einen wirtschaftlichen Betrieb notwendigen Dienstleistungen zu definieren. Dieser Basisdienst sollte verbindlich allen Landesbehörden von der DVZ M-V GmbH bereitgestellt werden.	Drs. 7/4162 mit Bezug auf **LFB 2019** Tz. 163	nicht umgesetzt
	Regulierung (Informationssicherheitsmanagement)	Hinsichtlich der Informationssicherheit sollte die DVZ M- GmbH auf den Grundschutz des BSI verpflichtet werden, da es bisher an einer solchen Verpflichtung fehlt.	Drs. 7/4162, mit Bezug auf **LFB 2019** Tzn. 111 – 115	nicht umgesetzt
2020	E-Government	Die Landesregierung wird aufgefordert, eine Digitalisierungsstrategie sowie eine IT-Strategie nach dem Vorbild des Bundes und der Mehrzahl der Länder zu erarbeiten und dem Ausschuss für Energie, Infrastruktur und Digitalisierung sowie dem Finanzausschuss bis zum 1. Mai 2021 für beide Strategien einen ersten Entwurf vorzulegen.	Drs. 7/5579, Ziff. I 5 mit Bezug auf **LFB 2020** Tzn. 102 – 105	nicht umgesetzt
	E-Government	Die Landesregierung wird gebeten, zeitnah ein neues Personalkonzept zu erarbeiten. Das Personalkonzept sollte insbesondere folgende Bestandteile umfassen: ... c) die Berücksichtigung eines temporären Mehraufwands für die Digitalisierung der Verwaltung und d) die Berücksichtigung der Auswirkungen der Digitalisierung auf die mittel-und langfristige Stellenentwicklung sowie auf Aus-und Fortbildung	Drs. 7/5579, Ziff. I 3 mit Bezug auf **LFB 2020** Tzn. 152 – 206	nicht umgesetzt
	E-Government (GPO)	Die Landesregierung wird aufgefordert, vorrangig IT-Projekte umzusetzen, die eine digitale Rendite bei Ressourceneinsatz und/oder Leistungserbringung in Form freiwerdender personeller und/oder sachlicher Ressourcen oder verbesserter Leistungserbringung erwarten lassen.	Drs. 7/5579, Ziff. I 6 mit Bezug auf **LFB 2020** Tzn. 207 – 210	nicht umgesetzt

	E-Government / IT-Controlling	Die Landesregierung wird aufgefordert, jährlich zum 31. Dezember, beginnend 2021, über die Fortschritte bei der Digitalisierung und über die Entwicklung der IT-Gesamtkosten schriftlich zu berichten.	Drs. 7/5579, Ziff. I 5 mit Bezug auf **LFB 2020** Tzn. 152 – 206	umgesetzt
	E-Government / OZG	Die Landesregierung wird aufgefordert, die Ressorts zur Erstellung von Zeit-, Kapazitäts- und Budgetplänen für die Umsetzung von Onlinezugangsgesetz-Leistungen (OZG-Leistungen) und zur Schaffung der haushaltsrechtlichen Voraussetzungen für deren Umsetzung zu verpflichten. Die Ressorts sind ebenso dazu anzuhalten, sich hinsichtlich des Umsetzungsstandes in den Kommunen einen Überblick zu verschaffen und auf die Entwicklung landeseinheitlicher Lösungen auf kommunaler Ebene hinzuwirken.	Drs. 7/5579, Ziff. I 7 mit Bezug auf **LFB 2020** Tzn. 231 – 250	teilweise umgesetzt
	E-Government / OZG	Das Energieministerium wird gebeten, die Empfehlungen des Landesrechnungshofes bezüglich der Umsetzung des Onlinezugangsgesetzes in den Landkreisen, kreisfreien Städten und großen kreisangehörigen Städten bei der laufenden Entwicklung eines Programmmanagements zu berücksichtigen und dabei insbesondere eine bessere Steuerung und Koordinierung anzustreben. Generelles Ziel sollte eine landesweit einheitliche Vorgehensweise und mindestens das Erreichen des Reifegrades 3 bei der Umsetzung des Onlinezugangsgesetzes sein.	Drs. 7/5922 mit Bezug auf **KFB 2020** Tzn. 164 – 196	teilweise umgesetzt
2022	Regulierung (Informationssicherheitsgesetz)	Der Landtag hatte das Energieministerium gebeten, die Notwendigkeit eines Informationssicherheitsgesetzes zu prüfen.	Drs. 7/4162 mit Bezug auf **LFB 2019** Tzn. 90 – 107	nicht umgesetzt
	Regulierung	Der Landtag hatte das Energieministerium gebeten, IT-Standards landesweit verbindlich festzulegen.	Drs 8/1533 mit Bezug auf **LFB 2019** Tzn. 90 – 107	nicht umgesetzt
	Technologie und Architektur (Open Source)	Der Landtag hatte das Energieministerium gebeten, die Abhängigkeit der Landesverwaltung von Softwareanbietern zu untersuchen, daraus resultierende Risiken zu bewerten sowie die Möglichkeiten einer stärkeren Nutzung von Open Source-Lösungen zu prüfen und dem Ausschuss für Energie, Infrastruktur und Digitalisierung sowie dem Finanzausschuss bis zum 31. Dezember 2021 schriftlich über die Ergebnisse zu berichten.	Drs 8/1533 mit Bezug auf **LFB 2020** Tzn. 127 – 151	nicht umgesetzt

