BREMISCHE BÜRGERSCHAFT **Drucksache 21/845 S**
Stadtbürgerschaft (zu Drs. 21/802 S)
21. Wahlperiode 23.06.2026

Mitteilung des Senats vom 23. Juni 2026

Versäumnisse bei der Informationstechnik der Stadtbibliothek Bremen – Steuergeldverschwendung und Sicherheitsrisiken

Die Fraktion BÜNDNIS DEUTSCHLAND hat unter Drucksache 21/802 S eine Kleine Anfrage zu obigem Thema an den Senat gerichtet.

Der Senat beantwortet die vorgenannte Kleine Anfrage wie folgt:

1. Wie bewertet der Senat die im Jahresbericht 2025 des Rechnungshofs dokumentierten erheblichen Versäumnisse bei der Informationstechnik der Stadtbibliothek Bremen insgesamt, insbesondere in Bezug auf IT-Sicherheit, Datenschutz, Wirtschaftlichkeit und ordnungsgemäße Vermögensdarstellung?

   Der Senat nimmt die Feststellungen des Rechnungshofs sehr ernst. Die angeführten Punkte sind aus Sicht des Senats nicht isoliert, sondern im Gesamtzusammenhang von IT-Sicherheit, Datenschutz, Wirtschaftlichkeit und ordnungsgemäßer Vermögensdarstellung zu betrachten.

   Zugleich ist zu berücksichtigen, dass die Stadtbibliothek Bremen keine Behörde mit ausschließlich standardisierten Verwaltungsarbeitsplätzen ist. Sie betreibt neben Verwaltungs-IT auch bibliotheksspezifische IT-Komponenten, etwa Kund:innen-PCs, Katalogzugänge, Kassen- und Selbstverbuchungssysteme sowie weitere technische Angebote im Publikumsbetrieb. Dies entbindet nicht von den Anforderungen an IT-Sicherheit, Wirtschaftlichkeit und ordnungsgemäße Dokumentation, macht aber eine differenzierte Betrachtung der IT-Struktur erforderlich. Der Rechnungshof hat gerade deshalb eine umfassende, zukunftsgerichtete Aufarbeitung des sicheren und wirtschaftlichen IT-Betriebs empfohlen.

   Die Stadtbibliothek hat die Feststellungen des Rechnungshofs angenommen und in die weitere Bearbeitung übernommen. Nach dem vorliegenden Sachstand wurden bereits wesentliche Maßnahmen umgesetzt; weitere Maßnahmen befinden sich in Umsetzung. Das

Ressort geht auf Grundlage des Sachstandsberichts davon aus, dass die offenen Punkte bis Ende 2026 abgeschlossen werden. Verzögerungen sind nach Darstellung der Stadtbibliothek insbesondere durch personelle Engpässe im IT-Team entstanden. Die Empfehlungen werden weiterhin mit hoher Priorität umgesetzt.

2. Welche konkreten Maßnahmen wurden seit Veröffentlichung des Jahresberichts 2025 bereits ergriffen, um ein den Anforderungen des BSI-Grundschutz-Kompendiums (Bundesamt für Sicherheit in der Informationstechnik) entsprechendes IT-Sicherheitskonzept und einen IT-Notfallplan für die Stadtbibliothek zu erstellen und umzusetzen? (Bitte mit Zeitplan und Verantwortlichkeiten darstellen.)

   Die Stadtbibliothek befindet sich im Aufbau eines verbindlichen Informationssicherheitsmanagements. Dieses umfasst auch die Erstellung der erforderlichen konzeptionellen Grundlagen für den IT-Sicherheitsbetrieb sowie die Erarbeitung eines IT-Notfallplans. Verantwortlich für die operative Umsetzung ist die Stadtbibliothek Bremen; die Umsetzung erfolgt unter Einbindung externer fachlicher Unterstützung, insbesondere im Bereich Informationssicherheit. Der Abschluss des Informationssicherheitsmanagements ist nach der vorliegenden Planung für das dritte Quartal 2026 vorgesehen; spätestens bis Ende 2026 sollen die noch offenen Punkte abgeschlossen sein.

