Bericht

Prüfung Strategische IT-Planung

003-3/199/21-2018

Dezember 2018

LAND SALZBURG

LRH

LANDESRECHNUNGSHOF

Impressum

Auskunft	Salzburger Landesrechnungshof Nonnbergstiege 2 5020 Salzburg Postfach 527 5010 Salzburg
Telefon	+43 662 8042 3500
Fax	+43 662 8042 3880
E-Mail	landesrechnungshof@salzburg.gv.at
Internet	www.lrh-salzburg.at
Herausgeber	Salzburger Landesrechnungshof Nonnbergstiege 2 5020 Salzburg
Redaktion	Salzburger Landesrechnungshof
Herausgegeben	Salzburg, Dezember 2018
Zahl	003-3/199/21-2018
Druck	Amt der Salzburger Landesregierung, Hausdruckerei
Bildnachweis	-

Kurzfassung

Die Fachgruppe 0/2 - Informatik und Interne Dienste („LI“) ist u.a. für die Auswahl, Integration und Betreuung von Fremd- und Standardsoftware im Client- und Serverbereich verantwortlich; sie ist vor allem für die Gestaltung, Installation und Betreuung der dezentralen, bei Kunden eingesetzten Hardware-, Software- und Telefoneinrichtungen, des Landesnetzwerkes sowie der daran angeschlossenen Server und Telefonanlagen einschließlich der zugehörigen Systemsoftware, Sicherheits- und Notfallmaßnahmen zuständig. Die LI verfügt über viele schriftliche Unterlagen, die Ihre Organisation betreffen. Ihr Organisationshandbuch aus dem Jahr 2015 hat die LI laufend weiterentwickelt, ohne dies jedoch mit der Landesamtsdirektion offiziell abzustimmen. Auch scheint der Landesamtsdirektor in keinem der beschriebenen Abläufe als Abteilungsleiter und als Vorstand des Inneren Dienstes als Verantwortlicher auf.

Um die regelmäßige, systematische Kontrolle des Internen Kontrollsystems zu erleichtern, empfiehlt der Landesrechnungshof, für die LI eine aktuell gehaltene, einheitliche Organisationsrichtlinie für verbindlich zu erklären. Wenn die IT-Strategie berührt ist, sollten neben dem Büro des Landesamtsdirektors und der LI auch andere strategierelevante Dienststellen des Landes einbezogen werden.

Der Landesamtsdirektor erklärt, dass seine Steuerungskompetenz in den IT-Prozessen im laufenden Projekt „Salzburg@2022“ verankert wird; auch die Prozesse in der LI werden angepasst. Die IT-Werte seien aufgrund der Empfehlung des Landesrechnungshofs bereits präzisiert worden.

Das Land Salzburg verfügt über kein IT-Leitbild. Die Organisationsrichtlinie der LI enthält allerdings Aussagen zu ihrer Positionierung und Werte-Ziele für die Mitarbeitenden. Die Richtlinie behandelt auch die Steuerung der LI und stellt die Hauptprozesse dar, die in der LI laufen und nennt Maßstäbe, die einzuhalten sind, wenn etwa neue Systeme in der IT eingeführt werden. Die LI regelt die Beschaffung, Entwicklung und Verwendung von Software. Über Jourfixes und Strategie-Workshops hält die LI Kontakt mit den IT-Anwendern.

Die Informatikstrategie aus dem Jahr 2008 wurde nicht wie vorgesehen alle zwei bis drei Jahre weiterentwickelt. Der Landesrechnungshof fordert, eine IT-Strategie des Landes zu entwickeln und in einem verbindlichen, mit dem Landesamtsdirektor abgestimmten Dokument zusammenzufassen. Die Aktualität der neuen IT-Strategie soll regelmäßig evaluiert und alle zwei bis drei Jahre weiterentwickelt werden. Um den Aufwand für externe Beratungen bei der Vergabe von IT-Leistungen zu mindern, empfiehlt der Landesrechnungshof, diese Vergaben an zentraler Stelle des Amtes abzuwickeln.

Der Landesamtsdirektor erklärt, dass die LI die IT-Strategie laufend angepasst und mit ihm abgestimmt habe. Ende des Jahres 2018 soll die IT-Strategie evaluiert und gemäß den übergeordneten strategischen Vorgaben neu ausgerichtet werden.

Der Landesrechnungshof empfiehlt, eine Stelle einzurichten, die dezentrale Organisationsprojekte und Applikationen steuert, deren Kosten und Nutzen analysiert und sie evaluiert. Der Landesamtsdirektor erklärt, dass dezentrale Organisationsprojekte grundsätzlich in der Verantwortung der einzelnen Dienststellen liegen. Besonders komplexe Organisationsprojekte dezentraler Dienststellen sowie Dienststellen übergreifende Projekte werden seit Mitte des Jahres 2018 von einer zentralen Stelle im Büro des Landesamtdirektors gesteuert. Noch im Jahr 2018 sollen in der Landesverwaltung neue Standards für Projektmanagement eingeführt werden.

Das Land Salzburg verfügt über Pläne, mit welchen Maßnahmen die strategischen IT-Ziele erreicht werden sollen. Ihre eigene Tätigkeit bewertet die LI mittels Kennzahlen. Diese werden jährlich mit dem Landesamtdirektor abgestimmt.

Die LI verfügt über eine verbindliche Leitlinie, wie die IT-Sicherheit der Landesverwaltung zu gewährleisten ist. Das Sicherheitsmanagement ist als kontinuierlicher Prozess mit konkreten Aufgaben konzipiert. Bei der Sicherheitsanalyse orientiert sich die IT-Sicherheitsrichtlinie am „Österreichischen Informationssicherheitshandbuch" sowie an internationalen Normen. Die Richtlinie bestimmt auch, wie das Risikomanagement zu organisieren ist und welche Technologien zur Datensammlung zu verwenden sind. Neue und bestehende Anwendungen sind drei Schutzbedarfskategorien zuzuordnen, für die unterschiedliche Sicherheitsmaßnahmen gelten.

Die LI verfügt über ein automatisiert gesteuertes Lizenzmanagement, ein zentrales Identity-Management sowie vom Schutzbedarf abhängige Mechanismen zur Authentifizierung.

Das Datenmanagement umfasst die Planung, Überwachung und Steuerung aller verwendeten Datenbestände. Die LI deckt vor allem die Analyse, Modellierung, Beschaffung, Sicherung und Sicherheit von Daten ab.

Der Landesrechnungshof empfiehlt der LI, alle zwei bis drei Jahre zu überprüfen, ob an externe Dienstleister ausgelagerte datenschutzrechtliche Verpflichtungen eingehalten werden. Der Landesamtsdirektor erklärt, externe Dienstleister datenschutzrechtlich künftig durch unabhängige, spezialisierte Firmen überprüfen zu lassen.

Inhaltsverzeichnis

Abkürzungsverzeichnis/Glossar

A

Application Service Providing – ASP	Der Application Service Provider bzw. Anwendungsdienstleister ist ein Dienstleister, der eine Anwendung zum Informationsaustausch über ein öffentliches Netz oder über ein privates Datennetz anbietet.

B

Bitlocker	BitLocker ist eine Festplattenverschlüsselung des Unternehmens Microsoft
BSI	Bundesamt für Sicherheit in der Informationstechnik

C

CAD	Computer-aided design, rechnerunterstütztes Konstruieren
Cloud-Lösung	Cloud Computing beschreibt die Bereitstellung von IT-Infrastruktur wie etwa Speicherplatz, Rechenleistung oder Anwendungssoftware als Dienstleistung über das Internet.

D

DSGVO	Datenschutzgrundverordnung

E

ELAK	Elektronischer Akt, Bundesweites System der elektronischen Aktenverarbeitung in Österreich.
ERP	Enterprise Resource Planning, übersetzt Geschäftsressourcenplanung. SAP ERP ist das wesentliche Hauptprodukt des deutschen Software-Unternehmens SAP.

G

GIS-Format	Standardisierte Datenformate von Geoinformationssystemen

I

Identity Management	Zielgerichteter und bewusster Umgang mit Identität, Anonymität und Pseudoanonymität.
IKS	Internes Kontrollsystem
Integrität	bezeichnet die Sicherstellung der Korrektheit (Unversehrtheit) von Daten und der korrekten Funktionsweise von Systemen.
ISO/IEC	Internationale Organisation für Normung; Internationale elektrotechnische Kommission.
ISO/IEC 27001	spezifiziert die Anforderungen für Einrichtung, Umsetzung, Aufrechterhaltung und fortlaufende Verbesserung eines dokumentierten Informationssicherheits-Managementsystems unter Berücksichtigung des Kontexts einer Organisation.
IT	Information Technology, Informationstechnik

J

jPISA	Projektinformationssystem zur auftragsbezogene Zeiterfassung, Kostenplanung und -verfolgung von Projekten.
JIRA	System um Vorgänge, Fehler und Aufgaben dienststellenübergreifend und nachvollziehbar zu dokumentieren. Die Vorgänge können dabei Mitarbeitern zugeteilt oder nach definierten Workflows abgearbeitet werden. Derzeit wird Jira vorwiegend für die Umsetzung von Softwareprojekten herangezogen.

L

Landesinformatik	Fachgruppe 0/2 - Informatik und Interne Dienste
LI	Fachgruppe 0/2 - Informatik und Interne Dienste
LINUX	ein freies Betriebssystem, Open Source Software

O

Office	Microsoft Office Komponenten sind etwa Word, Excel, PowerPoint, Outlook.
Open Source Software	ist eine Computersoftware, deren Quellcode unter einer Lizenz veröffentlicht wird, in der der Urheber die Rechte zum Studium, Ändern und Verteilen der Software an jedermann und für jeden Zweck gewährt.
Opentext archiv	stellt ein unternehmensweites Repository für die Langzeitarchivierung auf verschiedensten Speichermedien dar.
OrgRL	Organisationsrichtlinie

P

Portalverbund	Gemeinsame Infrastruktur für verwaltungsübergreifende Zusammenarbeit mittels Zusammenschluss von Verwaltungsportalen.

S

SAP	ist ein Hersteller von Enterprise-Resource-Planning-Systemen. Der Begriff „SAP“ gilt heute als Abkürzung für Systeme, Anwendungen, Produkte in der Datenverarbeitung. Er wird auch als Synonym für das Hauptprodukt der Firma SAP verwendet.
Security Policy	Eine Sicherheitsrichtlinie beschreibt den erstrebten Sicherheitsanspruch einer Institution. Mit „Sicherheit“ ist hier normalerweise „Informationssicherheit“ gemeint.
Software im Clientbereich	bezeichnet die auf dem Endgerät eines Netzwerks installierte Software, die mit einem Server (Zentralrechner) kommuniziert.
SVAK	Salzburger Verwaltungsakademie

U

u.a.	unter anderem
USP	Unternehmensservice Portal, eines zentralen Internetserviceportals für Unternehmen zur Unterstützung beim elektronischen Austausch von Informationen zwischen Teilnehmern (Transaktionen) und bei der Bereitstellung von Informationen.

