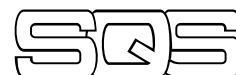


ASSESSMENTBERICHT MANAGEMENT SUMMARY



Schweizerische Vereinigung
für Qualitäts- und Management-
Systeme (SQS)

Bernstrasse 103
3052 Zollikofen
Schweiz

T +41 58 710 35 35
F +41 58 710 35 45

www.sqs.ch

Zollikofen, 27. Januar 2019
Seite 1 von 5
Dokument 599_1

Berenike Schmidt
berenike.schmidt@sqs.ch
T +41 58 710 33 72

Unternehmen/Organisation

LUSTAT Statistik Luzern
Burgerstrasse 22
Postfach 3768
6002 Luzern
Schweiz

Kontaktperson Herr Norbert Riesen
Herr Enrico Moresi

T +41 41 228 56 33

Anzahl Mitarbeitende 23.5 FTE

Dienstleistung

Audit/Assessment
Überprüfung LUSTAT durch SQS

Projektnummer
P44561.001.01.78

Audit/Assessment Beginn/Ende
10. Januar 2019

Auditierter Bereich
Ganze zentrale Statistikstelle des Kantons Luzern

Tätigkeitsgebiet
Statistische Tätigkeiten gemäss auf dem kantonalen
Statistikgesetz basierenden Mehrjahresprogramm

Geschäftskonto 319848

norbert.riesen@lustat.ch
enrico.moresi@lustat.ch

F

Normative Grundlagen
Statistikgesetz des Kantons Luzern, Stand: 1. Aug. 2009

Scopes
36

Nächste Überprüfung
2022, in Absprache mit LUSTAT

Auditorin/Assessorin 1
Frau Berenike Schmidt

Auditor/Assessor 2
Herr Dr. Reto Fanger (Juristischer Fachexperte)

Freigaben

Datum

Unterschrift

Leitende Auditorin/Assessorin

27. Januar 2019



1. Management Summary zum Audit vom 10. Januar 2019

1.1. Ausgangslage

Gemäss § 12 Abs. 1 des Statistikgesetzes (SRL 28a) werden die statistischen Tätigkeiten der zentralen Statistikstelle periodisch, mindestens alle vier Jahre, durch eine Fachstelle überprüft. Der Regierungsrat ordnet nach § 12 Abs. 2 Statistikgesetz diese periodische Überprüfung an, was mit Beschluss des Regierungsrates vom 9. März 2010 (Protokoll 252) erstmals erfolgt ist. Zur Umsetzung dieser Anforderungen hat LUSTAT die Schweizerische Vereinigung für Qualitäts- und Management-Systeme (SQS) mit der Überprüfung beauftragt.

Die SQS ist seit über 35 Jahren die führende Zertifizierungs- und Bewertungsinstitution in der Schweiz. Ihre umfassende Produktpalette deckt Zertifizierungen in nahezu allen Bereichen der Wirtschaft ab. Eingebunden ins weltweite Zertifizierungsnetzwerk von IQNet schafft sie durch ihre langjährige zuverlässige Tätigkeit Vertrauen, Sicherheit und nachhaltigen Erfolg bei ihren Kundinnen und Kunden. Sie ist die einzige Anbieterin für Zertifizierungen von Datenschutz Managementsystemen nach dem Schweizerischen Standard GoodPriv@cy. GoodPriv@cy ist in der Schweiz und den angrenzenden Ländern der mit Abstand bekannteste Standard zur Zertifizierung von Datenschutz-Managementsystemen. Die aktuelle Version ist GoodPriv@cy:2018. Diese Version bindet die Anforderungen, basierend auf ISO 9001:2015 (Struktur und Inhalt) und der EU Datenschutzgrundverordnung, ein.

1.2. Vorgehen

Die Überprüfung sollte sich gemäss Auftrag der Regierung auf alle Prozesse und Themen der statistischen Aufgaben beziehen. Die Überprüfung sollte vor dem Hintergrund der Einhaltung des Statistikgesetzes erfolgen. Es sind folgende Punkte einbezogen worden: Führung, Organisation, das statistische Mehrjahresprogramm, Datenschutz, die Unterstützungsfunktionen und die Sicherheitsaspekte.

