GPK Ettingen – Bericht über die Prüfungen 2022/2023

1 EINLEITUNG

Aufgabe

Die Geschäftsprüfungskommission („GPK“) ist beauftragt, zuhanden der Einwohnergemeindeversammlung jeweils im ersten Halbjahr über ihre das vergangene Jahr betreffenden Feststellungen zu Geschäften Bericht zu erstatten (Gemeindegesetz § 102a). Mit dem hier vorliegenden Bericht erfüllt die Geschäftsprüfungskommission somit ihren diesbezüglichen Auftrag für das Jahr 2022/2023.

Übersicht über die Themen

- Thema 1:
  Prüfung der IT
- Thema 2:
  Bauabrechnung Schulhaus «Hintere Matten»: Unterhalts- und Sanierungsarbeiten Trakt 4

Diese Themen wurden mit Frau Sibylle Muntwiler und Herrn Jean-Claude Baumann vorgängig abgestimmt.

Sitzungen

Datum	Thema	Teilnehmer
16.03.2023	Verabschiedung der Prüfungsthemen	DB, RH
08.06.2023	Besprechung GPK Bericht	SM, JCB, DB, RH, Geprüfte Stellen

Glossar

Abkürzung	Bedeutung
DB	Dieter Baumann
JCB	Jean-Claude Baumann
RH	Ralf Hofstetter
SM	Sibylle Muntwiler
GR	Gemeinderat

2 UNTERSUCHTES THEMA 1: "PRÜFUNG DER IT"

Ausgangslage

Die Informatik der Gemeinde Ettingen wird, mit punktueller Unterstützung durch externe Drittparteien, eigenständig betrieben. Der EDV-Verantwortliche der Gemeinde Ettingen ist für die Konzeption, die Implementierung sowie auch für den Betrieb der Informatik verantwortlich – er kann dabei ungefähr 40 bis 50 Stellenprozente für diese Tätigkeit aufwenden. Die Informatik der Schulen der Gemeinde Ettingen wird dabei nicht durch den EDV-Verantwortlichen, sondern in eigenständiger Regie durch die Schulen betrieben.

Ziele der GPK-Prüfung

1. Review der IT-Organisation
2. Review der relevanten Vorgaben im Bereich der IT (u.a. Policies, Proceduren, Guidelines)
3. Review der IT-Architektur (u.a. Betriebssysteme, Datenbanken und Applikationen sowie auch Schnittstellen)
4. Review der eigenständig erbrachten Dienstleistungen versus die ausgelagerten Dienstleistungen (sprich Outsourcing)
5. Review der wesentlichen IT-Prozesse und Kontrollen (namentlich Benutzeradministration, Änderungswesen / Patch Management, Incident / Problem Management, Datensicherung und Wiederherstellung, IT Desaster Recovery Management, Physische Sicherheit)
6. Review des Cyber Security Managements

Verwendete Unterlagen, unter anderem

- Aktenauflage / Sitzung des Gemeinderates, Nr. 2812022 vom Montag, 26. September 2022
- Budget EDV 2023
- Berechtigungen Server Gemeinde Ettingen
- IT-Sicherheits-Check vom 07. April 2022 inklusive zugehöriger Dokumente
- IT-Zusammenfassung des EDV-Verantwortlichen
- Systemdokumentation Dialog 23.01.2023
- Verträge zwischen der Gemeinde Ettingen und ausgewählten IT-Dienstleistern

Feststellungen GPK

Die Gemeinde Ettingen hat durch einen unabhängigen Berater eine Analyse der IT der Gemeinde Ettingen durchführen lassen. Die GPK hat unabhängig vom Bericht eine eigenständige Analyse durchgeführt und dabei folgende Feststellungen identifiziert:

- Wir weisen darauf hin, dass der EDV-Verantwortliche – trotz seiner Doppelfunktion – viel Zeit und Energie in die Informatik der Gemeinde Ettingen investiert, um diese möglichst optimal zu betreiben. Der EDV-Verantwortliche hat auch die Prüfung der GPK vorbereitet und optimal unterstützt.
- Der EDV-Verantwortliche der Gemeinde Ettingen konzipiert, implementiert und betreibt die Informatik für die Verwaltung der Gemeinde Ettingen mit ungefähr 40 bis 50

Stellenprozenten. Eine Stellvertretung innerhalb der Gemeinde Ettingen, welche im Bedarfsfall die relevanten Aufgaben zumindest temporär übernehmen könnte, ist nicht vorhanden. Die personelle Ausstattung wird dementsprechend durch die GPK der Gemeinde Ettingen als unzureichend erachtet.