Abbildungsverzeichnis

Literaturverzeichnis

BSI - Bundesamt für Sicherheit in der Informationstechnik. (27. 11 2018). Von https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/Glossar/glossar_node.html abgerufen

Lutz J., H., Riedl, R., & Stelzer, D. (11. Auflage 2014). *Informationsmanagement*. De Gruyter Oldenbourg.

1. Prüfungsgrundlagen

1.1 Anlass der Prüfung

(1) Der Landesrechnungshof setzte die Prüfung als Teil des Prüfungsprogramms 2018 um.

1.2 Gegenstand und Umfang der Prüfung

(1) Der Prüfauftrag lautete „Ziele und Strategien der Informationstechnologie (IT) im Amt der Salzburger Landesregierung samt Bestandsaufnahme von Software und Datenbeständen". Im Fokus stand die Strategie des Jahres 2018.
Nicht Gegenstand der Prüfung war(en)

- die Agenden des Referates 0/24 – Landesstatistik und Verwaltungscontrolling;
- die Umsetzung datenschutzrechtlicher Vorgaben;
- ob und in welchem Ausmaß die LI in der Praxis entsprechend den der Prüfung zugrundeliegenden schriftlichen Unterlagen vorgegangen ist.

1.3 Angewendete Prüfnorm und abgestrebte Prüfungssicherheit

(1) Die Prüfung erfolgte in Anlehnung an die Grundsätze, die der Europäische Rechnungshof anwendet.

Den Umfang seiner Prüfungshandlungen richtete der Landesrechnungshof danach aus, eine begrenzte Prüfungssicherheit zu erreichen. Dies bedeutet, dass eine Aussage nur über jene Sachverhalte getätigt wird, die auch konkret geprüft wurden.

1.4 Prüfungsziel und Prüfungsmaßstab

(1) Ziel war es, durch Einblick in die Dokumentation der LI festzustellen, ob die IT-Ziele und Strategien den Anforderungen und Standards entsprechen.

1.5 Zeitlicher Ablauf der Prüfung

(1) Nach der schriftlichen Ankündigung der Prüfung durch den Landesrechnungshofdirektor im Februar 2018, erfolgte das Startgespräch zur Prüfungsdurchführung mit der Fachgruppe 0/2 (Informatik und Interne Dienste) im April 2018. Die Schlussbesprechung mit den Verantwortlichen der Fachgruppe fand am 20. September 2018 statt.

1.6 Aufbau des Berichtes

(1) Vom Landesrechnungshof festgestellte Sachverhalte sind mit „(1)“ gekennzeichnet.

Die Bewertungen von Sachverhalten samt allfälligen Anregungen und Empfehlungen sowie Bemängelungen und Beanstandungen sind mit „(2)“ gekennzeichnet. Diese werden zusätzlich durch Schattierung hervorgehoben.

Die zusammenfassende Gegenäußerung der Landesverwaltung - für diese abgegeben vom Amt der Salzburger Landesregierung - wird kursiv dargestellt und ist mit „(3)“ kodiert[1] . Die vollständige Gegenäußerung ist dem Bericht als Anlage angeschlossen.

Eine abschließende Äußerung des Landesrechnungshofes ist mit „(4)“ gekennzeichnet und durch Schattierung hervorgehoben.

Um den Bericht übersichtlich zu gestalten, wurde das enthaltene Zahlenwerk fallweise gerundet. Auch wurden in einigen Fällen, um Entwicklungen besser veranschaulichen zu können, Daten über den geprüften Zeitraum hinaus dargestellt.

Im Bericht verwendete geschlechtsspezifische Bezeichnungen gelten grundsätzlich für Frauen und Männer.

[1] In Einzelfällen sind Gegenäußerungen, die lediglich den Sachverhalt betreffen, als Fußnote eingefügt.

2. Strategische IT-Planung

2.1 Organisation und Internes Kontrollsystem (IKS):

(1) Die zentrale Steuerungskompetenz für den Inneren Dienst liegt bei der Landesamtsdirektion[2]. Diese Kompetenz umfasst auch die Festlegung von Rahmenbedingungen und die Entwicklung von Strategien für die Organisation der Landesverwaltung.

Die Fachgruppe 0/2 - Informatik und Interne Dienste (hier Landesinformatik genannt und mit „LI“ abgekürzt) ist u.a. für die Auswahl, Integration und Betreuung von Fremd- und Standardsoftware im Client- und Serverbereich verantwortlich; sie ist vor allem für die Gestaltung, Installation und Betreuung der dezentralen, bei Kunden eingesetzten Hardware-, Software- und Telefoneinrichtungen, des Landesnetzwerkes sowie der daran angeschlossenen Server und Telefonanlagen einschließlich der zugehörigen Systemsoftware, Sicherheits- und Notfallmaßnahmen zuständig. Weiters obliegt der Fachgruppe die strategische Planung, die IT-Architektur und das Sicherheitsmanagement.

Ihre eigene Organisation betreffend, verfügt die LI über schriftliche Unterlagen zu folgenden Themen:

- Aufbauorganisation
- Prozesse
- Strategie Informatik
- dienstliche Regelungen
- Sekretariatsorganisation
- Interne Services und Organisationsrichtlinie (OrgRL).

Die Unterlagen zu diesen Themen sind weiter untergliedert und teilweise durch Diagramme erläutert. Der Abschnitt „Prozesse“ gliedert sich in die Abläufe „Leitung Landesinformatik“, „IT-Kundendienst“, „IT-Infrastruktur“ und „Landesstatistik“. Jeder Prozess enthält auch auf ihn abgestimmte, konkrete Risiko-Tatbestände, für den Fall ihres Eintritts vorgesehene Maßnahmen sowie Nachweise und Dokumentationen darüber.

[2] Seit 1. Oktober 2017 ist das Referat 0/01 – Büro des Landesamtsdirektors für die zentrale Steuerung verantwortlich; davor war das Referat 0/02 – Zentrale Aufgaben und Strategien dafür zuständig (Geschäftseinteilung des Amtes der Landesregierung LGBl. Nr. 81/2014, zuletzt geändert durch LGBl. Nr. 87/2017).

Die LI verfügt über ein Organisationshandbuch aus dem Jahr 2015. Darauf aufbauend hat die LI ihre Organisationsregeln in einer OrgRL laufend weiterentwickelt; diese ist für alle Mitarbeitenden der LI über das Intranet abrufbar. Eine formale Zustimmung des Landesamtsdirektors zum Inhalt der OrgRL fehlt allerdings.

Die OrgRL erfüllt die an ein Handbuch gestellten Anforderungen, indem sie die Aufgaben und die Kooperationsbeziehungen zwischen Organisationseinheiten der Abteilung sowie einzelnen Mitarbeitenden darstellt. Dies gilt auch für die Befugnisse und Verantwortungsbereiche sowie die Vertretungsregelungen der einzelnen Mitarbeitenden. Die aus der hierarchischen Ordnung folgenden Weisungszusammenhänge sind allerdings nicht vollständig abgebildet. Keiner dieser Prozesse berücksichtigt die zentrale Steuerungskompetenz des Landesamtsdirektors (z.B. Steuerung der LI, IT-Architekturstandards).[3]

Die OrgRL enthält auch Prozessbeschreibungen für 34 Prozesse, die den grundsätzlichen Anforderungen eines Internen Kontrollsystems (IKS) entsprechen. Die Prozesse sind in vier Gruppen unterteilt (Abläufe Leitung Landesinformatik; Abläufe IT-Kundendienst; Abläufe IT-Infrastruktur sowie Abläufe Landesstatistik, die seit Oktober 2017 Teil der Fachgruppe 0/2 ist). Eine Wertung innerhalb der Gruppe ist nicht erkennbar.

Grundsätzlich beinhaltet die Darstellung dieser Prozesse Ablaufdiagramme, die Beschreibung der Risiken, allfällige Gegenmaßnahmen und die Dokumentation dieser Maßnahmen.

Die einzelnen Prozesse sind unterschiedlich und inhomogen dargestellt. Dies ist darauf zurückzuführen, dass die Formulierungen auf den Erfahrungswerten der zuständigen Führungskräfte basieren. Einige Prozesse, wie etwa „Rechnungslegung-Eingangsrechnungen“ und „Softwareentwicklungsvorhaben“ werden sehr kurz und strukturiert beschrieben; konkrete Risiken, Maßnahmen und Nachweise werden in einer Matrix samt Ablaufdiagramm dargestellt.

„Problem Management“ und seine Erscheinungsformen werden sehr differenziert geschildert. Dabei wird auf die organisatorische Zuständigkeit eingegangen, der „Ablauf bei Problemen“ wird verbal und bildlich dargestellt. Einziges Risiko scheint das Auftreten von wiederkehrenden Störungen im Datenverarbeitung-Betrieb zu sein, deren

[3] § 7 Abs. 1 Geschäftsordnung des Amtes der Landesregierung.

Ursache nicht behoben wird (Symptombehandlung). Dokumentiert wird die Problembehebung im Projektinformationssystem jPISA / JIRA.

Die „Betriebsstörung Elisa“ enthält keine Risiken, Maßnahmen oder Nachweise. Die Abläufe werden in Form von Besprechungsprotokollen beschrieben, die Fragen und Ergebnisse enthalten.

Die Prozesse der mit der Änderung der Geschäftseinteilung im Oktober 2017 in die LI eingegliederten Dienststellen werden laut Auskunft der LI noch überarbeitet (z.B. die Telefonvermittlung, die Hausdruckerei und der Postversand).

Risikoerfassung

Die Erhebung der Risiken basiert auf den Erfahrungen der einzelnen Führungskräfte. Ihre Beschreibung fällt demnach – auch innerhalb derselben Gruppe, wie etwa in der Gruppe „Abläufe Leitung Landesinformatik“ – sehr unterschiedlich aus. So weisen die Prozesse „Produkteinstellung“, „Rechnungslegung-Eingangsrechnungen“ und „Software-Entwicklungsvorhaben“ eine Risikospalte mit bis zu sechs konkret beschriebenen Risikoszenarien auf. Demgegenüber geizen Prozesse, welche die strategischen Abläufe betreffen, mit der Darstellung konkreter Risiken; sie beschränken sich im Allgemeinen auf die Beschreibung von Gefährdungspotenzial.

Bei den drei genannten Beschaffungsvorgängen (Dienstleistung; Hardware und Büroartikel; Software) stellt das größte Risiko die Nichteinhaltung der Beschaffungsrichtlinie dar. Diese gibt den Rahmen für Beschaffungen bis zu einem Wert von 100.000 Euro vor.