Für die Überprüfung hat die SQS folgende Standards zur Orientierung und Bewertung beigezogen

- ISO 9001:2015 – Qualitäts- und Prozessmanagement
- GoodPriv@cy:2018 – Datenschutz Management

1.3. Gesamteindruck

Bei der Beurteilung des Managementsystems von LUSTAT nach den Kriterien der Standards ISO 9001:2015 und GoodPriv@cy kann festgestellt werden, dass weder Hauptabweichungen noch Nebenabweichungen identifiziert werden konnten und ein gutes Auditergebnis erzielt wurde.

Führung

Auf Basis der gesetzlichen Grundlagen und der relevanten Richtlinien für die Datenverarbeitung, sowie dem Leistungsauftrag, der Eignerstrategie, der Charta und der daraus resultierenden Mehrjahresplanung leitet die Führung gut nachvollziehbar die Ziele der Mitarbeitenden ab.

Seit dem 30. September 2015 verfügt LUSTAT über eine Geschäftsordnung, in der die Führungsgrundsätze, die Organisation, die Sitzungsordnung und die Dokumentation von Geschäften definiert sind. Auch die Aufgaben, Kompetenzen und Verantwortlichkeiten, sowie die Unterschriften- und Finanzkompetenzen sind hier pro Funktion dokumentiert. Dieses Dokument wird von Mitarbeitenden geschätzt und erleichtert aufgrund seines klärenden Charakters die Geschäftsführung.

Die Herausforderungen, die die Sparmassnahmen des Kantons ergeben, werden mit einer detaillierten Ressourcen-Planung unter Einbezug des Time Tools effektiv geführt. Es bestehen gut geeignete Messgrössen und Instrumente, die es erlauben, die Zielerreichung zeitgerecht zu überwachen.

Die Führung bekennt sich zu einem systematischen Managementansatz, der mit einem gut gepflegten Managementsystem unterstützt wird. Die Elemente des Managementsystems zeigen die Regelkreis-Systematik nach Deming auf (Plan-Do-Check-Act) und die gewählten Führungselemente zeigen einen guten Reifegrad.

Personal & Wissensmanagement

Die Aus- und Weiterbildung der Mitarbeitenden hat einen hohen Stellenwert und das Personal beeindruckt durch ein fundiertes Fachwissen. Die Mitarbeitenden sind verpflichtet, die für sie relevanten und anwendbaren Gesetze und die weiteren Rahmenbedingungen zu kennen.

Interne Schulungen (eLearning, regelmässig stattfindende „IT-Meetings“ etc.) und Einführungen werden wirksam durchgeführt. Die jährlich durchgeführten Mitarbeitergespräche bilden auch die Plattform, um Weiterbildungsmassnahmen zu besprechen und zu planen. LUSTAT gewichtet das Wissensmanagement bereits im Rahmen der Unternehmensstrategie hoch und setzt diese in ihren Prozessen konsequent um. Ein wichtiges Element für die kontinuierliche Verbesserung und den internen Wissenstransfer bilden die Projektabschlussberichte. Hier werden die Lessons Learned aufgeführt und Verbesserungen thematisiert. Das Personal ist methodisch gut geschult und flexibel einsetzbar, so dass je nach Arbeitsanfall auch zwischen den Bereichen Arbeiten übertragen werden können. Mit personellen Doppelbesetzungen in allen Kernkompetenzbereichen und klaren Stellvertretungsregelungen, sind zusätzliche Sicherungen des relevanten Know-Hows der Organisation implementiert.

Die Zusammenarbeit und die Unternehmenskultur erscheinen gut und die Mitarbeitenden zeigen grosses Engagement für ihre Aufgaben. Dementsprechend weist LUSTAT eine sehr tiefe Fluktuation auf.

