

# Cloud-Strategie des Landes Baden-Württemberg

Version 1.0

Stand 04.12.2020



**Baden-Württemberg**

MINISTERIUM FÜR INNERES, DIGITALISIERUNG UND MIGRATION

Herausgeber:

Ministerium für Inneres, Digitalisierung und Migration

## INHALT

Vorwort.....	5
1 Die Cloud-Strategie des Landes Baden-Württemberg – Motivation und Zielsetzung....	6
2 Einbettung in den länderübergreifenden Kontext .....	7
2.1 Bundesinitiativen.....	7
2.2 Europa .....	8
3 Ausgangssituation Baden-Württemberg.....	9
3.1 Bereitstellung von Cloud-Technologien innerhalb der Landesverwaltung.....	11
3.2 Koordinierung der Bedarfe an Cloud-Technologien .....	12
4 Einsatz von Cloud-Technologien und ihre Auswirkungen .....	13
4.1 Möglichkeiten .....	13
4.2 Grundlagen bilden.....	15
5 Leitprinzipien für den Einsatz von Cloud Technologien.....	16
6 Handlungsschwerpunkte .....	19
6.1 Organisatorische Maßnahmen.....	19
6.1.1 Konfiguration und Bereitstellung grundlegender Softwarelösungen für den Betrieb von Cloud-Infrastruktur .....	19
6.1.2 Aufbau des erforderlichen Know-hows .....	20
6.1.3 Organisatorische Veränderungen und Schnittstellen.....	21
6.1.4 Ausweitung der Cloud-Infrastruktur .....	21
6.1.5 Anpassung der landesinternen Vorgaben.....	22
6.2 Technologiebezogene Maßnahmen.....	22
7 Planung und Umsetzung der Cloud-Strategie .....	26
7.1 Planung / Initialisierung .....	26
7.1.1 Design der Cloud-Architektur.....	26
7.1.2 Cloud Portfolio Migration und Modernisierung.....	26
7.1.3 DevOps Transformation.....	26
7.2 Migrationsvorbereitung.....	27

7.3	Aufbau.....	27
7.4	Management.....	27
8	Risiken hinsichtlich der Umsetzung.....	27

## **Vorwort**

Der Einsatz von Cloud-Technologien eröffnet für die IT der Landesverwaltung neue Handlungsspielräume. Diese sind in vielfältiger Hinsicht zu betrachten, beispielsweise im Hinblick auf Vereinfachungen der Leistungsbereitstellung, einer stärkeren Standardisierung, der Nutzung vorgefertigter Services, der Reduzierung der Betriebskosten aber auch unter dem Aspekt einer sicheren und datenschutzkonformen Nutzung in der Landesverwaltung. Für die IT der Landesverwaltung ist eine Technologiestrategie, die diese Handlungsspielräume aufgreift und nutzt, unerlässlich. Die Cloud-Strategie benennt hierzu Handlungsschwerpunkte, die auf die Bereitstellung und das Management einer umfassenden Cloud-Infrastruktur zielen. Die zugehörigen Maßnahmen sind grundlegend, um den technologischen Abstand nicht nur zu IT-Dienstleistern anderer Bundesländer und kommunalen Dienstleistern, sondern auch zu privatwirtschaftlichen Anbietern von Cloud-Diensten, zu verringern.

Die aktuelle Entwicklung zeigt, dass Anbieter ihre Softwareprodukte immer häufiger als reine Cloud-Anwendungen bereitstellen bzw. diese nur noch in dieser Form weiter lizenzierbar sind. Eine Cloud-Strategie, welche die damit verbundenen Anforderungen aufgreift, die Abhängigkeit von einzelnen Herstellern und mit deren Produkten oftmals einhergehenden Datenverarbeitungen reduziert und den Aufbau von Alternativen innerhalb der IT der Landesverwaltung berücksichtigt, unterstützt die mittel- und langfristige Planbarkeit und Steuerbarkeit der IT-Landesarchitektur und ist damit ein wesentlicher Baustein der künftigen IT-Gesamtarchitektur des Landes.

## **1 Die Cloud-Strategie des Landes Baden-Württemberg – Motivation und Zielsetzung**

Die Cloud-Strategie des Landes Baden-Württemberg soll Fragestellungen im Zusammenhang mit der Bereitstellung und dem Einsatz von Cloud-Technologien aufgreifen und im Sinne einer Gesamtstrategie beantworten. Sie soll innerhalb der Landesverwaltung in Bezug auf Cloud-Technologien als Orientierung dienen und einheitliche Vorgaben für deren Verwendung definieren. Auf der strategischen und administrativen Ebene wendet sie sich an Entscheider, sowohl innerhalb der Ressorts als auch innerhalb der ressortübergreifenden Gesamtsteuerung der Landes-IT. Auf der technischen Ebene richtet sie sich gleichermaßen an Entwicklung und Betrieb, deren Form der Zusammenarbeit sich vor allem außerhalb der Landesverwaltung mit dem Einzug von Cloud-Technologien in den vergangenen Jahren in besonderem Maße gewandelt hat.

Der inzwischen hohe Standardisierungs- und Virtualisierungsgrad von IT-Services und Infrastruktur ermöglicht die zunehmende Nutzung dezentral bereitgestellter Dienste und deren Integration in die eigenen fachlichen Abläufe. Eine Vielzahl an IT-Services muss nicht mehr durch die eigene Anwendungsentwicklung erstellt und schließlich auf eigenen Servern betrieben und gewartet werden, sondern kann entweder in Form von Anwendungen (Software as a Service – SaaS), Plattformen für Entwickler (Platform as a Service – PaaS) oder Infrastruktur (Infrastructure as a Service – IaaS) für die eigenen Zwecke verwendet werden.

Die Nutzungsmöglichkeiten dieser Dienste sind vielfältig: Im Bereich der Infrastruktur ergeben sich aufgrund konsequenter Virtualisierung und Automatisierung beispielsweise dadurch Vorteile, dass die Rechenleistung bzw. der Speicherplatz einer bestehenden virtuellen Infrastruktur bedarfsgesteuert direkt und kurzfristig erweitert oder reduziert werden kann. Plattform-Dienste erlauben es dem Entwickler, von Dritten bereitgestellte Komponenten beispielsweise zur Künstlichen Intelligenz (KI) oder zur Datenanalyse etc., in die eigene Anwendung zu integrieren. Darüber hinaus lassen sich ganze Anwendungssysteme wie zum Beispiel Office- und Groupware-Systeme als Software-Dienste nutzen. All diesen Diensten ist gemein, dass sie nicht auf eigenen lokalen Servern installiert sein müssen, sondern als verfügbare „Cloud-Dienste“ zur Nutzung bereitstehen. Soweit externe Anbieter verwendet werden, steht den Nutzungsmöglichkeiten jedoch auch ein hohes Risiko von Abhängigkeiten, langfristig hohen Kosten und dem Verlust eigener Kompetenzen gegenüber.

Im Hinblick auf die weitreichenden Verwendungsmöglichkeiten von Cloud-Diensten ergeben sich aus Sicht der Nutzer aber auch aus Sicht der Landes-IT eine Reihe von Fragestellungen:

- Welche Art von Diensten sollte zentral im Land bereitgestellt werden und welche in Form externer Cloud-Angebote?
- Welche Vor- und Nachteile hat der Aufbau einer landeseigenen Cloud-Infrastruktur?
- Welche Vorteile bieten Cloud-Dienste im Hinblick auf Einfachheit und Schnelligkeit bei der Umsetzung von Fachanforderungen?
- Wie erfolgt die Auswahl eines konkreten externen Cloud-Angebots? Dürfen gleichartige Cloud-basierte Funktionen verschiedener Anbieter genutzt werden?
- Ob und wenn ja, wie kann das Land bei externen Cloud-Anbietern sowohl die Hoheit über die eigenen Daten als auch den Datenschutz gewährleisten?
- Inwieweit werden die Anforderungen an die Informationssicherheit und den Datenschutz durch die Verwendung von Cloud-Diensten berücksichtigt?
- Welche Grenzen bzgl. der Nutzung bestehen, d. h. wo bzw. wie sind Cloud-Dienste nicht sinnvoll einsetzbar?
- Wie können notwendige Kompetenzen innerhalb der Landesverwaltung aufgebaut und kontinuierlich weiter ausgebaut werden?

Die Cloud-Strategie des Landes Baden-Württemberg geht einher mit der Zielsetzung, eine moderne landesinterne und vollständig automatisierte virtuelle IT-Infrastruktur aufzubauen, die als zentrale Plattform für Leistungen innerhalb der Landesverwaltung zur Verfügung steht und die darüber hinaus auch in länderübergreifenden Kooperationen einen wesentlichen Beitrag zur Leistungsbereitstellung liefert. Mit ihr verbunden ist der Aufbau einer zukunftsfähigen IT-Gesamtarchitektur, die den Anforderungen unter anderem an Standardisierung, Eigenständigkeit, Sicherheit und Flexibilität Rechnung trägt.