Maßnahmen und Dokumentation

Als Maßnahme zur Risikovermeidung wird regelmäßig das Vier- oder Sechs-Augen-Prinzip angewendet. Auch das Prinzip der Funktionstrennung bei Beschaffungsvorgängen mit Rückkoppelung zum Führungsteam ist ein wesentliches IKS-Instrument. Weiters sollen EDV-unterstütze Kontrollmaßnahmen einen korrekten Prozessablauf gewährleisten. So übernimmt ein eigenes Programm die monatliche Kontrolle der Webservices; auch täglich erstellte Listen ermöglichen eine regelmäßige Kontrolle. Die durch Automatisation generierten Kontrolldokumente werden alle zwei Monate in Systemtechniker-Jour-fixes besprochen.

Grundsätzlich werden die Einhaltung der IKS-relevanten Vorgaben und die Funktionsfähigkeit des IKS nicht systematisch kontrolliert. Dasselbe gilt für Fehler und Mängel. Treten solche auf, sucht man regelmäßig nach pragmatischen Lösungen.

Zuständigkeiten

Die Zuständigkeiten im Rahmen der Prozesse sind zwar definiert, ihre genaue Darstellung findet sich jedoch an anderer Stelle, nämlich in der „Vertretungsregelung in der Landesinformatik".

Auffallend ist, dass in keinem der Prozesse der Landesamtsdirektor als Abteilungsleiter und als Vorstand des Inneren Dienstes als Verantwortlicher aufscheint. Insbesondere bei jenen Prozessen, die Strategie zum Thema haben oder IT-Ausrichtungen, die mehrere Abteilungen betreffen, erscheint dies ungewöhnlich, da die zentrale Steuerungskompetenz für den Inneren Dienst dem Landesamtsdirektor obliegt.

(2) Der Landesrechnungshof regt an, bei der Darstellung der in der LI laufenden Prozesse auch die zentrale Steuerungskompetenz des Landesamtsdirektors zu berücksichtigen. In Prozesse, welche die IT-Strategie betreffen, sollten neben dem Referat 0/01 - Büro des Landesamtsdirektors sowie der Fachgruppe 02 - Informatik und interne Dienste auch andere strategierelevante Dienststellen des Landes einbezogen werden.

Der Landesrechnungshof empfiehlt, für die LI eine aktuell gehaltene, einheitliche OrgRL für verbindlich zu erklären, um die regelmäßige, systematische Kontrolle des IKS zu erleichtern. Dabei ist darauf zu achten, dass Risiken konkret dargestellt werden. Damit kann das IKS auch laufend angepasst, qualitätsgesichert und im Voraus gesteuert werden.
Im Übrigen verweist der Landesrechnungshof darauf, dass es nach den anerkannten Regeln der Organisationslehre Aufgabe der Internen Revision ist, das IKS auf seine Funktionstüchtigkeit zu testen.

(3) Das Amt erklärt in seiner Gegenäußerung, dass es sich bei der „Betriebsstörung ELISA“ um keine Prozessbeschreibung, sondern um einen Teil des Problemmanagement-Prozesses handelt.

Das Amt teilt in seiner Gegenäußerung mit, dass die Steuerungskompetenz des Landesamtsdirektors in den IT-Prozessen im laufenden Projekt „Salzburg@2022“ verankert wird. Sobald die Ergebnisse für verbindlich erklärt werden, werden die Prozesse in der LI angepasst.

3. Planen von IT-Zielen

3.1 IT-Leitbild

(1) Ein IT-Leitbild enthält die Grundsätze, die die IT mittel- und langfristig verfolgen will. Es enthält Werte für Mitarbeitende im Umgang miteinander und im Verhältnis zu den Lieferanten sowie zu den Bürgern, welche die IT-Dienstleistungen des Landes in Anspruch nehmen.

Zum Zeitpunkt der Prüfung verfügt das Land Salzburg über kein derartiges IT-Leitbild. Allerdings enthält die OrgRL der LI Elemente eines IT-Leitbildes (Abschnitt IT-Strategie, Punkt 1 Werte der LI; 3 Positionierung der LI).

Für die Mitarbeitenden der LI stellt die OrgRL folgende Werte auf:

1. Individuen und Interaktionen sind wichtiger als Prozesse und Werkzeuge. Zwar sind wohldefinierte Entwicklungsprozesse und Entwicklungswerkzeuge wichtig, wesentlicher sind jedoch die Qualifikation der Mitarbeitenden und eine effiziente Kommunikation zwischen ihnen.
2. Funktionierende Programme sind wichtiger als ausführliche Dokumentation. Gut geschriebene und ausführliche Dokumentation kann zwar hilfreich sein, das eigentliche Ziel der Entwicklung ist jedoch die fertige Software.
3. Die stetige Abstimmung mit dem Kunden ist wichtiger als die ursprüngliche Leistungsbeschreibung in Verträgen. Statt sich an ursprünglich formulierten und mittlerweile veralteten Leistungsbeschreibungen in Verträgen festzuhalten, steht vielmehr die fortwährende konstruktive und vertrauensvolle Abstimmung mit dem Kunden im Mittelpunkt.
4. Der Mut und die Offenheit für Änderungen stehen über dem Befolgen eines festgelegten Plans. Im Verlauf eines Entwicklungsprojektes ändern sich viele Anforderungen und Randbedingungen ebenso wie das Verständnis des Problemfeldes. Das Team muss darauf schnell reagieren können.

In der Funktion als Dienstleister für die Dienststellen des Landes sieht die OrgRL der LI Folgendes vor:

1. Aktive Beratung und Unterstützung der Dienststellen beim optimierten und bedarfsgerechten Einsatz von Datenverarbeitung-Mitteln und Innovationen.
2. Aktive Unterstützung der Politik und Verwaltungs-Führungsspitze zur Gewährleistung der effizienten Umsetzung von Reformvorhaben.
3. Ausstattung und Betrieb mit der erforderlichen Hard- und Standardsoftware für die Arbeitsplätze.
4. Ausstattung und Betrieb mit der erforderlichen Hard- und Standardsoftware für die zentrale Infrastruktur.
5. Entwicklung und Betrieb von Individualsoftware zur Unterstützung von Aufgaben in der Landesverwaltung für die keine geeignete Standardsoftware am Markt verfügbar ist.

(2) Der Landesrechnungshof empfiehlt, die Werte für die Mitarbeitenden in der OrgRL allgemeiner und weniger aus Sicht der agilen Softwareentwicklung zu formulieren.

(3) Das Amt teilt in seiner Gegenäußerung mit, dass das IT-Leitbild aufgrund der Empfehlung des Landesrechnungshofs präzisiert wurde.

3.2 Planung von strategischen IT-Zielen

(1) Die Aufgaben einer strategischen IT-Planung basieren auf strategischen IT-Zielen. Die OrgRL der LI nimmt Bezug auf strategische Komponenten wie Werte, Ziele, Positionierung, Einbindung der Dienststellen und Standardisierung.

Zum Thema Steuerung führt die OrgRL der LI Folgendes aus:
„Die mittel- und langfristige Leistungsfähigkeit der Landesinformatik ist durch Steuerungsmaßnahmen und strategische Ausrichtungen zu gewährleisten. Dabei sind folgende Aspekte zu berücksichtigen:

- rechtzeitiges Erkennen von neuen technischen Möglichkeiten (einschließlich neuer Gefährdungspotentiale) und Initiierung angemessener Maßnahmen;
- rechtzeitiges Erkennen von sich ändernden Anforderungen/Erwartungen der Dienststellen des Landes und Initiierung angemessener Maßnahmen;
- rechtzeitiges Erkennen von landesinformatikinternem Verbesserungspotential und Initiierung angemessener Maßnahmen."
  (Strategieentwicklung Einführung, Punkt 8)

Die OrgRL der LI gliedert die angewendeten Steuerungsmaßnahmen nach dem monatlichen, vierteljährlichen und jährlichen Zeitpunkt ihres Einsatzes.

Die IT-Strategie der LI führt folgende Ziele an:

1. Schaffung von Innovationspotenzial
   Die LI forciert aktiv Innovationen und kreative Lösungen zur besseren Unterstützung ihrer Kunden unter Wahrung einer nach Möglichkeit kontinuierlichen Weiterentwicklung des Bestehenden.
2. Sicherheitsstreben
   Beim Betrieb der Anwendungen ist die Sicherheit (in der gesamten Landesverwaltung), Stabilität und Verlässlichkeit der Leistungserbringung für unsere Kunden zu gewährleisten.
3. Wirtschaftlichkeitsstreben
   Unseren Kunden werden zeitgerecht und in der wirtschaftlichsten Form die erforderlichen Anwendungen bereitgestellt, sofern gewährleistet werden kann, dass der Nutzen die Kosten (Erstellungs- und Betriebskosten) übersteigt.

Neben ihrer Aufbauorganisation listet die LI auch die bei ihr ablaufenden Hauptprozesse auf. Damit sollen alle Mitarbeitenden die wichtigsten Abläufe in der LI einsehen, nachvollziehen und auch entsprechend einhalten können.

Vorgesehen ist, dass Veränderungen in der Arbeitsweise unter Berücksichtigung der Auswirkungen auf die Prozesse abzustimmen sind. Veränderungen in den einzelnen Prozessen sollen in Abstimmung mit dem für den Prozess zuständigen Referatsleiter erfolgen. Dieser informiert bei Änderung den davon betroffenen Teilnehmerkreis. Für jeden Prozess ist dokumentiert, welche Gestaltungsüberlegungen aus Führungssicht dabei wichtig sind.

3.3 Maßstäbe für Ziele

(1) Aufbauend auf Formalzielen sind Zielmaßstäbe festzulegen, um Sollwerte für die Zielerreichung vorzugeben und Istwerte messen zu können. (Lutz J., Riedl, & Stelzer, 11. Auflage 2014)
Die OrgRL definiert zu verschiedenen Tatbeständen Ziele wie folgt:

Bei der Einführung neuer Systeme ist die Integration in die bestehende Systemlandschaft unter Vermeidung von Redundanzen vorrangiges Ziel, sodass die Informationen

möglichst frei von Redundanzen gespeichert werden. Weiters sollen die Arbeitsabläufe möglichst durchgängig in elektronischer Form, ohne Medienbrüche abgewickelt werden. Die Bearbeitung und Verwaltung der unterschiedlichen Informationstypen (z.B. GIS-Formate, CAD) erfolgt in einheitlicher Form mit den vorgegebenen, standardisierten Werkzeugen.

Die unterschiedlichen Informationstypen (z.B. GIS-Formate, CAD) werden in einheitlicher Form mit den vorgegebenen, standardisierten Werkzeugen bearbeitet und verwaltet.

Die LI entwickelt und betreibt Individualsoftware zur Unterstützung von Aufgaben in der Landesverwaltung, für die keine geeignete Standardsoftware am Markt verfügbar ist. Sie stattet die Infrastruktur mit der erforderlichen Hard- und Standardsoftware für die zentrale Infrastruktur aus und betreibt sie.