   Im Zuge der Verlagerung der Server in ein Rechenzentrum wurden die Serverprozesse dokumentiert. Diese Dokumentation bildet eine wesentliche Grundlage für die weitere Ausarbeitung des IT-Notfallplans. Zudem wurde eine Dienstanweisung für die Beschäftigten der Stadtbibliothek zum Umgang mit EDV-Geräten herausgegeben; darin werden bereits gelebte betriebliche Vorgaben schriftlich fixiert. Insgesamt ist festzuhalten, dass in vielen Prozessen der Stadtbibliothek die Anforderungen der Informationssicherheit bereits enthalten sind, jedoch die formelle Dokumentation noch nicht abgeschlossen wurde.

   Die Stadtbibliothek orientiert sich beim Aufbau des Informationssicherheitsmanagements an einem Managementsystem nach ISO 27001. Soweit bremische Vorgaben oder Feststellungen des Rechnungshofs Anforderungen aus dem BSI-Grundschutz in Bezug nehmen, werden diese im Rahmen des Informationssicherheitsmanagements fachlich bewertet und in die für die Stadtbibliothek geeignete Umsetzung überführt. Ziel ist ein dokumentierter, dauerhaft fortschreibbarer und prüffähiger Informationssicherheitsprozess.

3. Wie ist der aktuelle Stand der Überlegungen zur künftigen Unterbringung der Server der Stadtbibliothek (bauliche Anpassung des vorhandenen Serverraums, externes Rechenzentrum oder Anbindung an Dataport), und welche Varianten werden unter Sicherheits- und Wirtschaftlichkeitsaspekten konkret geprüft?

   Die Frage der künftigen Unterbringung der Server ist nach dem vorliegenden Sachstand entschieden. Die Stadtbibliothek hat die Server im vierten Quartal 2025 in ein zertifiziertes Rechenzentrum verlagert. Damit wurde die vom Rechnungshof besonders hervorgehobene Problemlage der physischen Serversicherheit, insbesondere in Bezug auf Brandschutz und unterbrechungsfreie Stromversorgung am bisherigen Serverstandort, behoben.

   Die Alternative einer baulichen Ertüchtigung des bisherigen Serverraums ist damit für den produktiven Serverbetrieb nicht weiter vorrangig. Eine vollständige Rückkehr in zentrale Landesnetzinfrastrukturen wird derzeit nicht als unmittelbar umsetzbare Option bewertet, weil die Stadtbibliothek aufgrund bibliotheksspezifischer Fachverfahren, externer Schnittstellen und Onlineangebote besondere Anforderungen hat. Eine Nutzung zentraler Dienstleistungen, insbesondere eine Einbeziehung von Dataport bei neuen IT-Bedarfen, erfolgt jedoch weiterhin anlassbezogen und wird seit der Rechnungshofprüfung regelhaft bei entsprechenden Leistungsanfragen berücksichtigt.

4. Welche Maßnahmen wurden getroffen, um die erheblichen Brandlasten im bisherigen Serverraum zu beseitigen, insbesondere hinsichtlich Lagerung von Neugeräten, Austauschgeräten und leicht entzündlichen Materialien?

   Die vom Rechnungshof beanstandete Brandlast im bisherigen Serverraum betraf den früheren produktiven Serverstandort. Durch die Verlagerung der Server in ein Rechenzentrum ist diese konkrete Gefährdungslage für den produktiven Serverbetrieb entfallen. Der bisherige Raum dient danach nicht mehr als maßgeblicher Standort der produktiven Serverinfrastruktur.