Anlage 2: Empfehlungen des Landesrechnungshofes und Umsetzungsstand

Jahr	Themenfeld	Empfehlung	Quelle	Umsetzung
2011	Regulierung (Standards)	Das Innenministerium sollte bei der Definition der Standards übergreifende und bereits vorhandene eGovernment-Standards, wie beispielsweise den für Bundesbehörden bindenden SAGA, mit einfließen lassen.	Bezug auf **LFB 2011** Tz. 126	nicht umgesetzt
	Organisation (IT-Controlling)	Das Innenministerium sollte eine ressortübergreifende IT-Steuerung und Koordinierung in einer separaten Organisationseinheit bündeln.	Bezug auf **LFB 2011** Tz. 140	teilweise umgesetzt
2012	Informationssicherheit und Datenschutz (Risikomanagement)	Das Innenministerium sollte Risiken systematisch erfassen, bewerten und zuordnen.	Bezug auf **LFB 2012** Tz. 206	teilweise umgesetzt
	Organisation (IT-Management)	Das Innenministerium sollte in Situationen, in denen keine umfassenden Tests möglich sind, für jede einzelne Änderung eine umfassende Risikobewertung durchführen	Bezug auf **LFB 2012** Tz. 213	teilweise umgesetzt
	Haushalt (Wirtschaftlichkeitsuntersuchungen)	Die Landesregierung sollte Aufgaben und Zuständigkeiten insbesondere bei der Prüfung der Notwendigkeit und Wirtschaftlichkeit von IT-Projekten regeln.	Bezug auf **LFB 2012** Tz. 225	umgesetzt
	Organisation (IT-Controlling)	Innenministerium und Finanzministerium sollten die Ziele, Aufgaben und Verantwortlichkeiten des strategischen und operativen IT-Controllings klar definieren und in dem entsprechenden Regelwerk eindeutig und verbindlich festlegen.	Bezug auf **LFB 2012** Tz. 234	teilweise umgesetzt
	Haushalt (Wirtschaftlichkeitsuntersuchungen)	Die Dienststellen der Landesverwaltung sollten die haushaltsrechtlichen Vorschriften und Verfahrensvorschriften konsequent einhalten. Das Innenministerium sollte den Nachweis der Notwendigkeit und das Vorhandensein einer plausiblen Wirtschaftlichkeitsuntersuchung im Rahmen der Haushaltsanmeldung bzw. der Projektfreigabe überprüfen.	Bezug auf **LFB 2012** Tz. 237	teilweise umgesetzt
2013	Anforderungsmanagement (Anforderungsmanagement)	Das Innenministerium sollte fachliche Anforderungen unabhängig vom IT-Grundsystem als Maßstab zur Auswahl von Ausstattungsgegenständen nutzen.	Bezug auf **LFB 2013** Tz. 198	teilweise umgesetzt
2014	Organisation (IT-Controlling)	Das Innenministerium sollte ein umfassendes und leistungsfähiges IT-Controlling einführen.	Bezug auf **LFB 2014** Tz. 250	nicht umgesetzt
	Organisation (IT-Controlling)	Das Innenministerium sollte in Abstimmung mit dem Finanzministerium - wie im Masterplan 2011 vorgesehen - ein Konzept zur Neufassung und Neustrukturierung des IT-Controllings erarbeiten.	Bezug auf **LFB 2014** Tz. 253	nicht umgesetzt
2015	Arbeitnehmerüberlassung	Die Landesregierung sollte klare Kriterien festlegen, welche Aufgaben für eine Auslagerung in Betracht kommen und welche nicht.	Bezug auf **LFB 2015** Tz. 138	teilweise umgesetzt

Jahr	Themenfeld	Empfehlung	Quelle	Umsetzung
	Regulierung (Standards)	Das Innenministerium sollte ergänzend zu den bestehenden Regelungen einheitliche IT-Standards für die Landesverwaltung verbindlich definieren.	Bezug auf **LFB 2015** Tz. 153	teilweise umgesetzt
	Haushalt (Vertragsgestaltung)	Das Bildungsministerium sollte EVB-IT Verträge verwenden.	Bezug auf **LFB 2015** Tz. 271	teilweise umgesetzt
	Informationssicherheit und Datenschutz (Informationssicherheitsmanagement)	Das LUNG sollte eine behördenspezifische IT-Sicherheitsrichtlinie erlassen und einen IT-Sicherheitsbeauftragten und seinen Vertreter benennen. Die Sicherheitskonzepte des LUNG sollten auf Basis des IT-Grundschutzes des Bundesamtes für Sicherheit in der Informationstechnik (BSI) systematisch überprüft werden. Regelmäßige Sicherheitsrevisionen zur Überprüfung der Wirksamkeit der IT-Sicherheitsmaßnahmen sollten durchgeführt und dokumentiert werden.	Bezug auf **LFB 2015** Tz. 349	teilweise umgesetzt
	Informationssicherheit und Datenschutz, IT-Organisation	Das LUNG sollte für seinen Informationsverbund eigene Sicherheitskonzepte erstellen. Das LUNG sollte Informationssicherheits-Revisionen durchführen Das LUNG sollte durch ein Informationssicherheitsmanagementsystem als kontinuierlichen Verbesserungsprozess sicherstellen, dass Schwachstellen in der Informationssicherheit aufgrund von technischen oder organisatorischen Veränderungen rechtzeitig erkannt und behoben werden.	Bezug auf **LFB 2015** Tzn. 320 – 351	teilweise umgesetzt
2019	Regulierung (Standards)	Der Landesrechnungshof empfiehlt, gesetzliche Regelungen zur Informationssicherheit in einem Informationssicherheitsgesetz zu regeln, um die Funktionsfähigkeit der öffentlichen Verwaltung, die von den Bürgern auf den IT-Systemen des Landes gespeicherten Daten sowie die Vertraulichkeit der Kommunikation zwischen Bürger und Staat sowie zwischen Behörden und Einrichtungen der Landes- und Kommunalverwaltung zu schützen.	Bezug auf **LFB 2019** Tzn. 90 – 107	nicht umgesetzt
	Regulierung (Standards)	Bevor das Energieministerium Standards und Basisdienste verbindlich festlegt, sollte es prüfen, ob die Anforderungen der EU-Datenschutz-Grundverordnung und des BSI-Grundschutzes eingehalten werden. In die IT-Richtlinie sollten Regelungen aufgenommen werden, die sicherstellen, dass die o. g. Anforderungen aus dem Vergabe-, Haushalts-, Datenschutz- und Informationssicherheitsrecht umgesetzt werden.	Bezug auf **LFB 2019** Tzn. 98 – 100	teilweise umgesetzt
	Regulierung (Standards)	Das Energieministerium sollte zeitnah das E-Government-Gesetz überarbeiten. Die Landesregierung sollte prüfen, ob ein Informationssicherheitsgesetz notwendig ist und gegebenenfalls darauf hinwirken, dass das Energieministerium den Entwurf eines IT-Sicherheitsgesetzes erarbeitet.	Bezug auf **LFB 2019** Tzn. 104 – 107	teilweise umgesetzt
	Regulierung (DSGVO)	Die Landesregierung sollte prüfen, ob die erforderlichen Festlegungen gemäß Art. 28 DS-GVO, wie z. B. die Verpflichtung der DVZ M-V GmbH, Überprüfungen und Inspektionen zu dulden oder daran mitzuwirken, im DVZG M-V geregelt werden können.	Bezug auf **LFB 2019** Tzn. 109 – 113	nicht umgesetzt