Die OrgRL der LI nennt folgende drei Zielmaßstäbe für Sicherheit (BSI - Bundesamt für Sicherheit in der Informationstechnik, 2018):

1. Vertraulichkeit
   Vertraulichkeit ist der Schutz vor unbefugter Preisgabe von Informationen. Vertrauliche Daten und Informationen dürfen ausschließlich Befugten in der zulässigen Weise zugänglich sein.
2. Integrität
   Integrität bezeichnet die Sicherstellung der Korrektheit (Unversehrtheit) von Daten und der korrekten Funktionsweise von Systemen. Wenn der Begriff Integrität auf "Daten" angewendet wird, drückt er aus, dass die Daten vollständig und unverändert sind. In der Informationstechnik wird er in der Regel aber weiter gefasst und auf "Informationen" angewendet. Der Begriff "Information" wird dabei für "Daten" verwendet, denen je nach Zusammenhang bestimmte Attribute wie etwa Autor oder Zeitpunkt der Erstellung zugeordnet werden können. Der Verlust der Integrität von Informationen kann daher bedeuten, dass diese unerlaubt verändert, Angaben zum Autor verfälscht oder Zeitangaben zur Erstellung manipuliert wurden.
3. Verfügbarkeit
   Die Verfügbarkeit von Dienstleistungen, Funktionen eines IT-Systems, IT-Anwendungen oder IT-Netzen oder auch von Informationen ist vorhanden, wenn diese von den Anwendern stets wie vorgesehen genutzt werden können.

Bei der dualen Zustellung - der elektronischen und physischen Zustellung von Poststücken - spielt auch der Maßstab „Verbindlichkeit“ eine Rolle: Unter diesem Begriff werden die Sicherheitsziele Authentizität und Nichtabstreitbarkeit zusammengefasst.

Werden Informationen übertragen, bedeutet dies, dass die Informationsquelle ihre Identität bewiesen hat und der Empfang der Nachricht nicht in Abrede gestellt werden kann.

Die OrgRL definiert auch die Zuständigkeit der LI für den IT-Betrieb (Abschnitt 03 IT-Betrieb für Organisationeinheiten). Die in der OrgRL genannten Zuständigkeiten haben Zielcharakter; die geplante Art der Ausstattung hat eher Maßnahmencharakter. Bei der Ausstattung wird zwischen den Betriebsstandards „Vollausstattung“ und „minimale Grundausstattung“ unterschieden.

4. IT-Strategie des Landes

(1) Eine IT-Strategie ist aufbauend auf der strategischen IT-Zielplanung zu entwickeln. Sie soll eine IT-Maßnahmenplanung ermöglichen. Die wesentlichen Merkmale von IT-Strategien sind Strategieobjekte. Solche Objekte sind die Komponenten der Informationsinfrastruktur und wesentliche Eigenschaften der Infrastruktur. (Lutz J., Riedl, & Stelzer, 11. Auflage 2014, S. 147 ff.)

Bei der Entwicklung einer nutzenmaximalen IT-Strategie bietet sich die Nutzwertanalyse auf Basis von festgelegten Formalzielen und Kriterien an. Als festgelegte Formalziele eignen sich vor allem Wirksamkeit und Wirtschaftlichkeit. So sind etwa die Kosten der Systementwicklung bei Eigenentwicklung oder jene des Fremdbezugs von Software oder Software-as-a-Service ein mögliches Attribut. (Lutz J., Riedl, & Stelzer, 11. Auflage 2014, S. 147 ff.)

4.1 Informationsstrategie 2012

(1) Die „Informatikstrategie 2012“ wurde zwischen dem damaligen Referat 0/02 - Zentrale Aufgaben und Strategien und der damaligen Fachgruppe 02 - Landesinformatik erarbeitet. Sie trat im Mai 2008 in Kraft.[4] Mit ihr sollte die Basis für das im Arbeitsübereinkommen der Landesregierung festgelegte Ziel geschaffen werden, die Landesverwaltung als innovatives, sparsames und effizientes Dienstleistungsunternehmen weiterzuentwickeln.[5]

Die Kernelemente der „Informatikstrategie 2012“ lauten:

- IT-Architektur in Richtung service-orientierter IT-Architektur
- Entwicklung von flexiblen, robusten, sicheren und wieder verwendbaren IT-Komponenten
- Organisationsübergreifende Integration und Vernetzung von IT-Systemen
- Rahmenbedingungen und Maßnahmen zur Ausrichtung der Systemlandschaft
- Basis für eine aus gesamtwirtschaftlicher Sicht ausgewogene IT-Infrastruktur
- Forcierung der Entwicklung zu einer modernen Systemlandschaft in Richtung mehr Herstellerunabhängigkeit und stärkerer Orientierung an Standards
- Weitere Forcierung von bereits begonnener Ausrichtung auf Open Source Alternativen (z.B. LINUX)

[4] Schreiben des Landesamtsdirektors vom 6. Mai 2008, Zl. 20002-IKT/4/8-2008.
[5] Arbeitsübereinkommen der Landesregierung für 2009 bis 2014, Abschnitt 14, Moderne Verwaltung, Seite 74.

Die „Informatikstrategie 2012“ geht davon aus, dass die Leistungsfähigkeit der Verwaltung vom bedarfsgerechten Einsatz der Informationstechnologie abhängt. Der Datenschutz und die Datensicherheit werden als sehr wichtig bewertet. In Zeiten knapper werdender Budgets und steigender Ansprüche sind die IT-Leistungen unter Wahrung der Grundsätze der Wirtschaftlichkeit, Zweckmäßigkeit und Sparsamkeit zu erbringen oder zu nutzen. Sach- und Personal-ressourcen sollen in allen Dienststellen bereitstehen, damit der Ausbau der IT-Unterstützung weiter erfolgen kann.

Die „Informatikstrategie 2012“ sieht vor, die IT-Strategie rollierend alle zwei bis drei Jahre weiterzuentwickeln. Als Grund dafür wird die hohe Dynamik der Entwicklungen in der Informations- und Kommunikationstechnologie genannt. Die „Informatikstrategie 2012“ sieht für den Einsatz der Hardware vor (z.B. Arbeitsplatzrechner, Serversysteme, Netzwerkkomponenten, Telefonie), dass wirtschaftliche und LINUX-taugliche Komponenten einzusetzen sind. Die Einsatzdauer für die Hardwareausstattung (z.B. PC, Notebook, Drucker) wird mit mindestens vier Jahren festgelegt.

Wesentliches Kernelement der „Informatikstrategie 2012“ ist die Ausrichtung der IT-Architektur in Richtung service-orientierter IT-Architektur, die es ermöglicht, die gestiegene Systemkomplexität zu bewältigen und flexible, robuste, sichere und wieder verwendbare IT-Komponenten zu entwickeln.

Ziel ist es, eine ganzheitliche IT-Architektur zu schaffen, welche die Kommunikation zwischen unterschiedlichen Applikationen unterstützt, auf einer Integration der IT-Lösungen aufbaut, mit der Verfahren einfacher abgewickelt werden können. Damit leistet die IT einen wesentlichen Beitrag zur Ablauf- und Prozessunterstützung sowie insgesamt zur Verwaltungsmodernisierung.

Die Zusammenarbeit und der Erfahrungsaustausch mit anderen Gebietskörperschaften wird von der „Informatikstrategie 2012“ weiter forciert; kooperiert wird vor allem mit anderen Bundesländern, da diese vergleichbaren Aufgaben zu bewältigen haben. Die LI stellt anderen Gebietskörperschaften gegen Kostenersatz Datenverarbeitung-Lösungen zur Verfügung (z.B. Application Service Providing-Lösungen) oder nutzt solche anderer Gebietskörperschaften. Durch die Mitarbeit in bundesweiten und länderübergreifenden Arbeitsgruppen werden die Anforderungen an übergreifende oder bundesweite Vorhaben eingebracht und abgestimmt.

Die „Informatikstrategie 2012“ sieht auch vor, dass Integration organisationsübergreifende Verbindung von IT-Systemen ermöglicht. Im Kontext der Digitalisierung schafft die Integration Möglichkeiten zum Einsatz von e-Government & Open (Government) Data.

In den Jahren 2014 bis Mai 2017 fanden etwa vierteljährlich Besprechungen zwischen dem damaligen Referat 0/02 - Zentrale Aufgaben und Strategien und der damaligen Fachgruppe 02 - Landesinformatik statt. Die „Informatikstrategie 2012“ wurde dabei jedoch nicht weiterentwickelt.

In mehreren schriftlichen Unterlagen der LI finden sich Überlegungen und Diskussionsergebnisse der LI zu strategischen Themen. Auch wenn die Unterlagen unterschiedlich datiert sind, sind sie nach Auskunft der LI aktuell und relevant. Über die „Informatikstrategie 2012“ hinausgehende strategische Festlegungen wurden mit der Landesamtsdirektion nicht formal abgestimmt.

4.2 Stand der IT-Strategie zum Zeitpunkt der Prüfung

(1) Zwischen dem damaligen Referat 0/02 - Zentrale Aufgaben und Strategien und der damaligen Fachgruppe 02 - Landesinformatik fanden etwa vierteljährlich Besprechungen statt. Der Landesrechnungshof ließ sich die Protokolle dieser Gespräche aus den Jahren 2014 bis 2017 vorlegen. Dabei zeigte sich, dass sich diese Gespräche mehr auf geplante oder in Umsetzung befindliche Projekte der LI bezogen, als auf die Weiterentwicklung der IT-Strategie des Landes. Die aus dem Jahr 2008 stammende „Informatikstrategie 2012“ wurde offiziell nicht wie vorgesehen, rollierend alle zwei bis drei Jahre weiterentwickelt. Die LI hat ihre OrgRL laufend aktualisiert, ohne dies jedoch mit der Landesamtsdirektion offiziell abzustimmen.

Zum Zeitpunkt der Prüfung setzt sich die IT-Strategie der LI aus folgenden Teilstrategien zusammen:

- Sicherheitsrichtlinie
- IT-Architektur-Standards
- Große Anwendungserneuerungen (z.B. Erneuerung Personalwesen)
- Hardware-Strategie
- Software-Strategie

Unter der Voraussetzung der Freigabe eines Projektes durch den Landesamtsdirektor und der Einhaltung der budgetären und personellen Rahmenbedingungen gelten für die LI folgende allgemeine Ziele:

- Unseren Kunden werden zeitgerecht und in der wirtschaftlichsten Form die erforderlichen Anwendungen bereitgestellt, sofern gewährleistet werden kann, dass der Nutzen die Kosten (Erstellungs- und Betriebskosten) übersteigt.
- Beim Betrieb der Anwendungen ist die Sicherheit (in der gesamten Landesverwaltung), Stabilität und Verlässlichkeit der Leistungserbringung für unsere Kunden zu gewährleisten.
- Die Landesinformatik forciert aktiv Innovationen und kreative Lösungen zur besseren Unterstützung unserer Kunden unter Wahrung einer nach Möglichkeit kontinuierlichen Weiterentwicklung des Bestehenden.