## **2 Einbettung in den länderübergreifenden Kontext**

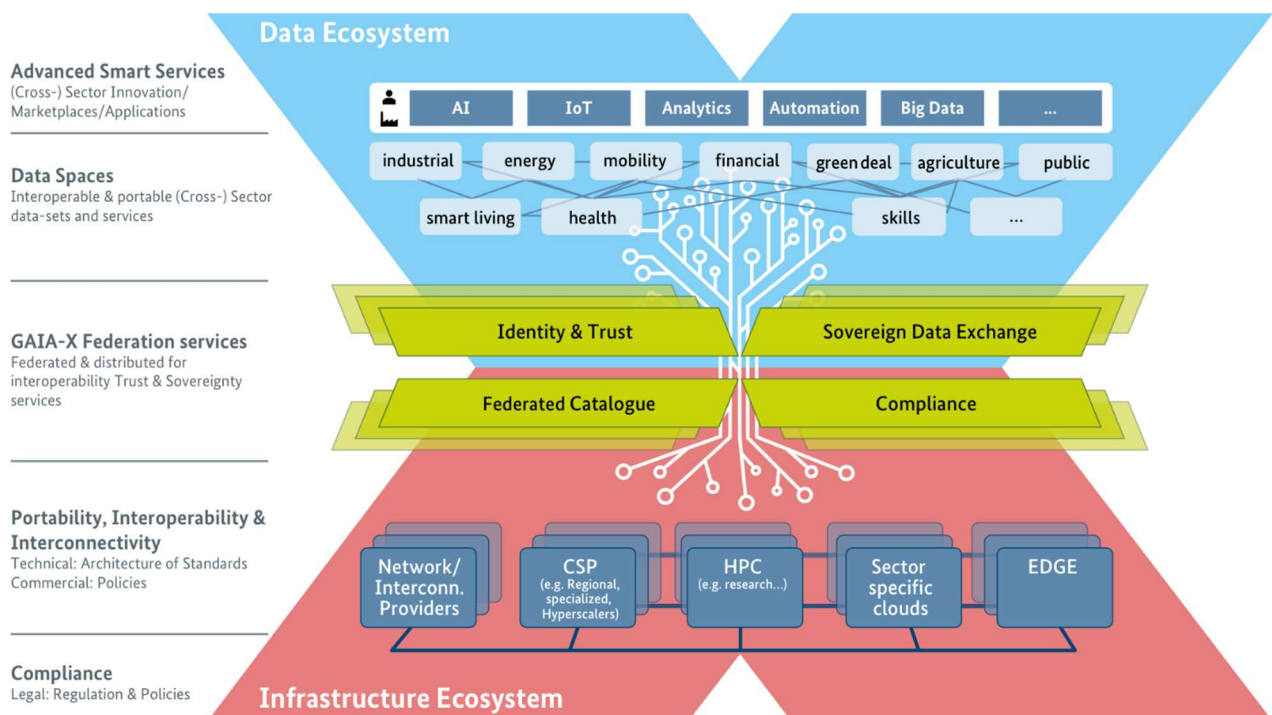
### **2.1 Bundesinitiativen**

Der IT-Planungsrat hat auf seiner 29. Sitzung am 27.06.2019 die Arbeitsgruppe „Cloud Computing und digitale Souveränität“ eingerichtet. Mit dieser Arbeitsgruppe soll einerseits eine föderale Cloud-Infrastruktur aufgebaut werden, die einzelne Clouds mit Schwerpunktaufgaben vernetzt und somit dezentral entwickelte Lösungen allen Verwaltungen zur Verfügung stellt. Zum anderen sollen zur Sicherung der digitalen Souveränität Möglichkeiten untersucht werden, die zu einer Reduzierung von Herstellerabhängigkeiten führen. Insgesamt verfolgt die Arbeitsgruppe das Ziel, alternative Lösungen zu den marktbeherrschenden Softwareanbietern zu untersuchen und somit sowohl Abhängigkeiten im wirtschaftlichen Sinne zu reduzieren als auch den Datenschutz und die Informationssicherheit zu gewähr-

leisten. Der Einsatz von Cloud-Infrastrukturen wurde im Rahmen eines gemeinsamen Eckpunktepapiers<sup>1</sup> von Bund, Ländern und Kommunen dementsprechend als Handlungsfeld definiert.

## 2.2 Europa

Auch über Deutschland hinaus wird unter dem Projektnamen GAIA-X<sup>2</sup> (maßgeblich getragen durch die deutsche Bundesregierung zusammen mit Frankreich, weiteren EU-Staaten und einem Zusammenschluss von Wirtschaft und Wissenschaft in der hierfür gegründeten GAIA-X Foundation<sup>3</sup>) der Aufbau einer leistungs- und wettbewerbsfähigen, sicheren sowie vertrauenswürdigen Dateninfrastruktur für Europa angestrebt.



Quelle: BMWi

**Abbildung 1 - GAIA-X Überblick: Architekturansatz föderierter GAIA-X Services**  
(aus "GAIA-X: Das europäische Projekt startet in die nächste Phase" BMWi, Juni 2020)

<sup>1</sup> [https://www.cio.bund.de/SharedDocs/Publikationen/DE/Bundesbeauftragter-fuer-Informationstechnik/Konferenz\\_der\\_IT-Beauftragten\\_der\\_Ressorts\\_Beschluesse/2020\\_01\\_Beschluss\\_Konferenz\\_IT-Beauftragte.pdf?\\_\\_blob=publicationFile](https://www.cio.bund.de/SharedDocs/Publikationen/DE/Bundesbeauftragter-fuer-Informationstechnik/Konferenz_der_IT-Beauftragten_der_Ressorts_Beschluesse/2020_01_Beschluss_Konferenz_IT-Beauftragte.pdf?__blob=publicationFile)

<sup>2</sup> GAIA-X – BMWi-Artikel: <https://www.bmw.de/Redaktion/DE/Artikel/Digitale-Welt/dateninfrastruktur.html>

<sup>3</sup> Siehe GAIA-X Foundation: <http://www.data-infrastructure.eu>



GAIA-X konzentriert sich dabei zunächst auf folgende Bereiche:

- die Implementierung eines sicheren und förderierten Identitätsmanagements und die Schaffung von Vertrauensmechanismen (Security and Privacy by Design)
- die Entwicklung von souveränen Daten-Services, die die Identität von Quelle und Empfänger der Daten gewährleisten und die Zugriffs- und Nutzungsrechte auf die Daten sowie die Datenhoheit der Anwender sicherstellen
- die Bereitstellung eines nutzerfreundlichen Zugangs zu verfügbaren Anbietern, Knoten und Diensten. Die notwendigen Informationen werden durch den förderierten Katalog bereitgestellt
- die Integration von bestehenden Standards, um die Interoperabilität und Portabilität zwischen Infrastruktur, Anwendungen und Daten sicherzustellen
- die Einführung von Compliance Regeln sowie von Zertifizierungs- und Akkreditierungsangeboten
- die Bereitstellung von Open-Source-Software und Standards, um Anbieter bei der Migration in eine sichere, förderierte und interoperable Infrastruktur zu unterstützen

Das über GAIA-X verfügbare Produkt- und Serviceportfolio wird dabei entlang verschiedener Use-Cases aus Anwendersicht entwickelt. Hierzu liegen bisher mehr als 40 Use-Cases in acht Domänen („Industrie 4.0/KMU“, „Gesundheit“, „Finanzwesen“, „Öffentlicher Sektor“, „Smart Living“, „Energie“, „Mobilität“ und „Agrar“) vor<sup>4</sup>.

In diesem Sinne entsteht im Rahmen von GAIA-X ein Lösungskonzept für ein cloudbasiertes europäisches Daten-/Infrastruktur-Ökosystem, inklusive relevanter offener Standards, Open-Source-Software und ein Portfolio von Cloud-Services, welche sowohl eine technologische, fachliche und auch wirtschaftliche Relevanz für IT und Verwaltung in Baden-Württemberg entwickeln und daher frühzeitig berücksichtigt werden müssen.

### **3 Ausgangssituation Baden-Württemberg**

Innerhalb der Landesverwaltung Baden-Württembergs werden inzwischen vielfältige Cloud-Dienste genutzt. Diese beziehen sich beispielsweise auf die Bereitstellung von Infrastruktur-Ressourcen, über Kommunikationsdienste bis hin zu Office-Lösungen.