Jahr	Themenfeld	Empfehlung	Quelle	Umsetzung
	Informationssicherheit und Datenschutz, IT-Organisation, Regulierung	Die Erfahrungen des LAF hinsichtlich der Gewährleistung von Informations- und Kassensicherheit sollten ressortübergreifend nutzbar gemacht werden. Finanzministerium und Energieministerium sollten auf eine Nachnutzbarkeit bewährter Lösungen hinwirken.	Bezug auf **LFB 2019** Tzn. 267 – 303	teilweise umgesetzt
	Informationssicherheit und Datenschutz, Organisation	Der Landesrechnungshof hatte empfohlen, die Auflagen aus der Zertifizierung der durch das LAF betriebenen Scanstrecke zeitnah zu erfüllen. Sie sind zur Aufrechterhaltung der Zertifizierung notwendig. Das LAF sollte prüfen, welche Zusatzmaßnahmen zur Übertragung von Daten mit einem höheren Schutzbedarf ergriffen werden müssen.	Bezug auf **LFB 2019** Tzn. 267 – 303	umgesetzt
	Anforderungsmanagement, Haushalt	Die interne Revision des LAF sollte regelmäßige Prüfungen zur Informationssicherheit und der Informationstechnologie (IS- und IT-Revisionen) durchführen.	Bezug auf **LFB 2019** Tzn. 267 – 303	umgesetzt
2020	Regulierung (Standards)	Damit die IT-Landesstandards als Grundlage für Leistungsbeschreibungen bei öffentlichen Auftragsvergaben herangezogen werden können, sollten sie nicht auf bestimmte Produkte, Marken, Erzeugnisse und Verfahren verweisen. Die gem. §§ 11 Abs. 2 und 15 Abs. 1 EGovG M-V festzulegenden Standards sind für den jeweiligen Nutzerkreis verbindlich vorzugeben.	Bezug auf **LFB 2020** Tz. 164 – 175	nicht umgesetzt
	E-Government (GPO)	Der Landesrechnungshof empfiehlt, vorrangig IT-Projekte umzusetzen, bei denen eine digitale Rendite in Form freigesetzter Stellen zu erwarten ist. Die Wirtschaftlichkeit der IT-Projekte muss gewährleistet werden. Die deutlich gesteigerten IT-Ausgaben müssen dazu genutzt werden, den Anstieg der Personalausgaben zu begrenzen. Die Effizienz des IT-Einsatzes sollte im Rahmen eines IT-Controllings nachgehalten werden.	Bezug auf **LFB 2020** Tz. 200 – 211	nicht umgesetzt
	Haushalt (IT-Ausgaben)	Steigende IT-Ausgaben sollten nicht akzeptiert werden, ohne sie zu hinterfragen. Vielmehr sollten sie mittelfristig durch Einsparungen aufgrund einer optimierten IT-gestützten Aufgabenerfüllung gegenfinanziert werden. Dafür sollte die Landesverwaltung eine Strategie entwickeln.	Bezug auf **LFB 2020** Tzn. 200 – 230	nicht umgesetzt
	E-Government (Datenschutz)	Der Landesrechnungshof hatte das Innenministerium aufgefordert, die Verwaltungspraxis der Sammelverfügungen gänzlich aufzugeben.	Bezug auf **LFB 2020** Tzn. 791 – 838	umgesetzt
2021	Informationssicherheit und Datenschutz, Organisation, Regulierung	Das Energieministerium sollte eine gesetzliche Regelung zur Anwendung/Umsetzung der BSI-Bausteine zum Outsourcing initiieren.	Bezug auf **LFB 2021** Tz. 434	nicht umgesetzt