Der Landesrechnungshof untersuchte die von der LI zur Verfügung gestellten schriftlichen Unterlagen nach Strategieinhalten und wählte dabei folgende Themen aus:

4.3 Beschaffung, Entwicklung und Verwendung von Software

(1) Zum Einsatz von Standardsoftware gilt für die LI folgendes:
Wenn es für eine Aufgabe im Land geeignete Standardsoftwareprodukte am Markt gibt, sind diese einer Individual- oder Fremdentwicklung vorzuziehen. Dazu ist es auch erforderlich, dass sich die Organisation im Land an die Funktionen des Standardsoftwareproduktes anpasst. Dies ist vor allem bei Standardprodukten erforderlich, die sehr komplex und umfangreich sind (z.B. SAP, Office); qualitativ vergleichbare Produkte können in diesen Bereichen mit dem im Land verfügbaren Personal nicht entwickelt werden.

Der Open-Source-Einsatz wird vor allem bei Arbeitsplatzlösungen und aufgrund der Gesamtkosten bei breit eingesetzten Arbeitsplatzlösungen vorrangig angestrebt.

In den Fällen, in denen das Land Salzburg öffentlicher Auftraggeber für IT-Leistungen ist und dem Bundesvergabegesetz unterliegt, bedient sich die LI der Beratung durch eine Anwaltskanzlei.

Für das Abwickeln der Hauptprozesse der LI gelten folgende Ziele:

- Für alle Mitarbeiter sind die wichtigsten Abläufe in der Landesinformatik einsehbar und nachvollziehbar, damit sie auch entsprechend eingehalten werden können.

- Veränderungen in der Arbeitsweise sind unter Berücksichtigung der Auswirkungen auf die Prozesse abzustimmen.
- Veränderungen in den einzelnen Prozessen erfolgen in Abstimmung mit dem für den Prozess zuständigen Referatsleiter. Dieser informiert bei Änderung den davon betroffenen Teilnehmerkreis.
- Für jeden Prozess ist dokumentiert, welche Gestaltungsüberlegungen aus Führungssicht dabei wichtig sind.

Darüber hinaus enthält ein Dokument der LI die für die Durchführung von Projekten erforderlichen Beschreibungen und Vorgehensweisen.

4.4 Art und Umfang der Benutzerbeteiligung

(1) Um die IT-Sicherheitsziele und -strategien des Landes zu überprüfen und zu aktualisieren, veranstaltet die LI vierteljährlich Jour-fixes und jährlich Strategie-Workshops. Mit den IT-Anwendern hält die LI Kontakt, indem sie jährlich eine Veranstaltung für alle von ihr betreuten Dienststellen organisiert. Auch die Beziehung zu den Lieferanten wird hauptsächlich durch die LI gepflegt.

In den letzten Jahren hat sich die LI in jährlichen Workshops mit den IT-Strategiebereichen Technologie, Personal und Sicherheit befasst. Abhängig von den verfügbaren Ressourcen wurden daraus Themenschwerpunkte erarbeitet und Umsetzungsschritte festgelegt. Nach Auskunft der LI ist geplant, die strategische Ausrichtung der LI im Herbst 2018 im Rahmen einer Abteilungsleiterkonferenz des Landesamtsdirektors zu diskutieren und abzustimmen.

4.5 Budgetierung und Finanzplanung

(1) Die LI steuert die Wirtschaftlichkeit ihrer Dienstleistungen über die interne Kostenrechnung. Sie legt vierteljährlich Rechnungen an die von ihr betreuten betriebsähnlichen Einrichtungen der Landesverwaltung und die Einrichtungen außerhalb der Landesverwaltung; alle anderen Kunden erhalten sogenannte Leistungsausweise, die Auskunft über Menge und Kosten der von der LI bezogenen Produkte und Dienstleistungen geben. Die Darstellung des Prozesses „Datenverarbeitung-Budget“ enthält auch ein Diagramm über dessen Jahreszyklus.

Die Kostenrechnung ist ein Instrument der Budgetplanung: Mit ihr können alle Kunden, denen Leistungen verrechnet werden, die im Folgejahr von der LI erwarteten Leistungen mit der LI abstimmen.

4.6 Umweltbewusstsein und Nachhaltigkeit

(1) Seit der stärkeren Forcierung im Zuge des „Trends Green IT" ist dieses Thema State-of-the-Art (z.B. Steigerung der Energieeffizienz der Hardware). Die LI stimmt sich bei umweltrelevanten Themen mit der Abteilung 5 - Natur- und Umweltschutz, Gewerbe ab. Im Oktober 2017 sind die Hausdruckerei und die Büromaterialbestellungen neu zur LI hinzugekommenen; hier wird dieses Thema gerade bearbeitet. So steht die Zertifizierung der Hausdruckerei für das Umweltgütesiegel kurz bevor. Bei Materialbestellungen wird das Thema Nachhaltigkeit berücksichtigt.

4.7 Vorstoß zu einer neuen IT-Strategie

(1) Seit der Änderung der Geschäftseinteilung im Oktober 2017 fanden Gespräche zwischen dem Landesamtsdirektor und dem Leiter der LI statt, die nach Auskunft des Leiters der LI auch die IT-Strategie des Landes betreffen. Über diese Gespräche wurden keine offiziellen Protokolle verfasst. Der Leiter der LI verfolgte die Ergebnisse dieser Gespräche auf Basis eigener Aufzeichnungen weiter.

Offizieller Vorstoß, die IT-Strategie des Landes weiterzuentwickeln, war der Start des Konzeptionsprojektes „Digitalisierungs- & Innovationsstrategie@2022" im Februar 2018. Das Projekt beschäftigt sich mit der Konzeption eines Strategie-Prozesses im Land Salzburg. Die LI ist dabei Pilotdienststelle. Im Zuge des Projektes werden bereichsübergreifend durchgängige Digitalisierungsprojekte in der Verwaltung forciert. Dabei sollen folgende Standards verstärkt eingesetzt werden:

- Konsequente Umsetzung der Einsatzstandards für digitale Büroarbeit als eine wesentliche Basis für die Umsetzung einer durchgängig elektronischen Arbeitsweise.
- Umstellung des automatisierten Schriftverkehrs auf duale Zustellung.
- Aufbau und durchgängige Nutzung des Elektronischen Rechtsverkehrs (=ERV) zur digitalen Kommunikation mit der Justiz.
- Die Integrationsfähigkeit von Anwendungen unter Nutzung bereits vorhandener Funktionalität hat Vorrang vor „isolierten" Systemen. So soll die bestehende digitale Infrastruktur (z.B. ELAK, Zentrales Archiv Opentext, Kofax-Scan, zentrale Register wie z.B. Adressdaten) verpflichtend eingesetzt werden.

- Durchgängige Nutzung der Stammzahlenregister (z.B. Zentrales Melderegister, Firmenbuch, Vereinsregister) zur eindeutigen Identifikation natürlicher und juristischer Personen in Verwaltungsverfahren.
- Bei allen Themen im ERP-Bereich hat die Implementierung auf Basis von SAP-Modulen Vorrang vor Individuallösungen. Abweichungen davon müssen entsprechend begründet und vom Herrn Landesamtsdirektor freigegeben werden.
- Die ganzheitliche Nutzung von Portallösungen ist landesweit zu forcieren, um allen "Kunden/Partnern des Landes" eine einheitliche, zeitgemäße Dienstleistung zu bieten:
  - Bürger (E-Government)
  - Unternehmen (Unternehmens Service Portal=USP)
  - Behörden (Portalverbund, Gemeinde-Portal Salzburg)
  - Businesspartner (=Partner-Portale z.B. für Wohnbauförderung, Soziales)
  - Nutzung etablierter, marktgängiger Cloud-Lösungen für Fachanwendungen mit geringem Integrationsbedarf unter Berücksichtigung der rechtlichen Rahmenbedingungen.

Das Projekt soll Ende des Jahres 2018 abgeschlossen werden; seine Ergebnisse sollen anschließend umgesetzt werden.

Der im Frühjahr 2018 von der Landesregierung geschlossene Koalitionsvertrag 2018 geht davon aus, dass die Digitalisierung nicht nur Wirtschaft und Gesellschaft verändert, sondern auch das Verwaltungshandeln. „Voraussetzung, um moderne und bürgernahe Verwaltung leben zu können, sind klare Rahmenbedingungen und politische Entscheidungen. Um dieses Ziel zu erreichen, haben wir ein Bündel an innovativen Maßnahmen im Reformprogramm „LandSalzburg@2022“ zusammengefasst. Wir streben konsequent und zielorientiert dessen Umsetzung in den kommenden Jahren an. Unsere ambitionierte Vision ist es, eine der modernsten und effizientesten Verwaltungen Europas zu werden.“[6]

[6] Koalitionsvertrag 2018, Stand 28. Mai 2018, Seiten 88 ff.

(2) Der Landesrechnungshof stellt fest, dass die aus dem Jahr 2008 stammende „Informatikstrategie 2012“ nicht wie vorgesehen, rollierend alle zwei bis drei Jahre weiterentwickelt wurde, sondern bis zum Zeitpunkt der Prüfung offiziell unverändert blieb. Die aktuellen strategischen Ziele der LI stammen aus ihrer OrgRL. Diese hat die LI laufend aktualisiert, ohne dies jedoch mit der Landesamtsdirektion offiziell abzustimmen.

Anlässlich einer anderen Prüfung des Landesrechnungshofs verwies der Landesamtsdirektor auf die geplante Wissensbündelung in Vergabeangelegenheiten an zentraler Stelle des Amtes.[7] Um den Aufwand für externe Beratungen bei der Vergabe von IT-Leistungen zu vermindern, empfiehlt der Landesrechnungshof, auch diese Vergaben über diese zentrale Stelle abzuwickeln.
(Verbesserungsvorschlag gemäß § 10 (11) Salzburger Landesrechnungshofgesetz 1993)

Der Landesrechnungshof fordert,

- eine IT-Strategie des Landes zu entwickeln und diese in einem verbindlichen, mit dem Landesamtsdirektor abgestimmten Dokument zusammenzufassen;
- die Aktualität der neuen IT-Strategie regelmäßig zu evaluieren und sie rollierend alle zwei bis drei Jahre weiterzuentwickeln;
- die Ergebnisse von Besprechungen, welche die IT-Strategie des Landes und die Aufgaben der LI berühren, in offiziellen Protokollen zu dokumentieren.