- Die Schulen der Gemeinde Ettingen werden nicht durch den bei der Verwaltung der Gemeinde Ettingen angehängten EDV-Verantwortlichen betreut. Dementsprechend können die Synergie- und damit Kosteneinsparungspotentiale, welche sich durch eine zentralisierte Informatik in der Gemeinde Ettingen ergeben würden, nicht ausgeschöpft werden.
- Eine IT- respektive eine Digitalisierungsstrategie, welche die langfristige Weiterentwicklung der Informatik der Gemeinde Ettingen beschreibt, liegt nicht vor. Dementsprechend sind auch keine davon abgeleiteten taktischen (mittelfristig) und operativen (kurzfristigen) Ziele definiert. Dementsprechend wird die Informatik opportunistisch betrieben und primär von kurzfristigen Prioritäten, das heisst dem operativen Tagesgeschäft, getrieben.
- Der EDV-Verantwortliche tritt gegenüber der Gemeinde auch als Lieferant von verschiedenen Softwareprodukten auf. Dabei wurde von seiner Einzelunternehmung ein jährlicher Betrag von ungefähr CHF 3’000 an die Gemeinde Ettingen fakturiert. Zugehörige Rechnungen wurden aussagegemäss durch den EDV-Verantwortlichen geprüft und genehmigt.
- Punktuell sind relevante Dienstleistungen an externe Leistungserbringer ausgelagert. Insbesondere existieren zahlreiche Verträge respektive Service Level Agreements (SLAs) mit der Dialog Verwaltungs-Data AG. Trotz mehrfachen Anfragen durch den EDV-Verantwortlichen stand die Dialog Verwaltungs-Data AG während der Prüfung durch die GPK aber nicht für ein Gespräch zur Verfügung. Aussagegemäss hat sich die Dienstleistungsqualität seit dessen Verkauf an die Schweizerische Post im Jahr 2022 verschlechtert.
- Üblicherweise werden die definierten Leistungen durch einen Leistungserbringer erbracht und im Rahmen eines sogenannten Service Level Reporting periodisch über diese Dienstleistungen Bericht erstattet. Damit schaffen Leistungserbringer Transparenz über die vertragskonforme Leistungserbringung. Im Rahmen der Prüfung konnte ein entsprechendes Service Level Reporting nicht zur Verfügung gestellt werden. Damit konnte auch nicht nachvollzogen werden, ob die Leistung vertragskonform erbracht wird.
- Ausgewählte Konzepte, welche die IT-Architektur sowie auch relevante IT-Prozesse und Kontrollen beschreiben, liegen vor. Eine umfassende Dokumentation der relevanten Prozesse und Kontrolle konnte allerdings nicht zur Verfügung gestellt werden. Insbesondere konnte nicht nachvollzogen werden, ob sich die konzeptionellen Grundlagen von einem international anerkannten Standard wie beispielsweise CobiT und / oder ISO 27001 ableiten.
- Der Nachvollzug der Einhaltung der definierten Prozesse und Kontrollen war mangels entsprechender Kontrollnachweise nicht respektive nur punktuell möglich. Dementsprechend konnte nicht umfassend nachvollzogen werden, ob die Informatik gemäss anerkannter Branchenpraxis betrieben wird.
- Der physische Serverstandort ausschliesslich an einer Lokation ist, obwohl die Datenhaltung an unterschiedlichen Lokationen in der Schweiz hinterlegt sind, sowohl aus organisatorischen als auch aus technischen Gründen nicht optimal gelöst.