Ein wesentlicher Aspekt liegt dabei auf der Bereitstellung von Softwarelösungen über Internettechnologien sowie auf der an Bedeutung zunehmenden Anforderung, im Land entwickelte Softwarekomponenten und Anwendungssysteme in Form von Anwendungscontainern auf einer entsprechenden virtuellen Infrastruktur betreiben zu können.

---

<sup>4</sup> Siehe auch BMWi GAIA-X Dossier / Use Case Galerie: <https://www.bmwi.de/Redaktion/DE/Dossier/gaia-x.html>

Je nach Nutzungsszenario unterscheiden sich teilweise die Zielgruppen. Komplette Softwarelösungen sind innerhalb der Landesverwaltung insbesondere für Endanwender von besonderem Interesse, da diese in der Regel ohne großen Installations- und Administrationsaufwand in die fachlichen Abläufe integriert werden können. Einzelne Softwarekomponenten bzw. Anwendungscontainer mit spezifischen Funktionen hingegen reduzieren eigene Entwicklungsaufwände und werden daher vorrangig von Entwicklern genutzt und in die eigene Anwendungssoftware eingebunden. Durch die Verwendung von Anwendungscontainern wird der Einsatz von Anwendungssystemen sowie der Betrieb aufgrund des damit einhergehenden höheren Automatisierungsgrads bzw. weitreichender Skalierungsmöglichkeiten vereinfacht.

Auch wenn bereits innerhalb der Landesverwaltung Cloud-Dienste genutzt werden, erfolgt dies bisher nur singular und entspricht nicht mehr dem immer stärker wachsenden Bedarf, wie etwa im Umfeld der Anwendungsentwicklung oder für eine automatisierte Bereitstellung von virtuellen Servern im Rahmen von Self-Services, wie sie für die Einrichtung von (Fach-)Testumgebungen eingesetzt werden können.

Konkret lassen sich die innerhalb der Landesverwaltung bestehenden funktionalen Anforderungen an Cloud-Dienste in vier Kategorien klassifizieren:

**1. Nutzung virtueller Server für die Entwicklung von Fachanwendungen und/oder deren Betrieb**

Ein wesentlicher Aspekt ist hierbei die Konfiguration und Bereitstellung mittels Web-Technologien, die es dem Nutzer ermöglicht, im Rahmen eines Self-Services die gewünschte Leistung unmittelbar zu beziehen.

**2. Verwendung von Container-Plattformen für das Deployment von Fachanwendungen**

Fachanwendungen, die als in sich geschlossene Software-Pakete (Container) pakettiert werden, lassen sich im Unterschied zu VMs flexibel, besser skalierbar und betriebssystemunabhängig auf eigenen Container-Plattformen oder in der Cloud einsetzen. Werkzeuge für die Orchestrierung von Containern<sup>5</sup> erlauben zudem die automatisierte Verwaltung von Containern (skalieren, verschieben, überwachen, wiederaufsetzen, ...).

**3. Einbindung Cloud-basierter Plattform-as-a-Service-Dienste im Rahmen der Entwicklung von Fachanwendungen**

---

<sup>5</sup> wie beispielsweise Kubernetes bzw. Docker Swarm

Über Web-Technologien bereitgestellte Plattform-as-a-Service-Dienste können in eigene Fachanwendungen eingebunden werden und reduzieren hierdurch Aufwände für die Entwicklung der geforderten Funktionalität, beispielsweise für Funktionen der Künstlichen Intelligenz, Datenanalyse etc.

#### 4. **Nutzung vollständiger webbasierter Software-Lösungen, die in einer Cloud zur Verfügung gestellt werden**

Diese ermöglichen eine client-neutrale Nutzung (mittels Web-Browser auf vielen Geräteklassen), was eine flexible und skalierbare Zurverfügungstellung und Nutzung verbessert. Beim Einsatz entsprechender UX-Standards (zum Beispiel über standardisierte Elementbibliotheken für Benutzungsschnittstellen), wird zudem eine über Einzelanwendungen konsistente Bedienung vereinfacht.

Weiterhin ermöglichen moderne Web-Technologien die Entwicklung von offline-fähigen „Progressive Web Apps“<sup>6</sup>, sodass für viele Anwendungsszenarien vollständig webbasierte Lösungen umgesetzt werden können.

Diese Einsatzzwecke gehen einher mit weiteren Anforderungen, insbesondere im Hinblick auf die Gewährleistung der Informationssicherheit, des Datenschutzes, einer möglichst weitreichenden Herstellerunabhängigkeit, der Gewinnung und Fortbildung qualifizierten Personals sowie rechtlichen Rahmenbedingungen.

Sowohl in technologischer Hinsicht als auch unter dem Aspekt der ressortübergreifenden Koordination der Anforderungen an Cloud-Dienste und strategischer Planung in Bezug auf zukünftige Bedarfe und Anbieterauswahl ist die Landesverwaltung unter Handlungsdruck. Beide Facetten sind bei der Umsetzung der Cloud-Strategie gleichermaßen zu berücksichtigen.

### 3.1 **Bereitstellung von Cloud-Technologien innerhalb der Landesverwaltung**

Die Fähigkeit, Cloud-Technologien innerhalb der Landesverwaltung anbieten zu können, ist für die IT des Landes von strategischer Bedeutung. Der mit der Entwicklung des Landesrechenzentrums hin zum Cloud-Anbieter einhergehende Virtualisierungs- und Automatisierungsgrad der IT-Infrastruktur stellt zum einen die Konkurrenzfähigkeit des Landesrechenzentrums gegenüber externen Anbietern sicher. Zum anderen erhöht es die Unabhängigkeit der Landesverwaltung von kommerziellen Cloud-Anbietern und somit die digitale Souveränität insbesondere in Bezug auf die landeseigenen Daten.

---

<sup>6</sup> Neben der Offline-Funktionalität zeichnen Progressive Web Apps weitere vorteilhafte Charakteristika aus, beispielweise geräteklassenübergreifende Oberflächen, Installierbarkeit (auf Mobilgeräten auch ohne die üblichen Hersteller-App-Stores), Push-Mitteilungen und ein tiefer Zugriff auf Geräteschnittstellen.

Der Einsatz zugehöriger moderner und marktüblicher Technologien fördert neben der Erhöhung der Wirtschaftlichkeit in der Umsetzung von Fachanforderungen zudem den Aufbau und Erhalt des für eine effiziente IT-Dienstleistungsbereitstellung erforderlichen Know-hows. Es ist zudem davon auszugehen, dass sich hierdurch positive Auswirkungen auf die Attraktivität der zugehörigen Aufgaben und der damit verbundenen Rollen bzw. Stellen innerhalb der IT-Organisation ergeben. Ferner eröffnen sich für die IT-Organisation neue Handlungsräume, beispielsweise im Hinblick auf die zunehmend an Bedeutung gewinnenden Kooperationen mit anderen Bundesländern und die länderübergreifende Bereitstellung eigener Dienste.

Derzeit sind die hierzu erforderlichen Fähigkeiten noch nicht bzw. nicht in ausreichendem Maß vorhanden, da gegenwärtig nur einzelne Teilbereiche der IT-Infrastruktur virtualisiert sind. Hierbei handelt es sich um die Bereitstellung und den Betrieb virtueller Server, während die Virtualisierung der Netzwerkinfrastruktur und der zugeordneten Infrastrukturkomponenten wie zum Beispiel Router und Firewalls noch nicht stattgefunden hat.

Für die Entwicklung und den Betrieb von Anwendungen haben sich mit dem Einzug der Container-Technologie erhebliche Verbesserungen ergeben. Hierbei sind vor allem die bessere Skalierbarkeit der Anwendungen, die deutlich höhere Ressourceneffizienz im Betrieb sowie die flexible Handhabung der Anwendungscontainer aufgrund ihrer plattformübergreifenden Einsatzmöglichkeiten zu nennen. Diese Technologie, die von einzelnen Ressorts bereits genutzt wird, ist in der Landesverwaltung bislang noch unzureichend etabliert. Hier ist ein Umdenken und eine konsequente Umstellung der Anwendungen auf diese Technologie anzustreben.

Darüber hinaus entspricht die Administration der Anwendungscontainer nicht dem erforderlichen Automatisierungsgrad. Technologien, die diese Aufgabe übernehmen, sind bislang im Landesrechenzentrum noch nicht etabliert.

Dies wird sich perspektivisch ändern: Im Zusammenhang mit der Evaluierung und Ertüchtigung der BITBW wird diese zukünftig orchestrierte Container-Umgebungen bereitstellen und entsprechende Self Services anbieten. Dies erfolgt gemäß der ressortübergreifend abgestimmten Diskussionsvorlage zum Umgang mit ressortspezifischen Fachverfahren im Rahmen des künftigen Leistungsportfolios der BITBW. Das Leistungsportfolio gründet auf den Ergebnissen zur „Strategie und Steuerung BITBW und IT-Land“ des Evaluierungs-Projekts.