(3) Das Amt erklärt in seiner Gegenäußerung, dass die LI die IT-Strategie laufend angepasst und mit dem Landesamtsdirektor abgestimmt habe. Im Anschluss an die Entwicklung einer Digitalisierungs- und Innovationsstrategie soll die IT-Strategie evaluiert und den übergeordneten strategischen Vorgaben entsprechend neu ausgerichtet werden; dabei werden die Forderungen des LRH berücksichtigt.

[7] Bericht des Landesrechnungshofs „Aufsicht über Tourismusverbände“, Februar 2018, 7. Anhang, Gegenäußerung des Amtes der Salzburger Landesregierung, Seiten 2 ff.

5. Planen strategischer Maßnahmen

5.1 Zweck der Planung der Maßnahmen

(1) Um die strategischen IT-Ziele und das strategische Projektportfolio im Rahmen der IT-Strategie zu erreichen, müssen Maßnahmen entwickelt werden. Das Budget muss auf das Ergebnis der Maßnahmenplanung abgestimmt werden.

Betreffen Maßnahmen der LI die zentrale Steuerungskompetenz des Landesamtsdirektors, müssen diese mit ihm abgestimmt und von ihm freigegeben werden. Seine Entscheidungen berücksichtigen die Erkenntnisse aus Abstimmungsbesprechungen mit den Ressorts, den Bezirkshauptleuten und Abteilungsleitern sowie den Führungskräften der Landesamtsdirektion.

Es ist Aufgabe der Dienststellen, den Nutzen von IT-Vorhaben darzustellen und umzusetzen. Die infrastrukturellen Vorhaben der LI werden abgewickelt, weil der Markt technische Änderungen erfordert; sie dienen vor allem der Verminderung des Risikos. Technologische Innovationen werden nach Nutzenüberlegungen priorisiert - etwa nach der Breite der Einsetzbarkeit oder dem Grad der Effizienzsteigerung. Die LI führt keine Nutzwertanalysen durch.

Eine Stelle, die dezentrale Organisationsprojekte und Applikationen steuert, besteht im Amt der Salzburger Landesregierung derzeit nicht. Dies gilt auch für die damit verbundenen Kosten- Nutzenanalysen sowie die Evaluierung solcher Projekte und Applikationen.

(2) Der Landesrechnungshof empfiehlt, im Amt der Salzburger Landesregierung eine Stelle einzurichten, die dezentrale Organisationsprojekte und Applikationen steuert. Das soll sicherstellen, dass nur solche Vorhaben umgesetzt werden, die bestimmte organisatorische Anforderungen erfüllen und deren Kosten ausreichender Nutzen gegenübersteht; nach ihrer Umsetzung sollten sie auch evaluiert werden.

(3) Das Amt erklärt in seiner Gegenäußerung, dass dezentrale Organisationsprojekte grundsätzlich in der Verantwortung der einzelnen Dienststellen liegen. Einfache und kleine Vorhaben könnten schon aus Gründen des Verwaltungsaufwandes nicht einem zentralen Controlling zugeführt werden. Besonders komplexe Organisationsprojekte dezentraler Dienststellen und Projekte, die Dienststellen übergreifen, werden seit

Mitte des Jahres 2018 von einer zentralen Stelle im Büro des Landesamtdirektors gesteuert.
Noch im Jahr 2018 sollen in der Landesverwaltung neue Projektmanagementstandards eingeführt werden. Diese sollen etwa den Inhalt von Projektaufträgen und Abschlussberichten regeln (Ziel-, Ressourcen-, Kosten- und Nutzenplanung, Zielerreichung).

5.2 Ergebnis der Planung der Maßnahmen

(1) Bei der strategischen Maßnahmenplanung werden Maßnahmen zur Erreichung der strategischen IT-Ziele oder des strategischen Projektportfolios im Rahmen der IT-Strategie entwickelt. Ergebnis ist der strategische IT-Plan, der in Teilpläne geteilt ist und auf Objekte oder Eigenschaften der IT Bezug nimmt. Der Landesamtsdirektor steuert diesen Prozess durch Aufträge an die LI. Diese plant alle Aufträge und Vorhaben im zentralen Projekt-Informationssystem. (Lutz J., Riedl, & Stelzer, 11. Auflage 2014, S. 159)

Maßnahmenpläne im Sinn der einschlägigen Literatur sind der Technologieeinsatzplan und der Informationssystemplan. Das Land Salzburg verfügt über solche Pläne, sie werden jedoch nicht unter diesen Bezeichnungen geführt. Zu finden sind die Maßnahmenpläne in folgenden Dokumenten:

- IT-Architektur-Standards,
- Planungen für strategische Vorhaben,
- IT-Kennzahlen,
- IT-Strategie,
- Produktfestlegungen in der zentralen IT-Bestandsverwaltung,
- Festlegungen/Planungen zu IT-Schlüsselthemen,
- Prozessdefinitionen / OrgRL,
- übergeordnete Vertretungsregelungen,
- Zuständigkeitszuordnungen der Technikerrollen für alle betreuten Produkte im zentralen,
- IT-Bestandsverwaltung,
- Zeitaufzeichnungen von Mitarbeitenden,
- Zentrales Stammdatenmanagement und Auswertestandards.

Für das Personalinformationssystem und das Soziale Informationssystem liegen in der LI Maßnahmenpläne vor, die die Anforderungen einer strategischen Maßnahmenplanung erfüllen.

Die LI legt fest, welche ihrer Mitarbeitenden für unternehmensweite Schlüsselthemen zuständig sind; dieser Plan enthält auch Regelungen für die Vertretung. So werden für 34 Schlüsselthemen subsidiäre Zuständigkeiten und Maßnahmen zur Gewährleistung der Vertretung festgelegt. Die LI verfügt auch über einen Plan für Ausbildungsmaßnahmen für neu in die LI eintretende Mitarbeitende.

Die LI bewertet ihre Tätigkeit mittels Kennzahlen. Diese sind sowohl allgemein als auch IT-spezifisch formuliert. Die allgemeinen Kennzahlen beziehen sich etwa auf Budget und Kosten sowie die Zahl der Mitarbeitenden. Die IT-spezifischen Kennzahlen behandeln etwa die IT-Sicherheit, die Abwicklung von Projekten sowie interne Dienstleistungen. Die Kennzahlen werden jährlich mit dem Landesamtsdirektor abgestimmt.

Nach Auskunft der LI hat deren Leiter mit dem Landesamtsdirektor vereinbart, dass die derzeit sehr guten Kennzahlen weiterhin erreicht werden sollen. Dazu werden dem Landesamtsdirektor vierteljährlich die aktuellen Kennzahlen übermittelt. Diese stellen für die LI „Sensoren“ für den IT-Betrieb dar, anhand derer sie die IT steuern. Laut LI bedeutet eine Schwankungsbreite von 20 Prozent bei den das Projektmanagement betreffenden Zahlen erfahrungsgemäß einen sehr guten Wert. Die Risikoeinstufung ist in den Erläuterungen der Kennzahlen angeführt. Die Kosten versucht die LI über die Kostenkennlinien zu reduzieren. Nach Angaben der LI setzt sie explizite Steuerungsmaßnahmen, wenn sich die Werte bei der Kostenrechnung verschlechtern oder wenn anlassbezogene Vergleiche mit externen Betriebsangeboten schlechtere Werte ergeben. Zur Verfügbarkeit strebt die LI Kennzahlen über 99 Prozent an. Bei den Bearbeitungszeiten des Kundendienstes und der Ticketbearbeitung überprüft die LI laufend, ob die Kennlinie eingehalten wird.

6. Management der Informationssicherheit (IS)

(1) Die IT-Sicherheitsrichtlinie ist Teil der Security Policy des Landes Salzburg. Die LI verfügt über eine verbindliche Leitlinie für die Informationssicherheit der Landesverwaltung. Diese IT-Sicherheitsrichtlinie sieht vor, dass der Landesamtsdirektor die LI (vormals Fachgruppe 0/2) mit der Erstellung der Security Policy und deren Umsetzung beauftragt. Die Leitung der LI ist in Abstimmung mit dem Landesamtsdirektor verantwortlich für alle Fragen der IT-Sicherheit. Dazu gehört, die Einhaltung der Security Policy laufend zu prüfen und das Risikopotenzial einzelner Teilbereiche neu einzuschätzen; weiters muss die Security Policy auf Vollständigkeit und Aktualität überprüft werden und müssen allenfalls Änderungen beauftragt werden. Die LI ist dafür zuständig, die Security Policy am aktuellen Stand der Technik auszurichten. Die IT Sicherheitsexperten der LI sind intern zentrale Ansprechpartner für sicherheitsrelevante Fragen; sie beraten die Leitung LI und führen Risikobewertungen durch.

Das Informationssicherheitsmanagement der LI ist als kontinuierlicher Prozess mit folgenden Aufgaben konzipiert:

- Festlegung der Sicherheitsziele und Sicherheitsstrategien
- Ermittlung und Bewertung der Informationssicherheitsrisiken
- Festlegung geeigneter Sicherheitsmaßnahmen
- Überwachung der Implementierung und des laufenden Betriebes der ausgewählten Sicherheitsmaßnahmen
- Förderung des Sicherheitsbewusstseins (IT Security Awareness)
- Entdeckung von und Reaktion auf sicherheitsrelevante Ereignisse (IT Security Krisenmanagement und „Incident Handling“)

Bei der Sicherheitsanalyse orientiert sich die IT-Sicherheitsrichtlinie am „Österreichischen Informationssicherheitshandbuch" sowie an internationalen Normen (z.B. ISO/IEC 27001 und 27002). Die LI wendet den kombinierten Risikoanalyse-Ansatz an. Dieser ermöglicht es, mittels Grundschutzanalysen rasch kostengünstige IT-Sicherheitsmaßnahmen auszuwählen; hohe Sicherheitsrisiken können über detaillierte Risikoanalysen wirksam vermindert werden.

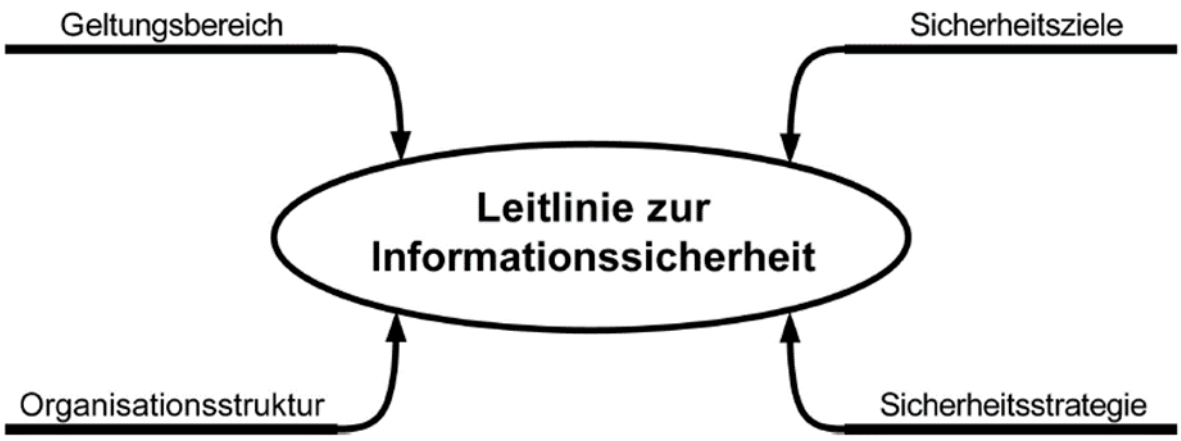

Abbildung 1: BSI IT-Grundschutz

Die IT-Sicherheitsrichtlinie regelt den Stellenwert der Informationssicherheit, ihren Geltungsbereich, die Verantwortung der Leitung, die Sicherheitsstrategie sowie die Struktur, wie die Informationssicherheit organisiert wird. Die Richtlinie zielt darauf ab, Vertraulichkeit, Integrität und Verfügbarkeit sicherzustellen. Zu diesem Zweck sieht sie etwa abgestufte Klassifizierungen für Daten und unterschiedliche Berechtigungen der Anwender vor. Außerdem legt die Richtlinie Sicherheitsziele fest.