   Unabhängig davon bleibt es Aufgabe der Stadtbibliothek, Räume, in denen IT-Komponenten, Ersatzgeräte oder sonstige technische Ausstattung gelagert werden, so zu organisieren, dass Brandschutzanforderungen und geordnete Lagerhaltung eingehalten werden. Die Feststellung des Rechnungshofs, dass Austauschgeräte und leicht entzündliche Materialien nicht in einem Serverraum zu lagern sind, wurde in die weitere Bearbeitung aufgenommen.

5. Hat die Stadtbibliothek inzwischen einen Wartungsvertrag für die USV-Anlage abgeschlossen und werden regelmäßige Wartungen durchgeführt? Wenn ja, seit wann, und mit welchem Leistungsumfang, wenn nein, aus welchen Gründen nicht?

   Die vom Rechnungshof beanstandete fehlende Wartungsvereinbarung bezog sich auf die unterbrechungsfreie Stromversorgung des bisherigen Serverstandorts. Durch die Verlagerung der Server in ein Rechenzentrum ist die bisherige USV-Thematik für den produktiven Serverbetrieb der Stadtbibliothek nicht mehr in derselben Weise einschlägig. Die Verfügbarkeits- und Betriebsanforderungen an die Serverinfrastruktur werden nunmehr im Rahmen des Rechenzentrumsbetriebs abgebildet.

   Weitere technische Einrichtungen, für die eine eigene USV-Anlage beziehungsweise gesonderte Anforderungen an eine unterbrechungsfreie Stromversorgung vorzuhalten wären, werden von der Stadtbibliothek nicht betrieben.

6. In welcher Form werden Datensicherungen aktuell durchgeführt (Sicherungsintervalle, Aufbewahrungsfristen, Offsite-Backups), und wie häufig finden praktische Wiederherstellungstests für kritische Systeme statt?

   Die Stadtbibliothek führt regelmäßige Datensicherungen durch. Der Rechnungshof hatte allerdings festgestellt, dass die Wiederherstellung aus Sicherungskopien zum Prüfungszeitpunkt regelmäßig nur für ein zentrales Fachverfahren getestet wurde und gefordert, die Nutzbarkeit der erzeugten Datensicherungen zur Wiederherstellung verlorener Daten regelmäßig zu überprüfen.

   Backups werden automatisiert nach einem definierten Sicherungskonzept durchgeführt. Die Sicherungsintervalle und Aufbewahrungsfristen richten sich nach der Kritikalität der jeweiligen Systeme sowie nach den jeweiligen betrieblichen Anforderungen. Alle Systeme werden regelmäßig gesichert; die Sicherungen werden zusätzlich offsite beziehungsweise getrennt von der Produktivumgebung aufbewahrt.

   Die Serverinfrastruktur wurde im vierten Quartal 2025 in ein Rechenzentrum migriert. Für die neue Betriebsumgebung liegt derzeit noch keine belastbare Historie regelmäßig dokumentierter praktischer Wiederherstellungstests für kritische Systeme vor. Die Einführung solcher Tests ist im Rahmen des Regelbetriebs vorgesehen. Künftig sollen Wiederherstellungstests in definierten Intervallen durchgeführt und dokumentiert werden.

7. Welche Regelungen gelten derzeit für die dienstliche Nutzung privater Smartphones in der Stadtbibliothek, insbesondere hinsichtlich der Verarbeitung von Anmeldedaten einschließlich Passwörtern sowie E-Mail- und Kalenderinhalten über Server in Drittstaaten, und inwieweit wurden die Empfehlungen des Rechnungshofs hierzu bereits umgesetzt?

   Die dienstliche Nutzung privater Smartphones ist nach dem aktuellen Sachstand beendet. Damit ist der vom Rechnungshof beanstandete Einsatz privater Endgeräte für dienstliche E-Mail- und Kalenderkommunikation abgestellt.

   Für den mobilen Zugriff auf E-Mails und Kalender ist vorgesehen, ausschließlich dienstliche Geräte zu nutzen, die zentral über ein Mobile Device Management verwaltet werden. Nach dem Sachstandsbericht war die Konzeption hierfür bereits abgeschlossen; die Zahl der hierfür vorgesehenen Dienstgeräte sollte auf einen eng begrenzten Bedarf beschränkt werden.