### **3.2 Koordinierung der Bedarfe an Cloud-Technologien**

In der Landesverwaltung besteht zunehmend der Bedarf, Anwendungsfunktionen und Dienste aus der Cloud zu beziehen. Ein Grund hierfür ist darin zu sehen, dass Hersteller

von Software-Lösungen dazu übergehen, ihre Dienste nicht mehr On-Premises anzubieten, sondern als Cloud-Dienst webbasiert zur Verfügung zu stellen. Zudem werden Angebote wie zum Beispiel Messaging-Dienste genutzt, die bereits als Cloud-Dienst konzipiert wurden und nur als solche genutzt werden können.

Hinsichtlich der Verwendung solcher Dienste sind in der Verwaltungsvorschrift des Innenministeriums über die IT-Standards des Landes (VwV IT-Standards) bereits Rahmenbedingungen definiert, die sowohl die Transparenz über den Einsatz als auch die Berücksichtigung der Sicherheitsanforderungen sicherstellen sollen. Dennoch fehlt es an einer ressortübergreifenden Abstimmung in Zusammenarbeit mit dem Landesrechenzentrum hinsichtlich gemeinsamer Anforderungen sowie absehbarer zukünftiger Bedarfe und einer darauf ausgerichteten Anbieterauswahl.

## **4 Einsatz von Cloud-Technologien und ihre Auswirkungen**

Ein wesentliches Ziel der Landesverwaltung ist es, durch die konsequente Nutzung von Virtualisierungs- und Automatisierungstechnologien Infrastrukturdienste aufzubauen und gegenüber den landesinternen Nutzern anzubieten, welche die Entwicklung und den Einsatz von Anwendungen in administrativer und technologischer Sicht erleichtern. Hierunter fallen insbesondere Technologien, die Anforderungen hinsichtlich IaaS und PaaS abbilden. Auf diesen Infrastrukturkomponenten aufbauend lassen sich neben individual entwickelten Fachanwendungen weitere Software-Dienste (SaaS) innerhalb des Landesverwaltungsnetzes bereitstellen. Hierzu zählen Standardprodukte beispielsweise für den Dateiaustausch, gemeinsames Arbeiten etc.

### **4.1 Möglichkeiten**

Dabei ergeben sich durch eine gezielt aufgebaute Cloud-Infrastruktur neue Möglichkeiten, die u. a. der IT-Entwicklung, dem IT-Betrieb aber auch den jeweiligen Nutzern der Fachverfahren zugutekommen.

Hierzu zählen:

- **Offenheit der IT-Dienste und Anwendungen**

In Übereinstimmung mit den in den IT-Standards des Landes verankerten Architekturvorgaben, ermöglichen entsprechende IT-Lösungen einen effizienten Einsatz in heterogenen bzw. einem stetigen Wandel unterliegenden IT-Umgebungen. Die Weiterentwicklung, das Verständnis der Anwendungen und Migrationsmöglichkeiten sind durch stark reduzierte oder standardisierte Abhängigkeiten optimiert (zum Beispiel bei Systemschnittstellen sowie keine bzw. reduzierte Abhängigkeiten von proprietären Standards).

- **Erhöhung von Skalierbarkeit und damit eine bedarfsgerechtere IT**

Durch den Einsatz entsprechender Technologien (zum Beispiel Containertechnologien) und einer auf Cloud-Prinzipien basierenden Architektur, sowie einem entsprechenden Deployment und Betrieb sind wesentliche Voraussetzungen geschaffen, um IT-Systeme schnell und bedarfsgerecht skalieren zu können (einschließlich Automatisierung).
- **Steigerung von Effizienz und Nachhaltigkeit (bei Entwicklung und Betrieb)**

Die verstärkte Nutzung von Standards und verfügbaren Vorprodukten (zum Beispiel vollständig vorkonfigurierte Entwicklungsumgebungen), sowie eine sehr effiziente, akut bedarfsgerechte und somit „elastische“ Skalierung (zum Beispiel mit Hilfe von Containermanagement) sorgt für eine einfachere, schnellere und ressourcenschonendere IT.
- **Zentrale Administration**

Durch zentrale Steuerung und Überprüfung von IT-Objekten, ergeben sich durchgängig von Back-End bis Front-End schnellere und effektivere Planungs- und Reaktionsmöglichkeiten. Dies schließt sämtliche Architektur- und Serviceebenen ein.
- **Zentral gespeicherte, aber inhaltlich und organisatorisch trennbare Daten**

Vorteile von zentralen Datenspeichern (zum Beispiel hinsichtlich Kosten, Administration, Skalierung und Redundanz) lassen sich mit den Bedürfnissen nach inhaltlich abgegrenzten und gesicherten Datenräumen verbinden. Aktuelle Technologien ermöglichen für Anwendungen und Anwender einfache, transparent nutzbare Datenspeicher (zum Beispiel mittels Ceph Storage Cluster und dessen Abbildung sowohl als Objekt-, Block- und Datei-Speicher).
- **Hoher Datenschutz und IT-Sicherheit**

Durch den richtigen Einsatz von einheitlichen und offenen Standards, Prozessen und entsprechenden Technologien in einer Cloud-Infrastruktur lässt sich ein hohes, meist sogar deutlich erhöhtes Niveau umsetzen. Einheitliche und datenschutzkonforme, zentral überwachbare Metriken erlauben eine möglichst frühzeitige Erkennung und Reaktion auf Sicherheitsvorkommnisse, sowie eine überprüfbare Umsetzung entsprechender Vorgaben in den jeweiligen Systemen und Teilkomponenten. Selbst betriebene Cloud-Dienste bieten im Gegensatz zu von Dritten betriebenen Cloud-Diensten die Voraussetzungen für ein hohes Datenschutz-Niveau. Insbesondere bei Anbietern, die ihren Hauptsitz außerhalb des Geltungsbereichs der DS-

GVO haben, bestehen große Herausforderungen bei der Einhaltung der gesetzlichen Vorgaben und der Gewährleistung der Grundrechte und Freiheiten der betroffenen Personen.

- **Bessere Steuerung der IT-Entwicklung**

Durch die deutlich direktere (automatisierte) und am fachlichen Bedarf und dessen Schwankungen orientierte Bereitstellung von IT-Dienstleistungen ergibt sich sowohl eine bessere Planungsgrundlage für die IT-Bedarfe (eine Cloud-Infrastruktur stellt entsprechende Daten für Bedarfsanalysen und darauf aufbauenden Prognosen zur Verfügung), als auch eine optimierte Bereitstellungskette von Ressourcen die sich effizient integrieren oder entfernen lassen.

- **Steigerung der Kundenorientierung und -zufriedenheit**

Durch eine bedarfsgesteuerte Self-service-basierte Anforderung von IT-Ressourcen, die daraufhin umgehend und automatisiert in der Cloud-Infrastruktur bereitgestellt werden, verringern sich die Aufwände und Zeiten bis zu deren Verfügbarkeit drastisch. Weiterhin sind für alle angebotenen Cloud-Ressourcen entsprechende Qualitätsnormen hinterlegt, bzw. auswählbar (zum Beispiel zu Mengengerüst, Performance, Verfügbarkeit) und werden für Kunden direkt einsehbar überwacht.

- **Stärkung von IT-Knowhow und -Leistungsfähigkeit (bzgl. moderner Technologien)**

Das für die Nutzung und den Betrieb einer Cloud-Infrastruktur notwendige Wissen ist kein Spezialwissen für singuläre Anwendungsfälle mehr, sondern Grundlage für die Umsetzung zukünftiger IT-Anforderungen. Von einer konsequenten Cloud-Strategie profitieren wissenstechnisch Anwender, Umsetzer und Betreiber von IT-Systemen. IT-Wissen in der aktuellen Ausbildung von Fachkräften und die sich entwickelnden Technologien basieren immer stärker auf Cloud-Aspekten.

- **Flexibilität im Technologie- und Produkteinsatz**

Durch die einer übergreifenden, einheitlichen Cloud-Infrastruktur innewohnende klare Strukturierung und Modularisierung ist ein deutlich flexiblerer Technologie- und Produkteinsatz realisierbar. Durch standardisierte Schnittstellen und Integrationsmöglichkeiten können die jeweils passenden Produkte zur Verfügung gestellt oder durch Austausch Optimierungen vorgenommen werden.