Jahr	Themenfeld	Empfehlung	Quelle	Umsetzung
	Haushalt (Vergabe)	Das LAiV sollte prüfen, ob es zukünftig auch Standardhard- und -software sowie weitere Fachverfahrenslösungen beschaffen könnte. Doppelstrukturen bei den Warenkörben der DVZ M-V GmbH und des LAiV sollten beseitigt werden.	Bezug auf **LFB 2021** Tzn. 274 – 301	nicht umgesetzt
	Organisation (Personalkonzept)	Das Energieministerium sollte bisher getroffene Organisationsentscheidungen überprüfen und regelmäßige und anlassbezogene Organisationsuntersuchungen durchführen.	Bezug auf **LFB 2021** Tzn. 361 – 364	nicht umgesetzt
	E-Government (Regelung)	Der Landesrechnungshof hatte **gefordert**, dass das LAiV bis zur Einführung elektronischer Akten revisionssichere Akten in Papierform führt.	Bezug auf **LFB 2021** Tzn. 274 – 301	nicht umgesetzt
	E-Government (Regelung)	Der Landesrechnungshof empfiehlt weiterhin, den Vergabemarktplatz M-V und den AIVergabeManager „light“ zu Basiskomponenten im Sinne des E-Government-Gesetzes M-V zu erklären. Die Dienststellen und Behörden der unmittelbaren Landesverwaltung sollten zu deren Anwendung verpflichtet werden.	Bezug auf **LFB 2021** Tzn. 274 – 301	nicht umgesetzt
	E-Government (Regelungen)	Der Landesrechnungshof hatte dem Innenministerium in Bezug auf die Weiterentwicklung und Pflege der dem eShop zugrundeliegenden Software empfohlen: • sicherzustellen, dass auch Externe oder zumindest mehrere Mitarbeiter in der Lage sind, die Software zu pflegen • zu prüfen, ob die Dokumentation der Veränderungen am Quellcode den Anforderungen genügt • festzulegen nach welchen Regeln und welchem Prozess die Freigabe von Änderungen an der Software erfolgt	Bezug auf **LFB 2021** Tzn. 274 – 301	nicht umgesetzt
	E-Government (Standards)	Die Landesregierung hat mit hoher Priorität alle notwendigen Maßnahmen zu ergreifen, um die Rechtmäßigkeit der Verarbeitung personenbezogener Daten sicherzustellen. Sie hat zu analysieren und zu dokumentieren, welche Betriebssysteme, Anwendungen und Dienste auf welcher Rechtsgrundlage personenbezogene Daten in welche Drittländer übermitteln. Die Landesregierung sollte ein ressortübergreifendes Konzept entwickeln, wie die Rechtsprechung des EuGH umgesetzt werden soll. Bei den für die Landesverwaltung festzulegenden IT-Architekturen und IT-Standards ist digitale Souveränität sicherzustellen. Bei bestehenden nicht datenschutzkonformen IT-Lösungen sind terminierte Migrationspläne zur Ablösung verbindlich zu beschließen. Hierzu zählt auch die Ablösung der derzeitigen Videokonferenzlösung.	Bezug auf **LFB 2021** Tzn. 79 – 88	nicht umgesetzt
2023	E-Government, Informationssicherheit und Datenschutz, Technologie und Architektur (Fachverfahrensstrategie)	Die Behörden sollten regelmäßig die Risiken beim Betrieb von Fachverfahren betrachten und die Wirtschaftlichkeit feststellen. Je älter das Verfahren, desto intensiver muss dies erfolgen. Ablösebedarfe sind systematisch zu ermitteln und rechtzeitig dem ZDMV anzuzeigen. Die Vorschläge des Landesrechnungshofes gelten für eine Vielfalt an möglichen Fachverfahren. Es ist jeweils die an den Anforderungen der Fachaufgabe ausgerichtete wirtschaftlichste	Bezug auf **LFB 2023** Tzn. 151 – 183	nicht umgesetzt

Jahr	Themenfeld	Empfehlung	Quelle	Umsetzung
		und zweckmäßigste Vorgehensweise auszuwählen.		
	Regulierung (Standards)	Das Innenministerium sollte prüfen, ob die Regelung im DVZG M-V zur Beschaffung auf Grundlage des veralteten IT-Strukturrahmens noch zweckmäßig ist. Alternativ sollte es regeln, wie die Landesverwaltung zukünftig die Vorgaben für die Beschaffungen der DVZ M-V GmbH festlegt. Sollte die Regelung beibehalten werden, ist der ITSR M-V sofort und regelmäßig zu aktualisieren	Bezug auf **LFB 2023** Tzn. 540 – 543	nicht umgesetzt

Glossar

Aufgabenkritik

Unter Aufgabenkritik versteht man die Überprüfung einer von der öffentlichen Verwaltung bislang wahrgenommenen Aufgabe unter der Fragestellung,

- ob die Aufgabe überhaupt, teilweise oder gar nicht (mehr) wahrgenommen werden muss und
- ob die Art der Aufgabenwahrnehmung sachgerecht und wirtschaftlich ist

Betriebsstandard

Betriebsstandard meint Normen und Standards für die Architektur von Fachverfahren, die einen einheitlichen Betrieb in Rechenzentren ermöglichen.

CERT

CERT steht für Computer Emergency Response Team. Dabei handelt es sich um ein Team von Experten, die sich mit Sicherheitsvorfällen im Bereich der Computer und Netzwerke beschäftigten.

Cyberresilenz

Fähigkeit einer Organisation, schnell und effektiv bei Angriffen auf Hardware, Software oder Daten der Organisation reagieren zu können. Zur Cyberresilenz gehört auch die Fähigkeit, den Betrieb nach einem solchen Angriff fortsetzen zu können.