Sicherheit

LUSTAT verfügt über ein methodisch und inhaltlich hervorragend erarbeitetes integrales Sicherheitskonzept (Stand 01.01.2019, Version 1.8). Hierin werden die Sicherheitsteilbereiche Informationssicherheit, Physische Sicherheit, Business Continuity Management, Arbeitssicherheit, Versicherungsschutz und Umweltschutz abgedeckt. Um die Umsetzung zu unterstützen, wurden mehr Ressourcen für die Funktion SIBE allokiert. Die Umsetzung ist noch nicht abgeschlossen. Insbesondere die Erstellung des Schutzinventars sollte rasch vollendet werden, um ggf. kritische Bereiche zu erkennen und (Sofort)- Massnahmen setzen zu können.

Dokumenten Management

Nachdem erkannt worden ist, dass hinsichtlich des Dokumenten Managements keine klare Vorgaben besteht, wurde die Weisung „GEVER Organisationsvorschriften LUSTAT“ erarbeitet, die die elektronische Geschäftsverwaltung definieren soll. Wiederum fällt bei diesem Konzept die professionelle und vorbildliche Aufarbeitung des Themenbereichs auf. Für die gewählte Methodik muss kein spezifisches GEVER Tool verwendet werden. Dennoch ist eine Überführung in ein bekanntes Tool (CMI Axioma) bereits im Konzept vorbereitet und kann zu einem späteren Zeitpunkt umgesetzt werden. Der Registraturplan ist bereits implementiert und die Archivierung kann halbautomatisch in der Explorer-Ablagestruktur vorgenommen werden. Die Weisung ist am Vortag des Audits in Kraft gesetzt worden.

Kern- und Unterstützungsprozesse

Während des Audits konnte festgestellt werden, dass die Prozesse sehr gut dokumentiert und aktuell gehalten wurden. Die Zusammenarbeit zwischen den Bereichen ist gut organisiert und die Schnittstellen werden zweckdienlich geführt. Auch hinsichtlich der Stellvertretungsregelungen sind durchgängig sinnvolle Lösungen gewählt worden.

Es ist zudem aufgefallen, dass auch hinsichtlich der externen Kommunikation und der Vermittlung von Informationen innovative Methoden evaluiert und umgesetzt werden. Insgesamt kann von einem gut geführten, effektiven Prozessmanagement berichtet werden.

1.4 Schwerpunkt Datenschutz

Die Einhaltung des Datenschutzes ist für die Vertrauenswürdigkeit und damit für die Arbeit von LUSTAT von zentraler Bedeutung. Die diesbezüglich anwendbaren gesetzlichen Anforderungen ergeben sich aus dem kantonalen Statistikgesetz und den dazu gehörenden Ausführungsverordnungen, aus dem kantonalen Registergesetz und der Registerverordnung. Darüber hinaus ist LUSTAT dem kantonalen Datenschutzgesetz und dessen Datenschutzverordnung, dem kantonalen Informatikgesetz mit den zugehörigen Ausführungsverordnungen und den daraus abgeleiteten, von der kantonalen Dienststelle Informatik (DIIN) erlassenen Sicherheitsregelungen, -vereinbarungen und -merkblättern sowie dem Bundesstatistikgesetz unterstellt. LUSTAT hat sich darüber hinaus verpflichtet, die Charta „Öffentliche Statistik der Schweiz“ sowie den Verhaltenskodex der EU für europäische Statistiken einzuhalten.

Insgesamt konnte festgestellt werden, dass das Personal bereits beim Eintritt die datenschutzrechtlichen Grundlagen erläutert und schriftlich abgegeben erhält und eine Vertraulichkeitserklärung unterzeichnet. Das Personal konnte während des Audits nachweisen, dass durchgängig in allen relevanten Prozessen und Projekten eine hohe Sensibilität bezüglich der Datenschutzthematik besteht und gelebt wird.