## 4.2 Grundlagen bilden

Um die genannten Möglichkeiten erschließen zu können und auch den Risiken beim Einsatz von Cloud-Diensten gezielt zu begegnen, sind über eine landesweite Cloud-Strategie

mit entsprechend verankerten Anforderungen und Rahmenbedingungen verschiedene Grundlagen zu entwickeln. Dazu gehören insbesondere:

- Wissen um potentielle Schwachstellen und Angriffspunkte von Cloud Technologien und ein entsprechender Umgang damit,
- Beherrschung der Betriebskomplexität von Cloud-Umgebungen,
- Absicherung von zentralisierten IT-Diensten auf einer geteilten Cloud-Plattform,
- Umgang mit zusätzlichen rechtlichen und regulatorischen Anforderungen,
- Prüfung und ggf. Ausrichtung der Entwicklungsartefakte an das Deployment in Cloud-Umgebungen,
- Stärkung der Zusammenarbeit zwischen Entwicklung und Betrieb der Anwendungen, u. a. durch Nutzung standardisierter Plattform-Dienste bzw. Organisationsmaßnahmen wie DevOps,
- rechts- und vorgabenkonforme Datenspeicherung,
- Abhängigkeiten zu bestehenden Verträgen,
- erhöhte Sorgfaltsanforderung bei der Auswahl von Dienstleistern, Produkten und Technologien,
- Berücksichtigung der Auswirkungen beim Entwurf und der Umsetzung von IT-Anwendungen (Komponentenarchitektur, Datenmodelle, genutzte Technologien etc.).

Diese Grundlagen fließen in die Leitprinzipien für den Einsatz von Cloud Technologien ein und sind bei den Handlungsschwerpunkten und der weiteren Umsetzungsplanung der Cloud-Strategie entsprechend zu berücksichtigen.

## **5 Leitprinzipien für den Einsatz von Cloud Technologien**

Der Einsatz von Cloud-Technologien und Cloud-Diensten in einer entsprechenden Cloud-Infrastruktur muss sich von verschiedenen Prinzipien leiten lassen, um effektiv, sicher und zielgerichtet zu erfolgen. Dazu gehören:

### **- Datenschutz**

Cloud-Lösungen dürfen nicht zu einer Verminderung des Datenschutz-Niveaus führen. Im Sinne der Cloud-Strategie zur Verfügung gestellte Lösungen, sollen grundsätzlich das allgemeine und das spezifische Datenschutz-Niveau erhöhen.

Die Verarbeitung von Daten unter der Hoheit des Landes ist eine wesentliche Voraussetzung, um langfristig Datenhoheit und hohe Datenschutz-Standards gewährleisten zu können und Datenabflüsse an bzw. Zugriffe durch Hersteller und sonstige



Dritte zu verhindern. Es ist auch darauf zu achten, dass Hersteller keine Daten zu eigenen Zwecken abgreifen.

- **Vertrauenswürdige Infrastruktur**

Cloud-Dienste müssen auf vertrauenswürdigen Infrastrukturen aufbauen, welche Authentizität, Zugriffskontrolle sowie die Datenhoheit für die Dienstverantwortlichen sicherstellen. Anerkannte Zertifikate und Testate für Cloud-Angebote, die den eigenen Sicherheitsanforderungen entsprechen, können als Faktor herangezogen werden, um die Einhaltung der Informationssicherheitsvorgaben zu beurteilen.

- **IT-Sicherheit**

Die spezifischen Sicherheitsanforderungen an Cloud-Lösungen bzw. einer Cloud-Infrastruktur müssen hinsichtlich der eingesetzten IT-Architekturen und Technologien berücksichtigt werden<sup>7</sup>. Dies gilt insbesondere für den Einsatz von Cloud-Diensten externer Anbieter im In- und Ausland, die nicht direkt den Vorgaben der Landes-IT unterliegen<sup>8</sup>.

- **Offenheit und Transparenz**

Der Einsatz von Cloud-Technologien erfordert Klarheit über die Leistung von angebotenen Cloud-Diensten sowie über zugehörige Bedingungen. Hierzu zählen insbesondere Funktionalität und Fähigkeit der angebotenen Lösung, Ort der Datenspeicherung und -verarbeitung, möglichen Zugriffen aus dem (nicht-EU-)Ausland, verwendete Technologien, Rechen- und Speicherleistung sowie ggf. ein Preismodell und ökologische Nachhaltigkeit (zum Beispiel Energieeffizienz und -verbrauch).

- **Architekturvorgaben für Cloud-Dienste**

Für die Nutzung von Cloud-Diensten sowie für die Entwicklung von Cloud-Lösungen sind die Vorgaben der VwV IT-Standards des Landes verbindlich. Hierbei ist vor allem der Einsatz offener Technologien und Schnittstellen zum einfachen und sicheren Datenaustausch und die Einhaltung von Standards, die eine leichte Datenmigration ermöglichen, zu berücksichtigen.

---

<sup>7</sup> Für Hinweise siehe auch die Broschüre des Bundesamt für Sicherheit in der Informationstechnik (BSI) „Sichere Nutzung von Cloud-Diensten“ - [https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Broschueren/Sichere\\_Nutzung\\_Cloud\\_Dienste.pdf?\\_\\_blob=publicationFile&v=9](https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Broschueren/Sichere_Nutzung_Cloud_Dienste.pdf?__blob=publicationFile&v=9)

<sup>8</sup> Siehe auch „Kriterienkatalog Cloud Computing C5“ des BSI - [https://www.bsi.bund.de/DE/Themen/DigitaleGesellschaft/CloudComputing/Kriterienkatalog/Kriterienkatalog\\_node.html](https://www.bsi.bund.de/DE/Themen/DigitaleGesellschaft/CloudComputing/Kriterienkatalog/Kriterienkatalog_node.html)

- **Souveränität und Selbstbestimmtheit**

Der Einsatz von Cloud-Technologien darf nicht Abhängigkeiten zu einzelnen Herstellern oder externen Beratungsunternehmen aufbauen oder verstärken. Die Vorgaben der VwV IT-Standards in Bezug auf Herstellerunabhängigkeit gelten gleichermaßen für die Nutzung von Cloud-Angeboten. Die hierzu erforderlichen Kompetenzen sollen intern aufgebaut werden.

- **Landesweite Wertschöpfung**

Cloud-Dienste sollen in der Breite der Landesverwaltung attraktiv sein und durch Mehrfachnutzung, durch Synergieeffekte oder neue Einsatzmöglichkeiten die Wertschöpfung von IT-Dienstleistungen und Anwendungen steigern.

- **Modularität und Interoperabilität**

Jeder Knoten der vernetzten Cloud-Infrastruktur als Teil der Cloud-Infrastruktur bildet eine eigenständige Einheit, folgt den Architekturvorgaben (falls vorhanden einer Referenzarchitektur) und ist eindeutig identifizierbar und erreichbar. Standardisierte Schnittstellen zum einfachen und sicheren Datenaustausch sind vorhanden, insbesondere mit der Möglichkeit durch neue beziehungsweise weitere Anwendungen genutzt zu werden.

- **Innovation**

Die Cloud-Strategie und die gemäß ihr umgesetzten Cloud-Dienste sollen ein Treiber für die IT-Innovation im Land, sowohl bei Betreibern wie auch Nutzern sein.

- **Automatisierung**

Integrierte und automatisierte Prozesse für Entwicklung und Betrieb sind eine wesentliche Grundlage für die Bereitstellung von Cloud-Diensten (inkl. Test).

- **Cloud-optimierte Anwendungen**

Neue Anwendungen sollen standardmäßig Cloud-fähig sein (Ausnahmen sind zu begründen) um in einer Cloud-Infrastruktur betrieben oder durch weitere Nutzer genutzt werden zu können.

- **Cloud-optimierte Technologien**

In der IT eingesetzte Technologien sollen Cloud-optimiert sein (um in einer Cloud-fähigen Anwendung eingesetzt zu werden), d.h. insbesondere diese sollen modular und zustandslos verwendbar, robust, flexibel und skalierbar, automatisch installier- und integrierbar, unabhängig von der darunterliegenden Infrastruktur, standardisiert (mit Parametrierung) nutzbar sein.

Neben diesen Leitlinien existieren rechtliche Rahmenbedingungen sowie nationale und internationale Standards, die hinsichtlich der Verwendung von Cloud-Diensten relevant und im Kontext der im Folgenden identifizierten Handlungsschwerpunkte und Aktivitäten zu betrachten sind. Diese reichen von Vorgaben hinsichtlich Datenschutz (DS-GVO) über Empfehlungen für einen sicheren Einsatz von Cloud-Diensten (zum Beispiel der Compliance Controls Catalogue C5 des Bundesamtes für Sicherheit in der Informationstechnik und die ISO 27000 Reihe) bis hin zu internationalen Standards und Definitionen, zum Beispiel NIST SP 800-145 (National Institute of Standards and Technology: Definition of Cloud Computing) sowie Empfehlungen von CERT EU und ENISA bzgl. Cloud-Computation.