Datenmodelle

Datenmodelle beschreiben alle für den Ablauf des Geschäftsprozesses bzw. eines Prozessschrittes notwendigen Daten. Dies sollte standardisiert z. B. nach den Vorgaben des Föderalen Informationsmanagements für Datenfelder vorgenommen werden. Neben der semantischen Beschreibung sollten auch technisch notwendige Anforderungen wie z. B. Dateiformate festgelegt werden.

Datenformate

Datenformate sind standardisierte Strukturen, die bestimmen, wie Informationen gespeichert und verarbeitet werden. Sie ermöglichen es, Daten effizient zwischen verschiedenen Systemen und Anwendungen auszutauschen und zu verstehen. Zu den bekanntesten Datenformaten zählen XML, JSON und CSV, die jeweils spezielle Einsatzgebiete und Vorzüge bieten.
Eine Unterform von Datenformaten sind Dateiformate. Beim Dateiformat handelt es sich um eine bestimmte Codierung der Datei, die verschiedene Informationen enthält, damit die Datei von einem geeigneten Programm geöffnet und verarbeitet werden kann.

Deutsche Verwaltungscloud	Die Deutsche Verwaltungscloud (DVC) ist eine Initiative der Bundesregierung, die darauf abzielt, eine sichere und interoperable Cloud-Infrastruktur für die öffentliche Verwaltung zu schaffen. Sie basiert auf dem Open Source-Projekt „Sovereign Cloud Stack“ als technischem Unterbau. Vgl. Landesrechnungshof Mecklenburg-Vorpommern (2023): Jahresbericht 2023 (Teil 1) – Landesfinanzbericht 2023, S. 42.
Digitale Souveränität	Digitale Souveränität beschreibt die Fähigkeit von Einzelpersonen und Organisationen, ihre Rolle(n) in der digitalen Welt unabhängig, autonom und selbstbestimmt auszuüben. Sie sichert Handlungsmöglichkeiten und Entscheidungskompetenzen im digitalen Raum. Außerdem leistet digitale Souveränität einen Beitrag, Daten, Informationen und digitale Identitäten zu kontrollieren und zu schützen.
Digitalisierungsstrategie	Eine Digitalisierungsstrategie beschreibt, wie Prozesse und Dienstleistungen des Staates durch digitale Technologien verbessert und modernisiert werden sollen. Sie umfasst Aspekte wie z. B. die Digitalisierung von Verwaltungsabläufen, die Bereitstellung digitaler Dienstleistungen sowie die Förderung von Innovation.
Distributed-Denial-of-Service (DDoS)-Angriff	Ein Distributed Denial-of-Service (DDoS)-Angriff ist ein böswilliger Versuch, den normalen Datenverkehr zu einer Webressource zu stören. Dabei wird das Ziel mit Anfragen überflutet, um es unzugänglich zu machen.
Dunkelverarbeitung	Geschäftsprozesse, die vollständig IT-gestützt automatisiert im Hintergrund ablaufen, ohne dass eine menschliche Interaktion notwendig ist.
EfA: Einer für alle	Mit dem "Einer für Alle" (EfA)-Prinzip wurde eine nachhaltige, arbeitsteilige Arbeitsstruktur für die interföderale Zusammenarbeit etabliert. Digitale Lösungen, die der Bund oder ein Bundesland entwickelt haben, können nachgenutzt werden.
Fachverfahren	Eine allgemein anerkannte Definition für Fachverfahren existiert nicht. Der Landesrechnungshof definiert Fachverfahren als technische Informationssysteme, mit deren Hilfe eine i. d. R. durch Gesetz oder Rechtsverordnung bestimmte Fachaufgabe von einer Fachbehörde in ihrem Zuständigkeitsbereich wahrgenommen wird.
Geschäftsprozessoptimierung	Systematische Analyse und Verbesserung der Verwaltungsprozesse. Ziel ist es, die Effizienz und Effektivität zu erhöhen und die Qualität der Prozessergebnisse zu verbessern.

IS-Penetrationstest

Ein IS-Penetrationstest ist ein Vorgehensmodell, um das Angriffspotenzial auf ein IT-Netz, ein einzelnes IT-System oder eine (Web-)Anwendung festzustellen. Dabei werden die Erfolgsaussichten eines vorsätzlichen Angriffs auf einen Informationsverbund oder ein einzelnes IT-System eingeschätzt und daraus notwendige ergänzende Sicherheitsmaßnahmen abgeleitet beziehungsweise die Wirksamkeit von bereits umgesetzten Sicherheitsmaßnahmen überprüft.

IS-Webcheck

Der IS-Webcheck als eine spezielle Variante des IS-Penetrationstests, bei der die Absicherung von Webanwendungen überprüft wird.

IT-Architektur

Die IT-Architektur beschreibt die Gesamtheit der technischen Aspekte der Informationstechnologie in einer Organisation. Sie legt die Grundstrukturen fest und definiert Regeln und Standards, die das dynamische Zusammenspiel der verschiedenen IT-Komponenten steuern (Anwendungen, Daten, Infrastruktur, Sicherheitsarchitektur).