   Der Rechnungshof hatte die frühere Nutzung insbesondere deshalb kritisch bewertet, weil bei der verwendeten mobilen Anwendung Anmeldedaten einschließlich Passwörtern sowie E-Mail-Inhalte über Server in den USA verarbeitet wurden und private sowie dienstliche Daten auf denselben Geräten verwaltet wurden. Durch die Beendigung der dienstlichen Nutzung privater Smartphones und die Umstellung auf zentral verwaltete Dienstgeräte wird diese Risikolage wesentlich reduziert. Die abschließende datenschutz- und informationssicherheitsrechtliche Bewertung der konkret eingesetzten Lösung erfolgt im Rahmen des Informationssicherheitsmanagements.

8. Welche Schritte wurden unternommen, um ein verbindliches Informationssicherheitsmanagement (ISM) für die Stadtbibliothek zu etablieren, und welche der vom Rechnungshof genannten 21 von 78 nicht oder nur teilweise umgesetzten Maßnahmen des Risikobehandlungsplans (darunter neun mit hoher Priorität) sind bereits umgesetzt, in Umsetzung oder noch offen?

   Die Stadtbibliothek baut ein verbindliches Informationssicherheitsmanagement auf. Dieser Prozess wird fachlich begleitet und soll nach der vorliegenden Planung im dritten Quartal 2026 umfassend abgeschlossen werden, spätestens jedoch bis Ende 2026. Das Informationssicherheitsmanagement soll künftig die Dokumentation, Bewertung, Priorisierung, Umsetzung und fortlaufende Pflege von Maßnahmen zur Informationssicherheit sicherstellen.

   Der Rechnungshof hatte festgestellt, dass von 78 Maßnahmen aus dem Risikobehandlungsplan 21 Maßnahmen nicht oder nur teilweise umgesetzt waren, davon neun mit hoher, sieben mit mittlerer und fünf

mit niedriger Priorisierung. Die Stadtbibliothek bearbeitet die aus den früheren Sicherheitschecks abgeleiteten Maßnahmen fortlaufend. Wesentliche offene Maßnahmen mit Bezug zur physischen Sicherheit der Server wurden durch die Verlagerung der Server in ein Rechenzentrum erledigt.

Eine detaillierte öffentliche Auflistung sämtlicher Maßnahmen des Risikobehandlungsplans ist aus Gründen der IT-Sicherheit nicht zweckmäßig, soweit dadurch Rückschlüsse auf konkrete Schutzmaßnahmen, Schwachstellen oder Prioritäten möglich wären. Der Maßnahmenstatus wird durch die Stadtbibliothek nachgehalten und kann dem zuständigen Gremium in geeigneter Form berichtet werden.

9. Wie ist der aktuelle Stand der Inventarisierung der IT-Geräte (einschließlich Zweigstellen), und inwieweit ist sichergestellt, dass Anlagenbestand, Inventarlisten und tatsächlicher Bestand übereinstimmen?

   Die Inventarisierung und Anlagenbestandsführung wurden nach Darstellung der Stadtbibliothek bereits im Zuge des Prüfungsvorgangs grundlegend neu aufgestellt. Die Stadtbibliothek nutzt seit der Prüfung ein Inventarisierungstool, das die im Netzwerk vorhandenen Komponenten laufend erfasst und automatisiert Hinweise auf Bestandslücken ermöglicht. Ergänzend wurden Verfahren zur Erfassung und Verschrottung von IT-Komponenten im Betrieb etabliert.

   Die Stadtbibliothek hat den zugesagten Prozess der Inventarisierung im Jahr 2025 umgesetzt. Die dauerhafte Sicherstellung der Übereinstimmung erfolgt künftig durch technische Inventarisierung, organisatorische Meldeprozesse und regelmäßige körperliche Bestandsaufnahmen.