## **6 Handlungsschwerpunkte**

Cloud-Technologien stellen gegenüber der herkömmlichen Bereitstellung von Produktionssystemen eine effiziente und wirtschaftliche Alternative dar. Zudem ermöglichen sie es, entsprechend virtualisierte Anwendungen flexibel auf verschiedenen Produktionsumgebungen zu betreiben. Um diese Vorteile im Sinne einer zukunftsfähigen Gesamtarchitektur nutzen zu können, bedarf es sowohl in organisatorischer als auch in technologischer Hinsicht entsprechender vorbereitender Maßnahmen sowie einer Einbettung in die Steuerungsprozesse der Landes-IT.

Die initiale Ausgestaltung, Durchführung, kontinuierliche Aktualisierung und Justierung dieser Maßnahmen ist Gegenstand der Planung und Umsetzung der Cloud-Strategie.

### **6.1 Organisatorische Maßnahmen**

Mit der VwV IT-Standards in der Neufassung vom 01.01.2020 wurde in Bezug auf die Entwicklung von Fachanwendungen der Fokus auf webbasierte Lösungen gelegt. Diese Vorgaben sind eine wichtige Grundlage, damit neue Fachanwendungen grundsätzlich auch als Cloud-Lösung betrieben werden können. Um dieses Ziel zu erreichen, sind jedoch weitere, im Folgenden genannte, Maßnahmen erforderlich.

#### **6.1.1 Konfiguration und Bereitstellung grundlegender Softwarelösungen für den Betrieb von Cloud-Infrastruktur**

Im Rahmen der Fortschreibung der VwV IT-Standards sind Vorgaben für die Anwendungsvirtualisierung, d. h. für die Erstellung in sich geschlossener Software-Pakete (Container), die innerhalb einer entsprechenden Container-Plattform betrieben werden können, erforderlich. Die entsprechenden konkreten Technologievorgaben werden in den IT-Standards des Landes durch den IT-Rat festgelegt. Darüber hinaus ist entlang der genannten Architekturvorgaben eine Konkretisierung der Zielarchitektur und des Technologieeinsatzes für Cloud-Computing vorzunehmen und in die IT-Strategie des Landes aufzunehmen.

Im Hinblick auf die Herstellerwahl als auch auf die Nutzung der am Markt verfügbaren fachlichen Funktionen lassen sich aufgrund des hohen Standardisierungsgrads von Cloud-Lösungen sowie eines oftmals vergleichbaren Produktportfolios der führenden Anbieter von Cloud-Diensten im Allgemeinen Synergien bilden. Für die Abstimmungsprozesse des Anforderungs- und Vorhabenmanagements sowie des Architekturmanagements sind dementsprechend potenzielle Grundverfahren zu identifizieren und im Rahmen einer ressortübergreifenden Gesamtstrategie zu planen.

Neben der Entwicklung neuer Fachanwendungen gilt es auch anhand anstehender bzw. absehbarer Bedarfe den Einsatz von Cloud-Lösungen externer Anbieter zu betrachten. Hierbei ist zu beachten, dass die organisatorische Umsetzung entlang der etablierten Regelprozesse, Strukturen und Verantwortlichkeiten erfolgt.

Grundsätzlich sind Anforderungen der Landesverwaltung an Cloud-Dienste in Bezug auf Infrastruktur-Self-Services und Containermanagement durch Maßnahmen zur Virtualisierung und Automatisierung abgedeckt. Darüber hinaus werden unter Beachtung der in den IT-Standards des Landes enthaltenen Vorgaben zur Anwendungsentwicklung Fachanwendungen bei Neuentwicklungen oder umfangreichen Änderungen als webbasierte Lösung konzipiert und implementiert. Der Betrieb dieser Anwendungen in Cloud-Umgebungen ist vorrangig vorzusehen. Weitere ergänzende Bedarfe an Cloud-Diensten werden über das Bedarfsmanagement erfasst und unter Berücksichtigung der strategischen Architekturplanung prozessiert.

Cloud-Services werden auf der Grundlage eines Service-Level-Agreements bereitgestellt, das alle wesentlichen Aspekte des entsprechenden Leistungsangebots in funktionaler und nicht-funktionaler Hinsicht enthält.

### **6.1.2 Aufbau des erforderlichen Know-hows**

Mit dem Aufbau von Cloud-Technologien verändern sich auch die Anforderungen an IT- und Fach-Architekten, Entwickler und weiteren IT-Rollen sowie insbesondere an das Betriebspersonal. In zunehmenden Maße sind Kenntnisse von Bedeutung, die über die reine System-Administration hinausgehen und Fähigkeiten im Hinblick auf die Entwicklung und das Lifecycle-Management von Systemen erfordern. Mit dem Begriff „Infrastructure-as-code“ wird dieser Prozess beschrieben.

Diese Veränderungen des Aufgabenzuschnitts und der technologischen Ausrichtung erfordern auch im Hinblick auf das Management der zugrundeliegenden Prozesse und ihrer Organisation Maßnahmen, die auf Führungsebene die technologische Neuausrichtung unterstützen. Sowohl auf Fach- als auch auf Führungsebene ist eine Erweiterung des bestehenden Know-hows vorzusehen.

Unabhängig von der Frage, in welchem Umfang Aufgaben im Zusammenhang mit dem Betrieb von Cloud-Technologien ausgelagert werden, ist der Aufbau landeseigenen Know-hows alleine schon für die Steuerung potenzieller Dienstleister essentiell. Das Verhältnis zwischen eigener und externer Leistung lässt sich dann im Anschluss an die Phase des Know-how-Aufbaus im Rahmen einer konkreten Umsetzungsstrategie festlegen. Für die Vergabe an externe Dienstleister sollte der interne Know-how-Aufbau ein wichtiges Kriterium darstellen.

Aber auch für die anderen, oben genannten Rollen, die sich vorrangig auf die Anwendungs- und Facharchitektur beziehen, sind detaillierte Kenntnisse über den Einsatz von Cloud-Technologien erforderlich. Hierbei geht es vor allem um Fähigkeiten im Zusammenhang mit der Virtualisierung von Anwendungen, die Nutzung von Plattformdiensten und die Einbindung bestehender Software-Dienste in die eigene Anwendung.

Grundsätzlich können im Rahmen von kleineren Teststellungen mit geringem Personalaufwand Erfahrungen mit Cloud-Technologien gewonnen werden. Eine sukzessive Ausweitung auf produktive Systeme ist möglich.

### **6.1.3 Organisatorische Veränderungen und Schnittstellen**

Der Aufbau von Cloud-Technologien erfordert über einen mehrjährigen Zeitraum und ggf. darüber hinaus den Parallelbetrieb von Cloud-basierten und Nicht-Cloud-basierten Anwendungen. Strukturen und Kompetenzen, die den herkömmlichen Betrieb sicherstellen, müssen erhalten bleiben, während neue Fähigkeiten und Verantwortlichkeiten sowohl im Betrieb als auch in der Entwicklung aufgebaut werden müssen. Wesentliche Änderungen sind dabei in der Zusammenarbeit zwischen diesen beiden Bereichen zu sehen, da durch die Virtualisierung der Infrastruktur die Grenzen zwischen Administration, Konfiguration und Programmierung nicht mehr trennscharf gezogen werden können. Die Bereitstellung von Cloud-Technologien in der gesamten Leistungskette ist daher als gemeinsame Aufgabe vieler unterschiedlicher IT-Rollen zu sehen, dessen optimales Zusammenwirken innerhalb der Organisation sichergestellt werden muss.

### **6.1.4 Ausweitung der Cloud-Infrastruktur**

Ausgehend von einem Kernteam aus Entwicklung und Betrieb, das die erforderlichen Rollen für einen zunächst stark begrenzten Leistungsumfang abdeckt, können weitere Dienste unter personeller Erweiterung des Kernteams in das Leistungsspektrum aufgenommen werden. Hierdurch ist eine schrittweise Weiterentwicklung unter Berücksichtigung der wahrzunehmenden gesamtheitlichen Betriebsverantwortung möglich.

### **6.1.5 Anpassung der landesinternen Vorgaben**

Landesinterne Vorgaben und Standards sollen hinsichtlich der Ziele und Prinzipien der Cloud-Strategie überprüft werden. Dazu gehören insbesondere die VwV IT-Standards, die Abstimmungsprozesse des Anforderungs- und Vorhabenmanagements sowie andere als relevant zu identifizierende Vorgaben.