IT-Controlling

IT-Controlling umfasst Prozesse und Methoden um sicherzustellen, dass IT-Projekte im Einklang mit den festgelegten Zielen, Budgets und Zeitplänen durchgeführt werden. Hierzu zählen die Planung, Überwachung und Steuerung aller Aktivitäten, die sich auf den Einsatz der Informationstechnik in der Landesverwaltung beziehen.
Durch das IT-Controlling ist sicherzustellen, dass die Formalziele Effizienz und Effektivität sowie die Sachziele Qualität, Funktionalität und Termineinhaltung erreicht werden. Die Formal- und Sachziele ergeben sich aus den Strategien der Landesregierung.
Das IT-Controlling soll die Fragen beantworten:

- Ist der IT-Einsatz effektiv, d. h. unterstützen die eingesetzten Informationssysteme die Ziele der Landesverwaltung?
- Ist der Einsatz der IT effizient, d. h. kostengünstig und wirtschaftlich?

IT-Controlling, operativ

Das operative IT-Controlling bezieht sich auf die systematische Überwachung und Steuerung des Einsatzes der IT in der Landesverwaltung. Hierzu zählen insbesondere

- die Überwachung der IT-Ausgaben hinsichtlich der Budgeteinhaltung und der Wirtschaftlichkeit,
- die Leistungsbewertung (Effizienz und Effektivität der IT-Systeme und IT-Prozesse) einschließlich der Bewertung von Verbesserungsmöglichkeiten,
- die Berichterstattung über IT-Leistung und IT-Ausgaben, um fundierte Entscheidungen zu ermöglichen.

IT-Controlling, strategisch

Das strategische IT-Controlling bezieht sich auf die langfristige Planung und Steuerung des Einsatzes von IT in der Landesverwaltung. Hierzu zählen

- eine zukunftsorientierte Planung,
- die Verbesserung der Effektivität des IT-Einsatzes und
- die Unterstützung der Entscheidungsprozesse durch Bereitstellung von Informationen und Analysen.

IT-Landesstandard

IT-Landesstandards sind grundlegende Techniken (Protokolle, Schnittstellen, Daten-und Austauschformate) und konkrete funktionale Anforderungen im Sinne der Vereinheitlichung und Kompatibilität der Informationstechnik. Sie sind gem. § 15 Abs. 2 EGovG M-V durch die für Digitalisierung zuständige oberste Landesbehörde festzulegen.

IT-Risikomanagement

IT-Risikomanagement ist ein systematischer Prozess, um Risiken des IT-Einsatzes zu identifizieren, zu bewerten und zu steuern. Im Ergebnis sind Maßnahmen festzulegen, um die identifizierten Risiken zu vermeiden oder zu mindern. Außerdem sollte es Aussagen treffen, in wieweit nicht vermeidbare oder verminderbare Risiken akzeptiert werden.

IT-Standard

Ein IT-Standard ist eine vereinheitlichte und allgemein anerkannte Methode, wie Produkte oder Verfahren in der Informationstechnologie hergestellt, dokumentiert oder ausgeführt werden.
Ein Standard setzt voraus, dass die grundlegende Technik in einem Standardisierungsprozess durch eine Standardisierungsorganisation als Standard empfohlen wird und sich die Nutzer auf deren Anwendung verbindlich einigen bzw. seine Anwendung verbindlich vorgegeben wird. Anwendungssoftware bestimmter Hersteller sind keine Standards. Vgl. Landesrechnungshof Mecklenburg-Vorpommern (2020): Jahresbericht 2020 (Teil 1) – Landesfinanzbericht 2020, Tz. 171.

IT-Standard, föderal (FIT-Standards)

Vom IT-Planungsrat festgelegte IT-Interoperabilitäts- und IT-Sicherheitsstandards. Die FIT-Standards können vom IT-Planungsrat als verbindlich beschlossen werden. Im Übrigen ist ihre Anwendung empfohlen.

IT-Strategie

Eine IT-Strategie beschreibt, wie Informationstechnologie eingesetzt werden soll, um die übergeordneten Ziele einer Behörde, eines Geschäftsbereichs oder der Landesregierung zu erreichen.

Lebenszyklus

Lebenszyklus beschreibt die Phasen, die ein Vertrag bzw. Hard- und Software während ihrer gesamten Nutzungsdauer durchlaufen. Hierzu zählen Planung, Beschaffung, Betrieb, Wartung und Stilllegung. Hardware und Soft-

ware(lizenzen) können während ihres Lebenszyklus in einem IT-Life-Cycle-Management-System und Verträge in einem Vertragsmanagementsystem verwaltet werden.

Low-Code

Low-Code ist eine Methode der Anwendungsentwicklung, bei der das Programmieren nicht mehr auf der Basis von Textzeilen, sondern mit visuellen Hilfsmitteln erfolgt. Anstatt in einer technischen Programmierumgebung arbeitet Low-Code mit einer modellgesteuerten Drag-and-Drop-Oberfläche. Die Kenntnis einer Programmiersprache ist nicht notwendig.

Monolithisches Fachverfahren

Eine monolithische Software-Architektur ist meistens als ein einziges großes System konzipiert und basiert auf genau einem Quellcode. Als eigenständige Software entworfen, wird sie im Ganzen bereitgestellt. Die Komponenten des Programms sind dabei miteinander verbunden und voneinander abhängig; dies bedeutet, dass bei Änderungen von Details die ganze Architektur bearbeitet werden muss.

Multicloudstrategie

Von Multicloud spricht man, wenn ein Unternehmen Cloud-Computing-Dienste von mindestens zwei Cloud-Anbietern nutzt, um seine Anwendungen auszuführen. Anstatt einen einzelnen Cloud-Stack zu verwenden, umfassen Multicloud-Umgebungen normalerweise eine Kombination aus zwei oder mehr öffentlichen Clouds, zwei oder mehr privaten Clouds oder eine Kombination aus beiden.