10. In welchen Abständen sollen künftig körperliche Bestandsaufnahmen der IT-Geräte durchgeführt werden, und welche organisatorischen Regelungen wurden eingeführt, um Gerätezugänge und -abgänge zeitnah zu erfassen?

    Körperliche Bestandsaufnahmen der IT-Geräte sollen künftig in einem dreijährigen Rhythmus durchgeführt werden. Dieser Turnus entspricht der Empfehlung des Rechnungshofs, mindestens alle drei Jahre eine körperliche Bestandsaufnahme durchzuführen und dabei auch die Zweigstellen einzubeziehen.

    Zur zeitnahen Erfassung von Gerätezugängen und -abgängen wurden die entsprechenden Verfahren in der Stadtbibliothek neu geordnet. Dazu gehören insbesondere die Nutzung eines Inventarisierungstools, definierte Prozesse zur Erfassung und Verschrottung von IT-Komponenten sowie organisatorische Abstimmungen zwischen IT,

Beschaffung und Anlagenbuchhaltung. Damit soll sichergestellt werden, dass die Anlagenbuchhaltung zeitnah Kenntnis von Zu- und Abgängen erhält und IT-Geräte eindeutig identifizierbar geführt werden.

11. Welche Konsequenzen hat der Senat aus den festgestellten Mängeln bei IT-Vergaben der Stadtbibliothek gezogen, und welche Vorgaben beziehungsweise Schulungsmaßnahmen wurden ergriffen, um künftige Vergabeverfahren rechtssicher zu gestalten?

    Der Senat teilt die Einschätzung, dass die vom Rechnungshof festgestellten Mängel bei IT-Vergaben abzustellen sind.

    Die Stadtbibliothek hat die Feststellungen des Rechnungshofs anerkannt und zugesagt, künftige Vergabeverfahren entsprechend den geltenden formellen und materiellen Anforderungen durchzuführen. Für größere Ausschreibungen ist vorgesehen, die Dienstleistung des zentralen Vergabemanagements zu nutzen, um die Rechtskonformität der Verfahren zu unterstützen. Zudem hat die Stadtbibliothek nach der Veröffentlichung des Rechnungshofberichts beschlossen, bei neuen Vertragsabschlüssen EVB-IT-Muster zu verwenden.

    Darüber hinaus wurde nach Darstellung der Stadtbibliothek der Kontakt zu Dataport intensiviert. Bei Preisanfragen und Anfragen zu IT-Dienstleistungen wird Dataport standardmäßig einbezogen, um die Vorgaben des Gesetzes zur Gewährleistung der digitalen Souveränität zu beachten.

12. In welchen Bereichen wurden seit der Rechnungshofprüfung IT-Leistungen vergeben, und inwieweit wurden dabei die EVB-IT-Vertragsmuster und die Vorgaben des Gesetzes zur Gewährleistung der digitalen Souveränität vollständig angewendet?

    Seit der Rechnungshofprüfung wurde insbesondere der Betrieb der Firewall vergeben. Dataport wurde hierzu zur Angebotsabgabe aufgefordert; von dort wurde zurückgemeldet, dass kein Angebot abgegeben wird. Die Stadtbibliothek hat die Dienstleistung anschließend auf Grundlage eines Angebotsvergleichs vergeben. Für den Vertrag wurde das EVB-IT-Vertragsmuster verwendet. Damit wurden bei dieser Vergabe sowohl die Einbeziehung Dataports als auch die Verwendung eines EVB-IT-Vertragsmusters berücksichtigt.

    Für künftige IT-Vergaben gilt, dass die Stadtbibliothek EVB-IT-Vertragsmuster bei neuen Vertragsabschlüssen verwenden und die Vorgaben des Gesetzes zur Gewährleistung der digitalen Souveränität beachten wird. Der Rechnungshof hatte ausdrücklich gerügt, dass im November 2023 der Umzug der Homepage nach einem Angebotsvergleich zwischen privaten Unternehmen vergeben wurde, ohne Dataport oder eine andere geeignete juristische Person des öffentlichen Rechts einzubeziehen.