## **6.2 Technologiebezogene Maßnahmen**

Mit dem Einsatz von Cloud-Technologien sind für die Landesverwaltung wesentliche Rahmenbedingungen verbunden, die einen sorgfältigen Umgang unter Berücksichtigung der in Kapitel 5 genannten Leitlinien erfordern. Für die landeseigene IT-Bereitstellung ist es essentiell, Cloud-Technologien einzuführen bzw. konsequent zu nutzen. Der hiermit verbundene Virtualisierungsgrad, der eine hochgradige Automatisierung des Betriebs sowie ein Continuous Deployment ermöglicht, ist als wesentlicher Faktor für die Konkurrenzfähigkeit, auch gegenüber anderen öffentlichen Rechenzentren, und somit für die Wirtschaftlichkeit der landesinternen IT-Dienstleistung zu verstehen.

Insbesondere aus technologischer und wirtschaftlicher Sicht ist es erforderlich, die vorhandenen Virtualisierungs- und Automatisierungsmaßnahmen auszuweiten. Ziel ist es daher, innerhalb der Landesverwaltung eine zentrale Cloud-Infrastruktur aufzubauen, die folgende Zielsetzung adressiert:

- Durchgängige Automatisierung und Einsatz von Virtualisierung im IT-Betrieb,
- Zentrale Bereitstellung von Lösungen zur Infrastruktur- und Anwendungsvirtualisierung für Kunden innerhalb der Landesverwaltung,
- Erfüllung fachlicher Anforderungen in Bezug auf konkrete Cloud-Services als auch hinsichtlich einer einfachen und ggf. eigenständigen Umsetzung,
- Mitwirkung an länderübergreifenden strategischen Cloud-Projekten,
- Einhaltung hoher Datenschutz- und Informationssicherheitsstandards und Schaffung einer ausgewogenen digitalen Unabhängigkeit.

Für diese Ziele sind bezüglich der Planung und Umsetzung entsprechende Strategien zu entwickeln und auszuarbeiten, die sich auf die verschiedenen Handlungsfelder beziehen. Hierzu zählen insbesondere eine Technologiestrategie, die alle relevanten Infrastrukturkomponenten umfasst, sowie eine darauf ausgerichtete Entwicklungsstrategie.

Der Aufbau einer Cloud-Infrastruktur innerhalb der Landesverwaltung ist unter dem Aspekt der effizienten Nutzung von IT-Ressourcen sowie einer bestmöglichen Souveränität gegenüber externen Anbietern am Markt ein wichtiger Bestandteil einer zukunftsfähigen IT-Strategie. Eine Cloud-Infrastruktur, die sich an diesen Zielen orientiert, ermöglicht zum einen den eigenständigen Umgang mit Daten und ist nicht von der deren Bereitstellung durch Dritte abhängig. Zum anderen ist sie Grundlage für einen effizienten und modernen

Entwicklungsprozess, der es erlaubt, Kernfunktionen der Landesverwaltung nach Bedarf in eigener Hoheit zu entwickeln und den Nutzern zur Verfügung zu stellen.

Für eine solche Infrastruktur sind in technologischer Hinsicht Handlungsfelder in den Bereichen Infrastruktur, Anwendungsvirtualisierung und Containermanagement vorzusehen, die zunächst unabhängig voneinander betrachtet werden können, perspektivisch jedoch aufeinander aufbauen. In Bezug auf die Infrastruktur geht es um die Bereitstellung einer technischen Cloud-Infrastruktur, mit der sich skalierbare virtuelle Rechner über webbasierte Schnittstellen konfigurieren und auf Anforderung als Infrastruktur-Dienste unmittelbar bereitstellen lassen. Hierdurch können zum einen die vom Landesrechenzentrum verwalteten Server effizienter verwaltet werden. Zum anderen werden Self-Services zur Bereitstellung virtueller Server für weitere Nutzer innerhalb der Landesverwaltung ermöglicht, die gleichzeitig den administrativen Aufwand reduzieren.

Auf einer solchen IaaS-Umgebung kann die Anwendungsvirtualisierung einschließlich dem Containermanagement aufbauen. Dieser Schritt kann prinzipiell auch losgelöst von einer IaaS-Umgebung umgesetzt werden. Bei der Anwendungsvirtualisierung sind insbesondere zwei Aspekte zu betrachten: Zum einen können durch die Erstellung in sich geschlossener Software-Pakete im Rahmen des Entwicklungsprozesses Anwendungen plattformunabhängig in beliebigen dafür vorgesehenen Container-Umgebungen installiert werden. Zum anderen lassen sich derartige virtualisierte Anwendungen automatisiert betreiben. Dies schließt die Skalierung von Anwendungen sowie die Gewährleistung der Hochverfügbarkeit ein.

Eine solche Schichtung ist grundsätzlich als Zielarchitektur vorzusehen, um eine durchgängige Virtualisierung und Automatisierung zu erreichen. Für die Umsetzung dieses Handlungsfeldes ist dies jedoch keine Voraussetzung. Vielmehr lässt sich die vorrangige Fokussierung der Anwendungsvirtualisierung nutzen, um bereits heute bestehende fachbezogene Anforderungen umzusetzen. Die weitere Virtualisierung hin zur Infrastruktur erfolgt dann anhand konkreter fachlicher und technischer Bedarfe deren Nutzen sukzessive erkennbar ist.

Für die Ebene der Anwendungsvirtualisierung ist dabei zu beachten, dass sie keine produktbezogenen Abhängigkeiten zur darunterliegenden (virtuellen) Infrastrukturebene aufweist. Nur so lassen sich unabhängig von der bereitgestellten Container-Plattform unterschiedliche Technologien zur Infrastrukturvirtualisierung einsetzen. Durch die Trennung der Anwendungsvirtualisierungs- und Infrastrukturvirtualisierungsschicht werden Abhängigkeiten von Produkten und Herstellern vermieden.

Zur Umsetzung sind nachfolgende Kategorien innerhalb der Cloud-Infrastruktur einzurichten:

Kategorie	Beispiele (nicht vollständig)
<b>Rechenleistung</b>	<ul style="list-style-type: none"> <li>• Virtuelle oder „Bare-Metal“ Rechner,</li> <li>• Cloud functions (Serverless functions)</li> </ul>
<b>Speicher</b>	<ul style="list-style-type: none"> <li>• Blockspeicher,</li> <li>• Objektspeicher,</li> <li>• Dateispeicher,</li> <li>• Datenbanken</li> </ul>
<b>Netzwerk</b>	<ul style="list-style-type: none"> <li>• Virtuelle Netzwerke,</li> <li>• Load-Balancing,</li> <li>• Firewalls,</li> <li>• Virtual Private Clouds<sup>9</sup>,</li> <li>• DNS</li> </ul>
<b>Sicherheitsfunktionen</b>	<ul style="list-style-type: none"> <li>• Identity und Access Management,</li> <li>• Threat Detection,</li> <li>• Data Loss Prevention</li> <li>• Container-Sicherheit</li> </ul>
<b>Container</b>	<ul style="list-style-type: none"> <li>• Container-Instanzen (Möglichkeit zur Nutzung von Containern auf Docker-Basis)</li> <li>• Container-Register (erleichtert das Speichern, Verwalten und Bereitstellen von Container-Images)</li> </ul>
<b>Containermanagement</b>	<ul style="list-style-type: none"> <li>• Container-Dienst (skalierbarer, schneller Container-Management-Service zum leichteren Ausführen, Beenden und Verwalten von Containern)</li> <li>• Container-Orchestrierung (zur effizienteren Orchestrierung von Containern auf Basis von Kubernetes)</li> </ul>

---

<sup>9</sup> Virtual Private Clouds bezeichnen Cloud-Dienste, die durch einen öffentlichen Cloud-Anbieter mit Hilfe entsprechender Sicherheitsvorkehrungen isoliert von anderen Organisationen zur Verfügung gestellt werden und hierdurch eine private Einheit bilden.