Zusammenfassende Würdigung

- Der Leistungsauftrag ist durch die Eignerstrategie konkretisiert und der gesamte Zielsetzungs- und Zielcontrolling-Prozess folgt einer klaren Systematik.
- Die Organisation zeigt sich hinsichtlich der Aufbauorganisation gefestigt und sehr effektiv. Die Verantwortlichkeiten und die Stellvertretungen sind definiert und die Schnittstellen werden gut geführt.
- Die Führungsprozesse sind etabliert und werden befolgt. Die Planung erfolgt weitsichtig und systematisch. Dies trifft nicht nur auf die oberste Ebene, sondern auch auf die Bereichsebenen zu.
- Das Personal verfügt über die notwendigen Kompetenzen und Qualifikationen.
- Die gesetzlichen Grundlagen sind bekannt. Die Anforderungen an die Organisation LUSTAT sind systematisch identifiziert, analysiert und umgesetzt worden.
- Der Auftrag im Bereich der öffentlichen Statistik wird gesetzeskonform auf Basis des Mehrjahresprogramms umgesetzt und die Umsetzung mit geeigneten Instrumenten überwacht.
- Die Abläufe sind geeignet sowie festgelegt und werden von den Mitarbeitenden gut beherrscht.
- Geeignete Kontrollstrukturen (Vier-Augen-Prinzip, Redaktion etc.) stellen sicher, dass nur Publikationen veröffentlicht werden, die den Qualitätsanforderungen von LUSTAT genügen.
- Dem Datenschutz kommt ein sehr hoher Stellenwert zu. Das Personal ist über die Datenschutzvorgaben informiert. Die Datenschutzvorgaben werden in den statistischen Prozessen angemessen befolgt.
- Die Organisation realisiert Optimierungen und Verbesserungen und achtet auf eine fundierte wissenschaftliche Aufbereitung von Themen und Konzepten.

2. Relevante Hinweise zur kontinuierlichen Verbesserung

- 1 Es empfiehlt sich die Umsetzung des Sicherheitskonzepts zügig voranzutreiben und hierfür Ressourcen zu allokalieren.
- 2 Bei den in Projekten organisierten Geschäftsprozessen werden nach Projektabschluss die Lessons Learned im Projektabschluss-Bericht zusammengefasst und Verbesserungen umgesetzt. Diese Vorgehensweise wird von Managementsystemen, wie der ISO 9001 bewusst gefördert/ verlangt (ISO 9001:2015 Kap. 9.2 Interne Audits). Es empfiehlt sich, auch für alle anderen Prozesse eine periodische Überprüfung der Aktualität und Wirksamkeit einzuführen. Die Management-Reviews (Quartalsberichte) könnten auf die Veränderungen des Umfelds (Kontext) gegenüber der Planungsphase eingehen. Auch die Bewertung der bestehenden Risikomassnahmen könnte hier thematisiert werden.
- 3 Für die Zusammenarbeit mit der DIIN besteht ein Service Level Agreement. Dieses SLA beschreibt die Definitionen von Ausfallzeiten und die Kriterien einer Priorisierung der kritischen Geschäftsapplikationen. Es fehlen hingegen jegliche Angaben für Verfügbarkeiten und Reaktionszeiten oder Wiederherstellungsgeschwindigkeiten. Dies entspricht nicht der bestehenden guten Geschäftspraxis, weshalb das SLA entsprechend zu ergänzen ist.
- 4 Die bei Verlust und Diebstahl von Informatikmitteln zu ergreifenden Massnahmen gemäss Ziffer 4.8 der Sicherheitsweisung LUSTAT Sicherheit lassen sich ohne Mobile Device Management-Lösung (MDM-Lösung), die von der kantonalen Dienststelle Informatik (DIIN) bereitzustellen ist, nicht umsetzen. Dies entspricht nicht der bestehenden guten Geschäftspraxis, weshalb DIIN zur zeitnahen Lieferung einer MDM-Lösung aufzufordern ist

Das Auditorenteam dankt allen Beteiligten für die konstruktive sowie offene Gesprächsatmosphäre während des Audits und wünscht weiterhin viel Erfolg bei der Weiterentwicklung des Managementsystems sowie der Organisation.

Für Fragen und Unterstützung stehen Ihnen die Auditoren gerne zur Verfügung.

Zollikofen, 4. März 2019 SHB/FNR/HIA