Die Stadtbibliothek hat zugesagt, das Gesetz künftig zu beachten. Nach dem Sachstandsbericht wird Dataport seit der Prüfung bei entsprechenden Preisanfragen und Dienstleistungsanfragen standardmäßig einbezogen.

13. Wie bewertet der Senat den vom Rechnungshof kritisierten überhöhten Ausstattungsgrad mit Desktops, Notebooks und Netzwerkdruckern hinsichtlich Wirtschaftlichkeit, und welche konkreten Maßnahmen zur Reduzierung auf ein angemessenes Maß wurden beschlossen oder bereits umgesetzt?

    Der Senat bewertet den vom Rechnungshof festgestellten Ausstattungsgrad als Anlass für eine konsequente Überprüfung unter Wirtschaftlichkeitsgesichtspunkten.

    Die Stadtbibliothek hat den erhöhten Ausstattungsgrad im Wesentlichen mit zwei Faktoren erklärt: Zum einen erfordert der Betrieb einer Stadtbibliothek neben Büroarbeitsplätzen auch Funktionsarbeitsplätze im Bibliotheks- und Publikumsbereich, insbesondere an Service- und Infoplätzen. Zum anderen kam es pandemiebedingt zu zusätzlichen Notebookbeschaffungen, um kurzfristig ortsflexibles Arbeiten beziehungsweise Homeoffice zu ermöglichen; vorhandene Desktopgeräte wurden zunächst parallel weiterbetrieben.

    Die Betriebsleitung der Stadtbibliothek hat als Zielwert ein Ausstattungsniveau von 1,2 Geräten je beschäftigter Person festgelegt. Dieser Zielwert sollte im Zuge der Umstellung auf Windows 11 und der Umsetzung einer Ein-Geräte-Strategie erreicht werden. Eine weitergehende Reduzierung wird von der Stadtbibliothek wegen der besonderen Struktur mit acht Standorten, die jeweils Bibliotheks- und Bürobereiche haben, Verfügungslaptops für aufsuchende Bibliotheksarbeit sowie ortsflexibler Arbeit nicht als sachgerecht angesehen. Der Zielwert konnte bislang nicht vollständig erreicht werden. Hintergrund ist, dass eine durchgängige Ein-Geräte-Strategie im Bibliotheksbetrieb nicht in allen Konstellationen sachgerecht ist; dies betrifft insbesondere standortübergreifende Einsätze und kurzfristig erforderliches ortsflexibles Arbeiten. Nach aktuellem Bearbeitungsstand liegt der Ausstattungsfaktor bei rund 1,25 Geräten je beschäftigter Person (das sind acht Geräte mehr als bei einem Soll-Wert von 1,2 bei einer Gesamtzahl von 188 Geräten). Weitere Rechner sind für eine kurzfristige Aussonderung beziehungsweise einen Abbau vorgesehen.

    Die Zahl der Netzwerkdrucker in der Zentrale wurde nach Darstellung der Stadtbibliothek seit dem Prüfungszeitpunkt um über ein Viertel reduziert. Eine weitere Reduzierung wird dort nur insoweit verfolgt, wie sie mit den betrieblichen Anforderungen vereinbar ist. Insbesondere

Auskunftsplätze im Publikumsbereich und bestimmte Arbeitsprozesse können einen unmittelbaren Zugriff auf Drucktechnik erfordern.

14. Plant der Senat, die Stadtbibliothek stärker an die zentralen IT-Strukturen und Dienstleistungen des Landes (insbesondere Dataport) anzubinden, um ein einheitliches Sicherheitsniveau und wirtschaftliche Skaleneffekte zu erreichen? Wenn ja, mit welchem Konzept und Zeitrahmen, wenn nein, aus welchen Gründen nicht?