MV-Beratung

Die MV-Beratung ist ein Referat in der Abteilung 5 des Finanzministeriums. Sie soll ressortübergreifend Fachministerien sowie nachgeordnete Behörden und Landesgesellschaften der Landesverwaltung in den Themenbereichen Projektmanagement, Prozessanalyse und Prozessoptimierung sowie Organisationsberatung beraten.

Normen

Organisatorische, fachliche und technische Vorgaben mit allgemeingültigem Charakter für ein bestimmtes Anwendungsgebiet, die von anerkannten Normungsorganisationen erarbeitet und national als DIN oder international als ISO verbindlich verabschiedet wurden (Organisationskonzept elektronische Verwaltungsarbeit, Baustein E-Akte, www.verwaltung-innovativ.de/SharedDocs/Publikationen/Organisation,S. 17).
Von einer anerkannten Normungsorganisation (national, europäisch oder international) angenommene technische Spezifikation zur wiederholten oder ständigen Anwendung, deren Einhaltung nicht zwingend ist (Art. 2 Nr. 1 Verordnung (EU) Nr. 1025/2012, Anlage 1 zu § 31 Absatz 2 VgV).
Anerkannte Normungsgremien auf europäischer Ebene: Europäisches Komitee für Normung (CEN), Europäisches

	Komitee für Elektrotechnische Normung (CENELEC) und Europäisches Institut für Telekommunikationsstandard (ETSI) Nationale deutsche Normierungsgremien: Deutsches Institut für Normung e. V. (DIN) und Deutsche Elektrotechnische Kommission .
nicht-proprietäre Protokolle, Schnittstellen und Datenformate	Protokolle, Schnittstellen und Formate werden als „nicht-proprietär“ oder „offen“ bezeichnet, wenn sie frei von rechtlichen und technischen Einschränkungen verwendet werden können. Sie können unabhängig von einzelnen Anbietern durch Dritte geprüft und weiterentwickelt werden. Sie sind frei verfügbar.
NIS-2-Richtlinie	EU-Richtlinie, die das Niveau der Cyberresilienz in der Union stärken soll. Die Richtlinie soll ein hohes gemeinsames Sicherheitsniveau für Netzwerke und Informationssysteme schaffen. Sie legt Kriterien fest, um Betreiber kritischer Infrastrukturen zu identifizieren. Für diese kritischen Infrastrukturen definiert sie Mindeststandards für Sicherheitsmaßnahmen.
openDesk	OpenDesk umfasst Büroanwendungen z. B. zum Erstellen von Texten oder Tabellenkalkulationen und für die Zusammenarbeit. OpenDesk basiert auf Open Source.
open Source	Open Source bezieht sich auf Software, deren Quellcode öffentlich zugänglich ist. Dies bedeutet, dass jeder den Code einsehen, modifizieren und verteilen kann.
Outsourcing	Beim Outsourcing lagern Behörden Geschäftsprozesse oder Tätigkeiten ganz oder teilweise zu einem oder mehreren externen Dienstleistungsunternehmen aus. Outsourcing kann die Nutzung und den Betrieb von Hard- und Software betreffen. Die Leistung kann in den Räumlichkeiten der Auftraggebenden oder in einer externen Betriebsstätte der Anbietenden von Outsourcing erbracht werden. Typische Beispiele des klassischen "IT-Outsourcings" sind der Betrieb eines Rechenzentrums, einer Anwendung oder einer Webseite. Die Verantwortung aus Sicht der Informationssicherheit verbleibt stets bei der auslagernden Institution.
privacy by design	Das Prinzip privacy by design ist in der Datenschutzgrundverordnung, insbesondere Art. 25 „Datenschutz durch Technikgestaltung“ verankert. Datenschutzaspekte sind bereits bei der Entwicklung von Hard- und Software sowie Diensten zu berücksichtigen.

Produktneutralität	Bei der Vergabe öffentlicher Aufträge dürfen in Leistungsbeschreibungen grundsätzlich keine spezifischen Produkte, Marken oder Anbieter genannt werden.
Proprietäre Protokolle, Schnittstellen und Datenformate	Protokolle, Schnittstellen und Formate werden als „proprietär" bezeichnet, wenn sie nicht oder nur mit Schwierigkeiten von Dritten implementierbar sind. Sie befinden sich im Eigentum von Einzelpersonen oder Organisationen und sind durch Patente, Urheberrecht oder Lizenzbedingungen geschützt. Technische Einzelheiten sind nicht veröffentlicht. Die Nutzung durch andere ist in der Regel nur über kostenpflichtige Lizenzen möglich ist.
Protokolle	Ein Protokoll in der Informationstechnologie ist eine definierte Vereinbarung über die Art und Weise des Informationsaustausches zwischen zwei oder mehreren Systemen. Es legt Regeln, Formate und Parameter fest, die für eine vollständige, fehlerfreie und effektive Datenübertragung notwendig sind. Es ist eine Unterform eines IT-Standards für den Bereich Informationsaustausch.
Ransomware	Spezielle Art von Schadsoftware, die den Zugriff auf persönliche Daten der Systeme des Opfers so lange blockiert, bis ein Lösegeld gezahlt wird.
Ressortprinzip	Verfassungsrechtliches Prinzip der Regierungsorganisation. Jede Ministerin/jeder Minister leitet ihren/seinen Geschäftsbereich eigenverantwortlich im Rahmen der von der Ministerpräsidentin/dem Ministerpräsidenten vorgegebenen Richtlinien.
Schnittstelle(n)	Eine Schnittstelle ist ein definierter Punkt der Interaktion zwischen zwei oder mehreren Systemen oder Komponenten, über den Daten oder Informationen ausgetauscht werden. Sofern als Standard anerkannt oder als Norm beschlossen, gewährleisten sie die Kompatibilität von Hard- und Software. *Hardwareschnittstellen* ermöglichen die physische Verbindung zwischen Geräten. *Softwareschnittstellen* ermöglichen den Austausch von Daten und Befehlen zwischen verschiedenen Softwareanwendungen oder -modulen. *Benutzerschnittstellen* stellen die Verbindung zwischen dem Benutzer und einem System her. Hierzu gehören z. B. grafische Benutzeroberflächen und Bedienelemente. Eine Vereinheitlichung fördert die Nutzerfreundlichkeit. Die Benutzerschnittstelle muss zudem Barrierefreiheit gewährleisten.
Schwachstellenanalyse(n)	Die Schwachstellenanalyse ist eine besondere Form des IS-Penetrationstests, bei der keine manuellen Prüfungen