Nachfolgende Tabelle fasst die wesentlichen Handlungsstränge zusammen:

Organisatorische Maßnahmen	
O1	Entwicklung von Vorgaben für die Anwendungsvirtualisierung
O2	Konkretisierung der Zielarchitektur für Cloud-Computing
O3	Identifikation von potentiell Cloud-fähigen Grundverfahren im Rahmen einer ressortübergreifenden Gesamtstrategie
O4	Bedarfe bzgl. des Einsatzes von Cloud-Lösungen externer Anbieter bewerten
O5	Maßnahmen zur Virtualisierung und Automatisierung planen und umsetzen
O6	IT-Standards des Landes hinsichtlich Vorgaben zur Anwendungsentwicklung überarbeiten
O7	Erstellung von Service-Level-Agreements für landesintern entwickelte und bereitgestellte Cloud-Services
O8	Aufbau landeseigenen Know-hows bzgl. Cloud-Computing
O9	Durchführung kleinerer Teststellungen
O10	Stärkung der Zusammenarbeit zwischen Entwicklung und Betrieb
O11	Landesinterne Vorgaben und Standards hinsichtlich der Ziele und Prinzipien der Cloud-Strategie überprüfen
Technologische Maßnahmen	
T1	Ausweitung der Virtualisierungs- und Automatisierungsmaßnahmen
T2	Erstellung einer Technologie- und Entwicklungsstrategie für Cloud-Computing
T3	Bereitstellung einer technischen Cloud-Infrastruktur
T4	Virtualisierung der Anwendungsebene

## **7 Planung und Umsetzung der Cloud-Strategie**

Die Planung und Umsetzung der Cloud-Strategie obliegt dem Ministerium für Inneres, Migration und Digitalisierung. Im Sinne einer landesweiten IT-Strategie und einem ressortübergreifenden gemeinsamen Vorgehen erfolgt hierbei eine enge Abstimmung mit dem Architekturboard der Landesverwaltung.

### **7.1 Planung / Initialisierung**

#### **7.1.1 Design der Cloud-Architektur**

Ausgangspunkt für den Aufbau und Einsatz von Cloud-Infrastrukturen ist ein Zielbild, das die Bedürfnisse der Landesverwaltung abdeckt und eine Vision in Bezug auf den Technologieeinsatz und dessen Nutzung beinhaltet. Dieses Zielbild ist in Ergänzung zu den durch die Evaluierung der BITBW erreichten Ergebnissen zur Mission und Vision sowie dem zukünftigen Leistungsportfolio der BITBW zu konkretisieren.

Für das Design der Cloud-Architektur sind einhergehend mit einer Analyse des Geschäftswerts die strategischen Prioritäten festzulegen. Diese beantworten insbesondere die Frage, welche grundlegenden Dienste hinsichtlich der Bereitstellung von Cloud-Infrastrukturen in Eigenleistung erbracht werden oder durch externe Anbieter ausgeführt werden.

#### **7.1.2 Cloud Portfolio Migration und Modernisierung**

Cloud-Technologien werden sich auch für die Landesverwaltung in zunehmenden Maße zum zentralen Bestandteil der IT-Infrastruktur und des IT-Service-Portfolios entwickeln und nicht Cloud-basierte Dienste nach und nach weitgehend verdrängen. Das hierzu erforderliche Know-how sowie die zugehörigen Aktivitäten sollten in einem ggf. zunächst virtuellen Cloud-Kompetenzzentrum innerhalb des Landesrechenzentrums BITBW gebündelt werden. Die von diesem Kompetenzzentrum bereitgestellten Services sind auf Basis der Cloud-Architektur und den Anforderungen der Landesverwaltung in einem ersten Schritt zu identifizieren, planen und zu bewerten.

#### **7.1.3 DevOps Transformation**

Als Grundlage für die weitere Entwicklung und Migration hin zu Cloud-basierten Diensten und deren effiziente Bereitstellung ist ein passendes DevOps-Vorgehen zu entwerfen und einzuführen.

Wichtig für diesen DevOps Ansatz ist eine enge und methodische Zusammenarbeit von Entwicklungs- und Betriebs-Teams die auf einer einheitlichen Tool-Chain und definierten Bereitstellungsprozessen basiert. Dabei müssen manuelle Schritte weitestgehend durch

standardisierte Automatisierungen ersetzt werden (zum Beispiel mittels Release-Automatisierung) und Status und Verlauf mittels passender Key-Performance-Indikatoren messbar und damit nachvollzieh-, steuer- und planbar sein.

## **7.2 Migrationsvorbereitung**

Eine effiziente Grundlage für eine Migration von Anwendungen in eine Cloud-Umgebung ist eine kontinuierliche Modernisierung der jeweiligen Anwendungsarchitektur. Dies gilt insbesondere für die Identifikation und Bereitstellung von Microservices.

Dies wird über die IT-Standards und Architekturvorgaben des Landes unterstützt und sollte in entsprechenden Pilotprojekten gefördert werden.

## **7.3 Aufbau**

Gemäß der identifizierten Bedarfe und entsprechender Pilotprojekte erfolgt ein sukzessiver Cloud-nativer Aufbau und Rollout von Anwendungen. Insbesondere Anwendungen mit einer Microservice-Architektur, die ein hohes Wiederverwendungspotential aufweisen und / oder für die ein entsprechender Bedarf besteht, sollten vorrangig umgesetzt werden.

## **7.4 Management**

Um eine effektive und den Leitprinzipien für den Einsatz von Cloud Technologien entsprechende Umsetzung, Betrieb und Nutzung von Cloud-Anwendungen bzw. -Diensten zu ermöglichen, sind entsprechende Prozesse zur Steuerung und Aufrechterhaltung der Einsatzfähigkeit notwendig. Diese basieren auf der Möglichkeit einer jederzeit transparenten Zustandsermittlung (in Echtzeit) der Cloud-Infrastruktur und entsprechender Indikatoren.

Hierzu sind passende und datenschutzkonforme Monitoring- und Management-Plattformen notwendig, die in Echtzeit automatisiert Zustand und Übereinstimmung mit definierten Key-Performance-Indikatoren überwachen und in die weitergehenden Betriebs-, Planungs- und Entwicklungsprozesse eingebunden sind.

Nur so ist eine entsprechend umfangreiche Cloud-Landschaft beherrschbar, insbesondere wenn diese aus Cloud-Diensten besteht, die von unterschiedlichen Dienstleistern bereitgestellt werden (Hybrid-Cloud mit Diensten bezogen von unterschiedlichen Privat- und Public-Clouds).

Auf der organisatorischen Ebene sind begleitend Maßnahmen des Change Managements durchzuführen.

## **8 Risiken hinsichtlich der Umsetzung**

Der Einsatz von Cloud-Technologien eröffnet neue Möglichkeiten und Handlungsspielräume. So vielfältig sich die Chancen darstellen, bestehen auch Risiken, die sich u. a. auf

eine mangelnde Berücksichtigung der Informationssicherheit und des Datenschutzes oder den Aufbau von Abhängigkeiten zu Anbietern von Cloud-Technologien beziehen.

Grundsätzlich kann und muss diesen Risiken durch eine sorgfältige Analyse der Anforderungen, Planung der Umsetzung und Auswahl der Hersteller begegnet werden. Wie alle weitreichenden Technologieentwicklungen können auch Cloud-Technologien sowohl zu einer Verbesserung als auch, bei einer mangelnden Berücksichtigung der Sicherheitsanforderungen, zu einer Verschlechterung des IT-Sicherheitsniveaus sowie einer deutlichen Beeinträchtigung der IT-Gesamtarchitektur führen.

Hierbei ist ebenfalls zu beachten, dass eine enge Bindung an einen Cloud-Provider zu erheblichen Problemen führen kann, beispielsweise im Fall von Rechtsstreitigkeiten oder Systemausfällen<sup>10</sup>. Die Risiken eines Vendor Lock-in können durch eine konsequente Nutzung offener Standards und von Freier und Open Source Software deutlich reduziert werden.

Für die IT der Landesverwaltung ist der Aufbau einer Ziel-Architektur für Cloud-Computing sowie eine Technologiestrategie, welche die hierdurch entstehenden weitreichenden Handlungsspielräume aufgreift und nutzt, unerlässlich. Ansonsten besteht die Gefahr, dass die Planbarkeit und Steuerbarkeit der IT-Architektur beeinträchtigt wird und sich zudem der technologische Abstand nicht nur zu privatwirtschaftlichen Anbietern von Cloud-Diensten, sondern auch zu IT-Dienstleistern anderer Bundesländer sowie kommunalen Dienstleistern vergrößert. Der Erfolg der Cloud-Strategie hängt jedoch in hohem Maße auch mit der Verfügbarkeit adäquat ausgebildeter IT-Fachkräfte zusammen. Dem Risiko unzureichendem Know-hows muss frühzeitig begegnet werden.

---

<sup>10</sup> Die Europäische Agentur für Netz- und Informationssicherheit (ENISA) sieht im sog. Vendor Lock-in daher ein hohes Risiko bei der Cloud-Nutzung. *Siehe Cloud Computing Security Risk Assessment*, [https://resilience.enisa.europa.eu/cloud-security-and-resilience/publications/cloud-computing-benefits-risks-and-recommendations-for-information-security/at\\_download/file](https://resilience.enisa.europa.eu/cloud-security-and-resilience/publications/cloud-computing-benefits-risks-and-recommendations-for-information-security/at_download/file)