    Der Senat verfolgt grundsätzlich das Ziel, zentrale IT-Strukturen und zentrale Dienstleistungsangebote dort zu nutzen, wo dies fachlich geeignet, sicher und wirtschaftlich ist. Dies gilt auch für die Stadtbibliothek. Zugleich sind die besonderen Anforderungen des Bibliotheksbetriebs zu berücksichtigen. Die Stadtbibliothek betreibt bibliotheksspezifische Fachverfahren, benötigt externe Schnittstellen, nutzt Onlineangebote und bezieht Mediendaten über Schnittstellen. Nach dem in der Akte enthaltenen Bearbeitungsstand stehen diese Anforderungen einer kurzfristigen vollständigen Rückkehr in das Bremische Verwaltungsnetz beziehungsweise einer vollständigen Standardisierung auf zentrale Verwaltungs-IT derzeit entgegen.

    Dies bedeutet nicht, dass zentrale Dienstleister nicht einbezogen werden. Vielmehr wurde seit der Prüfung ein engerer Kontakt zu Dataport aufgebaut. Bei Preisanfragen und Anfragen zu IT-Dienstleistungen wird Dataport standardmäßig berücksichtigt, insbesondere auch zur Einhaltung der Vorgaben des Gesetzes zur Gewährleistung der digitalen Souveränität.

    Eine stärkere Anbindung an zentrale IT-Strukturen ist daher nicht als pauschale Vollmigration, sondern als einzelfallbezogene Prüfung geeigneter Leistungen zu verstehen. Maßgeblich sind hierbei IT-Sicherheit, Datenschutz, Wirtschaftlichkeit, Kompatibilität mit bibliotheksspezifischen Anforderungen und die Sicherstellung des öffentlichen Bibliotheksauftrags.

15. Welche übergreifenden Konsequenzen zieht der Senat aus den Feststellungen zur Stadtbibliothek für andere Eigenbetriebe und Kulturinstitutionen mit eigener IT-Infrastruktur im Land Bremen?

    Der Senat zieht aus den Feststellungen zur Stadtbibliothek die Konsequenz, dass eigenständige IT-Strukturen in Eigenbetrieben und Kulturinstitutionen einer regelmäßigen, risikoorientierten Betrachtung unterzogen werden müssen. Dabei sind insbesondere Informationssicherheit, Datenschutz, Notfallvorsorge, Inventarisierung, ordnungsgemäße Vertrags- und Vergabeverfahren, Einhaltung der Vorgaben zur digitalen Souveränität sowie Wirtschaftlichkeit gemeinsam zu betrachten.

Der Fall der Stadtbibliothek zeigt, dass eine ausschließlich maßnahmenbezogene Betrachtung einzelner IT-Komponenten nicht ausreicht. Erforderlich ist eine strategische Gesamtbetrachtung, die sowohl die konkrete Aufgabenwahrnehmung der jeweiligen Einrichtung als auch die Anforderungen an sichere, wirtschaftliche und nachvollziehbar dokumentierte IT berücksichtigt. Der Rechnungshof hat hierzu ausdrücklich empfohlen, den sicheren und wirtschaftlichen IT-Betrieb umfassend und zukunftsgerichtet aufzuarbeiten.

Für Einrichtungen mit eigener IT-Infrastruktur bedeutet dies insbesondere, dass vorhandene IT-Strukturen regelmäßig daraufhin zu überprüfen sind, ob zentrale Dienste des Landes oder von Dataport genutzt werden können, ob eigene Lösungen weiterhin fachlich erforderlich und wirtschaftlich vertretbar sind und ob die jeweils geltenden Anforderungen an Informationssicherheit, Datenschutz, Vergabe und Dokumentation eingehalten werden. Eine pauschale Gleichbehandlung aller Einrichtungen ist dabei nicht sachgerecht; maßgeblich ist eine differenzierte Bewertung nach Aufgabenprofil, Schutzbedarf, technischen Abhängigkeiten und Wirtschaftlichkeit.