vorgenommen werden. Es wird im Unterschied zum Penetrationstest nicht simuliert, wie die erkannten Schwachstellen ausgenutzt werden können.

Schwellenbereich

Im öffentlichen Auftragswesen gibt es Schwellenwerte, die bestimmen, welche Verfahren bei der Vergabe von Aufträgen durchgeführt werden müssen. Der Schwellenwert, bei dessen Überschreiten europäisches Vergaberecht angewendet werden muss, wird als „Oberschwellenbereich" bezeichnet. Unterhalb des Oberschwellenwertes (Unterschwellenbereich) gelten die haushalts- und vergaberechtlichen Regelungen des Landes Mecklenburg-Vorpommern.

security by design

Security by design zielt darauf ab, die Sicherheit von Hard- und Software während des gesamten Lebenszyklus eines Produkts zu gewährleisten. Sicherheitsaspekte sind bereits in der Entwicklungsphase des Produkts zu berücksichtigen. Das Produkt ist so widerstandsfähig wie möglich gegen Angriffe zu gestalten.

Single Digital Gateway Verordnung

Eine EU-Verordnung, die darauf abzielt, einen einheitlichen Zugang zu Verwaltungsstrukturen der EU zu schaffen.

(teil)automatisierte Verarbeitung

Teilautomatisiert: Einzelne Verfahrensschritte und Entscheidungen innerhalb des Verwaltungsverfahrens werden nach Regeln gesteuert, die definiert und in Software abgebildet werden können. Der Gesamtprozess wird weiterhin von Menschen gesteuert.
Automatisiert: Alle Verfahrensschritte und Entscheidungen innerhalb eines Verwaltungsverfahrens werden nach Regeln gesteuert, definiert und in Software abgebildet. Sonderfälle können weiterhin von Menschen bearbeitet werden.

Traffic Light Protocol (TLP)

Das Traffic Light Protocol (TLP) ist eine standardisierte Vereinbarung zum Austausch von schutzwürdigen Informationen. Es wurde ursprünglich in Großbritannien vom National Infrastructure Security Coordination Centre (NISCC) entwickelt, Das TLP dient der Erhöhung der Sicherheit bei der Weitergabe sensibler Daten. Alle Dokumente werden in eine von vier Klassen eingeteilt, welche die Bedingungen für ihre Weitergabe regeln.

Transaktionskosten

Kosten die im Rahmen wirtschaftlicher Austauschprozesse entstehen und nicht Teil der Gegenleistung für die erbrachte Leistung sind. Hierzu zählen Aufwendungen für die Anbahnung, Durchführung und Kontrolle von Geschäften.

Vertragscontrolling	Vertragscontrolling ist das systematische Überwachen und Steuern von Verträgen. Hierzu ist zu überwachen, dass alle vertraglichen Verpflichtungen (Fristen, Qualität, Preis) eingehalten werden. Es sind Risiken zu identifizieren und zu analysieren, die mit den Verträgen verbunden sind. Es sind Kennzahlen zur Performance der Verträge zu messen.
Vertragsmanagement	Vertragsmanagement ist ein Prozess zur Verwaltung von Verträgen über ihren gesamten Lebenszyklus hinweg (Abschluss, Ausführung, Beendigung bzw. Verlängerung). Teil des Vertragsmanagements ist das Vertragscontrolling. Zum Vertragsmanagement gehört auch das ordnungsgemäße und revisionssichere Archivieren aller vertragsrelevanten Dokumente.
Verwaltungsinformatik	Teilgebiet der Wirtschaftsinformatik, dass sich mit der Anwendung von Informationstechnologie in der öffentlichen Verwaltung beschäftigt.
Vollzeitäquivalent	Ein Vollzeitäquivalent ist definiert als die Anzahl der gearbeiteten Stunden geteilt durch die übliche Arbeitszeit eines Vollzeitbeschäftigten in einem bestimmten Zeitraum. Die Kennzahl ermöglicht es, die Arbeitsleistung von Teilzeit- und Vollzeitkräften vergleichbar zu machen.
Workflow	Verfeinerte Beschreibung von Geschäftsprozessen im Sinne einer formalen exakten technischen Spezifikation. Der Workflow dient der Ausführung des Geschäftsprozesses durch ein hierfür eingesetztes Informationssystem. Arbeitsschritte sind so detailliert beschrieben, dass sie durch einen Beschäftigten oder automatisiert durch eine Anwendung durchgeführt werden können.
Zentrum für Digitale Souveränität (Zendis)	Das ZENDIS ist eine Initiative verschiedener Bundesministerien, Landesregierungen und Wissenschaftseinrichtungen. Ziel ist es, die digitale Souveränität in der öffentlichen Verwaltung zu fördern und zu stärken.