Die IT-Sicherheitsrichtlinie definiert auch, welche organisatorischen Eigenschaften das Risikomanagement aufzuweisen hat. Sie bestimmt auch, welche Technologien zur Datensammlung zu verwenden sind. Bei fehlenden internen Ressourcen sieht die Richtlinie die Möglichkeit vor, Risikomanagement auch auszulagern.

Sowohl die IT-Sicherheitsrichtlinie, als auch die tatsächliche Sicherheit der LI wurde und wird laufend auch externen Prüfungen unterzogen. Mitarbeitende werden in IT-Sicherheit in der Landesverwaltung und in Veranstaltungen der SVAK geschult. Die „Sicherheitsbestimmungen für Anwenderinnen und Anwender“ sind für jeden Mitarbeitenden im Intranet verfügbar.

In den Fällen, in denen die LI am Portalverbund der öffentlichen Verwaltung teilnimmt, erfüllt sie auch dessen übergreifende IT-Sicherheitsrichtlinien.

Informationssysteme und Netzwerke sind generell Sicherheitsbedrohungen unterschiedlichster Art von Innen und Außen ausgesetzt. Täglich gehen eine Vielzahl mit Schadsoftware behaftete E-Mails ein. Zudem zielen Spionageangriffe von professionellen Angrei-

fern auf Unternehmen und öffentliche Verwaltungen ab. Um den Schutzbedarf herzustellen sind notwendige technische und organisatorische Maßnahmen zwingend erforderlich.

Die LI überprüft und aktualisiert ihre Sicherheitsziele und -strategien regelmäßig. Weitere Maßnahmen zur Verbesserung der Sicherheit sind konkret geplant. Auch die Leitlinie zur Informationssicherheit wird jährlich auf ihre Aktualität hin überprüft und gegebenenfalls angepasst.

Die LI sieht folgende Schutzbedarfskategorien vor:

1. Normal: Die Schadensauswirkungen sind begrenzt und überschaubar. Maßnahmen des IT-Grundschutzes gemäß dem Österreichischen Informationssicherheitshandbuch reichen im Allgemeinen aus.
2. Hoch: Die Schadensauswirkungen können beträchtlich sein. Wahlweise können weitere verstärkte Grundschutzmaßnahmen eingesetzt oder eine detaillierte Risikoanalyse durchgeführt werden.
3. Sehr hoch: Die Schadensauswirkungen können ein existentiell bedrohliches Ausmaß erreichen. IT-Grundschutzmaßnahmen alleine reichen nicht aus, die erforderlichen Sicherheitsmaßnahmen sollten individuell auf Basis einer Risikoanalyse ermittelt werden.

Die Schutzbedarfsfeststellung bildet die Grundlage für eine Entscheidung über die weitere Vorgehensweise und ist daher mit entsprechender Sorgfalt durchzuführen. Sie erfolgt in drei Schritten:
Schritt 1: Erfassung aller vorhandenen oder geplanten IT-Systeme
Schritt 2: Erfassung der IT-Anwendungen und Zuordnung zu den einzelnen IT-Systemen
Schritt 3: Schutzbedarfsfeststellung für jedes IT-System

Neue und bestehende Anwendungen sind diesen Schutzbedarfskategorien zuzuordnen. Zur Unterstützung und Dokumentation der Schutzbedarfsanalyse wird ein Fragebogen eingesetzt. Für alle IT-Systeme der Schutzbedarfskategorie „normal“ ist eine Grundschutzanalyse durchzuführen.

Alle IT-Systeme der Schutzbedarfskategorie „hoch bis sehr hoch“ sind einer detaillierten Risikoanalyse zu unterziehen.

Die Sicherheitsmaßnahmen der Security Policy sind so definiert, dass für IT-Systeme mit Schutzbedarf „normal“ ein einheitlicher, möglichst hoher Sicherheitsstandard auch ohne eine eigene detaillierte Risikoanalyse zur Verfügung gestellt wird.

Über den Grundschutz hinausgehende Sicherheitsmaßnahmen für IT-Systeme mit hohem oder sehr hohem Schutzbedarf werden eigens dargestellt.

Bei der Einführung neuer IT-Systeme ist der Auftraggeber verantwortlich für die Festlegung, von wem und von wo aus auf Daten zugegriffen wird. Die LI führt die Schutzbedarfsfeststellungen von IT-Systemen und IT-Anwendungen in enger Abstimmung mit dem Auftraggeber durch.

Die manuelle Übermittlung und die Weitergabe von Daten liegen im vollen Verantwortungsbereich der Endanwender. Aufgrund der Sensibilität von Daten und Informationen hat der Anwender selbst zu entscheiden, welche Kommunikationsmittel er verwendet. Die LI stellt den Dienststellen ein Verzeichnis von Verarbeitungstätigkeiten gemäß DSGVO zur Verfügung. Die Berechtigungsverwaltung (Rollenzuordnung) hält für jede Anwendung den Dateneigentümer (auftraggebende Dienststelle) fest. Die Schnittstellen für alle Daten werden in einem Verzeichnis beschrieben und erfasst.

Alle Dienststellen des Landes haben eigenverantwortlich je nach Art der verwendeten Daten, nach Umfang und Zweck der Verwendung sowie unter Beachtung des Standes der technischen Möglichkeiten und der wirtschaftlichen Vertretbarkeit Maßnahmen zu treffen, dass die Daten

- vor zufälliger und unrechtmäßiger Zerstörung und Verlust geschützt sind,
- ordnungsgemäß verwendet werden und
- Unbefugten nicht zugänglich sind.

Folgende Sicherheitsmaßnahmen sind in allen Dienststellen jedenfalls einzuhalten:[8]

1. Belehrung der Mitarbeiter über Datenschutzvorschriften und
2. Datensicherheitsvorschriften und über die damit in Verbindung stehenden Pflichten;
3. Festlegung der Berechtigung zum Betrieb der Datenverarbeitungsgeräte
4. (Benutzerkennwort und Passworteingabe bei jedem von einer Person in Betrieb genommenen Gerät);

[8] Erlass 9.10. vom 20. September 2001, Datenschutz und Sicherheit.

5. selektive Auswahl der Zugriffsberechtigungen auf Daten und Programme;
6. Absicherung jedes Gerätes oder Programmes durch Vorkehrungen gegen unbefugte Inbetriebnahme (Geheimhaltung der Passwörter, unverzügliches Ändern bei Bekanntwerden eines Passwortes, Verbot, Sperre der Arbeitsstationen bei kurzzeitiger Abwesenheit);
7. Schutz der Datenträger vor Einsicht und Verwendung durch dienststellenfremde Personen (Aufbewahrung von Akten und Datenträgern unter Verschluss)
8. Zutrittsregelung zu den Räumlichkeiten der Dienststelle (Schließanlagen, Versperren der Büroräume bei Abwesenheit);
9. klare Aufgabenverteilung zwischen Organisationseinheiten und Mitarbeitern;
10. Bindung der Verwendung von Daten an das Vorliegen gültiger Aufträge.

Den Dienststellenleitern obliegt es, für die Einhaltung der Sicherheitsmaßnahmen Sorge zu tragen und gegebenenfalls eine dienststelleninterne Dokumentation über die getroffenen datenschutzrechtlichen Maßnahmen zu führen.

Daneben kann die LI weitere technische Sicherheitsmaßnahmen veranlassen. So kann sie etwa bei Änderungen, Abfragen und Übermittlungen Daten mitprotokollieren.

Dezentrale IT-Anwendungen der Dienststellen, wie etwa Förderungen in den Abteilungen 1 und 4 und beim Sozialen Informationssystem in der Abteilung 3, werden federführend durch die Abteilungen mit Unterstützung der IT entwickelt oder beauftragt und eingesetzt.

7. Management der Software

(1) Die LI verfügt über ein übergreifendes und automatisiert gesteuertes Lizenzmanagement. Grundsätzlich setzt die LI möglichst nur eine Softwareversion eines Produktes ein. Bevor Lizenzen beschafft werden, prüft die LI, ob bestehende Lizenzen umverteilt werden können, um ungenutzte Lizenzen zu vermeiden.

Die LI verfügt über ein Verzeichnis, welche Versionen einer Software derzeit eingesetzt werden. Über eine Applikation verteilt die LI Software im Clientbereich und aktualisiert sie.

Benutzer und Benutzergruppen werden über ein zentrales Identity-Management eingerichtet. Dabei wird von den im Personalinformationssystem festgelegten Aktivitäten ausgegangen. Die zugelassenen Benutzer, angelegten Benutzergruppen und Rechteprofile sind nachvollziehbar dokumentiert. Die Mitnahme von Datenträgern und Komponenten außer Haus ist in den Datenschutzinformationen für Anwenderinnen geregelt. Je nach Schutzbedarf der IT-Systeme und IT-Anwendungen werden angemessene Identifikations- und Authentifizierungsmechanismen angewendet; so ist etwa im Sozialbereich eine Drei-Faktor-Authentifizierung üblich.

Die Konfiguration der Anwendungen, Systeme und Netze wird nachvollziehbar dokumentiert, wobei die Systemkonfiguration in die Datensicherung eingeschlossen wird.

Es existiert ein Konzept, das den Umfang und die Auswertung der Protokollierung festlegt. So gibt es etwa Standardfestlegungen für Protokolldateien; diese werden nach Ablauf der Aufbewahrungsfrist automatisch gelöscht. Das OrgRL sieht für den Zugriff auf diese Protokolldateien ein eigenes Verfahren vor.

Die LI hat Externe damit beauftragt, die eingesetzte Software laufend zu überprüfen. Diese Prüfungen gewährleisten, dass sicherheitsrelevante Updates unverzüglich und in Abstimmung mit anderen Systemänderungen durchgeführt werden können. Darüber hinaus werden Upgrades für alle Anwendungen in Abstimmung mit anderen Systemänderungen geplant. Anlässlich dieser wird auch geprüft, ob die zur Verfügung stehende Software noch benötigt wird.

8. Datenbestände im Kontext zum Datenmanagement

(1) Aufgabe des Datenmanagements ist es, auf der Grundlage der Datenarchitektur alle im Unternehmen verwendete Datenbestände zu planen, zu überwachen und zu steuern. Um gewünschte Daten angemessener Qualität verfügbar zu machen, sollte das Datenmanagement mehrere Kernaufgaben abdecken. Diese betreffen vor allem die Datenanalyse, Datenmodellierung, Datenbeschaffung, Datensicherung und Datensicherheit.

Die LI deckt diese Kernaufgaben wie folgt ab:

Datenanalyse

Ziel der Datenanalyse ist es, einen Überblick darüber herzustellen, wer welche Daten für welche Anwendungen erhält oder benutzt. So führt die LI für personenbezogene Daten ein zentrales Verzeichnis von Verarbeitungstätigkeiten. Dieses enthält etwa Dateneigentümer sowie Daten- und Empfängerkategorien pro Verarbeitung.

Datenmodellierung

Bei der Datenmodellierung werden zu einem definierten Kontext relevante Objekte mittels ihrer Attribute und Beziehungen beschrieben. Konsolidierte Daten, wie etwa Stammdaten, werden zentral verwaltet und können von allen Anwendungen genutzt werden. Zu den Stammdaten zählen etwa Adressen, Postleitzahlen und Dienststellen. Die Integration von zentralen, übergeordneten Daten oder Anwendungen ist gesondert geregelt.

Datenbeschaffung

Der Dateneigentümer (auftraggebende Dienststelle) ist für die organisatorischen Regelungen und Berechtigungen und damit auch für die Dateninhalte verantwortlich. Dies gilt sowohl für strukturierte als auch unstrukturierte Daten.

Datensicherheit

Die IT-Sicherheitsrichtlinie der LI regelt, wie die Sicherheit der Daten zu gewährleisten ist (Verfügbarkeit, Vertraulichkeit und Integrität). Sie regelt etwa Authentisierung, Zugangskontrolle, Sicherung der Serversysteme und Überwachung der Sicherung. Der

IT-Grundschutz ist gewährleistet, Zertifizierungen gemäß ISO/IEC 27001 bestehen derzeit nicht.

Aufgabenträger des Datenmanagements

Für das Datenmanagement definiert die LI den IT-Architekten, der für das Festlegen von IT-Standards zuständig ist, im Referat 0/23 – Softwareentwicklung und den Datenbankadministrator im Referat 0/22 - Infrastruktur als Aufgabenträger.

Datensicherung

Die LI verfügt über ein Konzept, welches das Datensicherungsgrundkonzept und Verfahren zur Sicherung festlegt. So sind etwa für Betriebssysteme und Datenbanken Fristen für die Aufbewahrung von Sicherungen festgelegt. Für das Wiederherstellen von Netzlaufwerkdaten ist ein eigener Ablauf vorgesehen.

Outsourcing

Derzeit sind die Dienststellen für Cloudlösungen in ihrem Zuständigkeitsbereich verantwortlich (z.B. Energieausweise in der Abteilung 4, Beteiligungsverfahren in der Abteilung 7, Wohnbauförderung in der Abteilung 10). Dementsprechend beauftragen die Dienststellen auch Cloudlösungen.

In ihrem Zuständigkeitsbereich schließt die LI mit externen Dienstleistern Verträge ab. Einen Überblick über die von der Landesverwaltung insgesamt ausgelagerten Arbeits- oder Geschäftsprozesse hat die LI zum Zeitpunkt der Prüfung nicht.

(2) Der Landesrechnungshof empfiehlt der LI, an externe Dienstleister ausgelagerte datenschutzrechtliche Verpflichtungen alle zwei bis drei Jahre auf deren Einhaltung hin zu überprüfen.

(3) Das Amt erklärt in seiner Gegenäußerung, externe Dienstleister datenschutzrechtlich künftig durch unabhängige, spezialisierte Firmen überprüfen zu lassen; dafür erforderliche Budgetmittel seien für das Jahr 2019 bereits eingeplant.

Kryptokonzept

Die IT-Sicherheitsrichtlinie enthält Vorgaben, welche Daten oder Datenträger bei Zugriff und Weitergabe zu verschlüsseln sind. Alle lokalen PC-Daten werden standardmäßig verschlüsselt. Bei der Smartphone-Synchronisation wird eine Verschlüsselung am Smartphone erzwungen.

Auf jedem PC/Notebook steht der Bitlocker zur Verfügung. Im IT-Anwenderforum steht eine entsprechende Beschreibung zur Verfügung. Signiert wird generell über die Amtssignatur.

Der Direktor des Landesrechnungshofes:

Mag. Ludwig F. Hillinger e.h.

9. Anhang:

9.1 Gegenäußerung des Amtes der Landesregierung

LAND SALZBURG

Landesrechnungshof
z.H. Herrn Direktor Mag. Ludwig F. Hillinger
Nonnbergstiege 2
Postfach 527
5020 Salzburg

Landesamtsdirektion

Zahl (Bitte im Antwortschreiben anführen)
2002-42/22-2018

Datum
14.11.2018

Betreff
Feststellungen zur Prüfung "Strategische IT-Planung";
Stellungnahme
Bezug: 003-3/199/19-2018

Chiemseehof
Postfach 527 | 5010 Salzburg
Fax +43 662 8042-2164
landesamtsdirektion@salzburg.gv.at
Dipl.-Ing. Rudolf Krejsa
Telefon +43 662 8042-2853

Sehr geehrter Herr Direktor!

Bezugnehmend auf das Schreiben des Landesrechnungshofes vom 17.10.2018 wird folgende Stellungnahme abgegeben:

Zu 2.1 - Organisation und internes Kontrollsystem (IKS):

Bei der angeführten "Betriebsstörung ELISA" handelt es sich um keine Prozessbeschreibung, sondern um ein dem Prozess "Problemmanagement" angehängtes, praktisches Beispiel zur konkreten Abbildung des Problemmanagement-Prozesses.

Die Anregung des Landesrechnungshofes, die Steuerungskompetenz des Herrn Landesamtsdirektors in den IT-Prozessen explizit zu verankern, wird bereits im laufenden Reformvorhaben Land-Salzburg@2022 berücksichtigt. Die Fachgruppe "Informatik und interne Dienste" ist Pilotdienststelle bei der Festlegung eines einheitlichen Strategieprozesses als wesentliche Grundlage, um das strategische Denken und Handeln in der Salzburger Landesverwaltung zu stärken. Sobald die Ergebnisse für verbindlich erklärt werden, erfolgt die entsprechende Anpassung der Prozesse in 0/2.

Zu 3.1 - IT-Leitbild:

Das IT-Leitbildung wurde auf Grund der Empfehlung des Landesrechnungshofes bereits präzisiert.

Zu 4.7 - Vorstoß zu einer neuen IT-Strategie:

Die Fachgruppe 0/2 hat inhaltlich die IT-Strategie laufend an die aktuellen Erfordernisse angepasst und mit mir abgestimmt. Darüber hinaus wird im Rahmen des Reformprozesses LandSalzburg@2022 derzeit an einer Digitalisierungs- und Innovationsstrategie für die Salzburger Landesverwaltung gearbeitet. Daran anknüpfend ist im nächsten Schritt vorgesehen, die bestehende IT-Strategie zu evaluieren und dann den übergeordneten strategischen Vorgaben entsprechend neu auszurichten. Die Empfehlungen des Landesrechnungshofes werden dabei einbezogen werden.

Zu 5.1 - Zweck der Planung der Maßnahmen:

Bedingt durch den raschen technologischen Wandel wird es für Dienststellen immer einfacher, ohne Einbindung der zentralen IT Anwendungen (Cloud) eigenständig einzusetzen. Deshalb ist geplant, die Regeln für diese Thematik im Rahmen des Projektes "Digitalisierungs- und Innovationsstrategie" (LandSalzburg@2022) auszuarbeiten.

Hinsichtlich dezentraler Organisationsprojekte wird Folgendes angemerkt: Die Verantwortung, dass nur solche dezentralen Organisationsprojekte umgesetzt werden, deren Kosten ein ausreichender Nutzen gegenübersteht, kann grundsätzlich nur bei der für ein Projekt verantwortlichen Dienststelle liegen. Gerade kleinere Projekte bzw. Vorhaben, die in sehr großer Anzahl in der Landesverwaltung vorhanden sind, können schon aufgrund ihrer Anzahl nicht zentral einem Controlling zugeführt werden. Ein zentrales Controlling würde in diesen Bereichen auch mehr Verwaltungsaufwand als Nutzen erzeugen. Anders stellt sich die Situation bei besonders komplexen Organisationsprojekten in einer dezentralen Dienststelle oder bei Projekten, die mehrere oder sogar alle dezentrale Dienststellen betreffen, dar. Für diese übergeordneten Projekte (insbesondere jene aus dem Reformprogramm LandSalzburg@2022, aber zukünftig auch für weitere größere Organisationsentwicklungsprojekte) existiert seit Sommer dieses Jahres eine zentrale, koordinierende Stelle im Büro des Landesamtsdirektors.

Darüber hinaus werden noch im Herbst 2018 in der Landesverwaltung neue Projektmanagementstandards eingeführt. Diese Standards sehen für alle Projekte einen schriftlichen Projektauftrag vor, welcher die angestrebten Ziele und die geplanten Ressourcen eines Projektes enthalten muss. In einem ebenfalls vorgesehenen schriftlichen Abschlussbericht muss dargestellt werden, inwieweit die Ziele und damit der angestrebte Nutzen erreicht werden konnte. Diese Standards sollten das Projektmanagement in der Landesverwaltung weiter professionalisieren und damit dazu beitragen, dass nur solche Vorhaben umgesetzt werden, die bestimmte organisatorische Anforderungen erfüllen und deren Kosten ausreichender Nutzen gegenübersteht.

Zu 8 - Datenbestände im Kontext zum Datenmanagement:

So wie in der IT-Branche üblich, sollte die empfohlene datenschutzrechtliche Überprüfung der externen Dienstleister durch unabhängige, darauf spezialisierte Firmen durchgeführt werden. Die Empfehlung des Landesrechnungshofes wird aufgegriffen. Die dafür zusätzlich erforderlichen Budgetmittel werden bereits im Budget 2019 eingeplant.

Der Landesamtsdirektor:
DDr. Sebastian Huber, MBA

www.salzburg.gv.at

Amt der Salzburger Landesregierung | Landesamtsdirektion
Postfach 527 | 5010 Salzburg | Österreich | Telefon +43 662 8042-0* | post@salzburg.gv.at