- Die Cyberangriffe, insbesondere Ransomware Attacken, haben in der letzten Zeit massiv zugenommen – dabei standen vermehrt auch öffentliche Institutionen, das heisst Gemeinden, im Fokus der Aufmerksamkeit. Das diesbezügliche Kontrolldispositiv ist daher ständig unter Druck, um den immer wieder neuen Herausforderungen gerecht zu werden und somit noch ausbaufähig.

Beurteilung und Empfehlung GPK

Wir empfehlen die Umsetzung der nachfolgenden Massnahmen:

1. Die durch die Firma «IT Management & Beratung» durchgeführte Analyse und zugehöriger Bericht vom November / Dezember 2022 sollte entsprechend berücksichtigt werden. Die dabei vorgeschlagenen Varianten sollten beurteilt und in die Weiterentwicklung der Informatik aufgenommen werden.
2. Eine IT-Strategie sollte definiert und durch die zuständigen Stellen genehmigt werden. Diese IT-Strategie sollte sich dabei von den strategischen Zielen der Gemeinde ableiten und die Ziele sowohl der Verwaltung als auch der Schulen umfassen.
3. Aus der langfristigen IT-Strategie sollten die taktischen (mittelfristig) sowie auch die operativen (kurzfristig) Pläne ableiten.
4. Basierend auf der IT-Strategie und zugehörigen Plänen sollte entschieden werden, welche Dienstleistungen intern respektive welche Dienstleistungen durch externe Leistungserbringer erbracht werden sollen. Dabei ist auch die vertiefte Zusammenarbeit mit dem Kanton respektive mit den umliegenden Gemeinden zu prüfen.
5. Aus Gründen der Unabhängigkeit sollte kritisch geprüft werden, ob Mitarbeitende der Gemeinde auch als Lieferanten auftreten sollten. Im Zweifelsfall sollten unabhängige Softwareanbieter präferiert werden. Entsprechende Rechnungen sind in jedem Fall zwingend durch eine unabhängige zweite Person zu prüfen und freizugeben.
6. Im Zuge der Prüfung einer möglichen Auslagerung ist auch zu validieren, ob der physische Serverraum aufgelöst und die Systeme, Applikationen sowie auch zugehörige Daten in ein ordentliches Rechenzentrum oder in eine (private) Cloud in der Schweiz migriert werden könnten.
7. Insbesondere sollte auch validiert werden, ob der bestehende Leistungserbringer die gewünschte Leistung in einem adäquaten Kosten-/ Nutzenverhältnis sowie in der entsprechenden Qualität erbringt.
8. Daraus abgeleitet ist die Informatikorganisation entsprechend mit Ressourcen auszugestalten, damit die Dienstleistungen für die Verwaltung als auch für die Schulen in der entsprechenden Qualität erbracht werden können.
9. Basierend auf den entsprechenden international anerkannten Standards sind die wesentlichen IT-Prozesse und IT-Kontrollen zu definieren, zu genehmigen und zu implementieren sowie zu betreiben. Die wesentlichen IT-Kontrollen sind dabei so zu dokumentieren, dass deren adäquate Durchführung nachvollzogen werden kann.
10. Periodisch sollten die Prozesse und Kontrollen einem internen und auch externen Assessment unterzogen werden, um die kontinuierliche Maturität sowie auch Qualität sicherstellen zu können.
11. Aufgrund zahlreicher medienwirksamer Ereignisse bei Gemeinden sollten dem Themengebiet Cyber Security weiterhin Aufmerksamkeit geschenkt werden. Die durch die Gemeinde bereits initiierten Massnahmen im Bereich der Informatik müssen prioritär und

risikoorientiert weiterverfolgt werden. Auch sollten die Mitarbeitenden bezüglich relevanter Aspekte entsprechend periodisch geschult und trainiert werden.

3 Untersuchtes Thema 2: "Bauabrechnung Schulhaus «Hintere Matten»: Unterhalts- und Sanierungsarbeiten Trakt 4"

Ausgangslage

Am 12. Dezember 2018 wurde an der Gemeindeversammlung die Sondervorlage für die Sanierung des Mehrzweckgebäudes Möslibach (Trakt 4) genehmigt. Die Sondervorlage über CHF 1.9 Mio. wurde dabei von der Gemeindeversammlung einstimmig angenommen. Die Vergabe des Planungsauftrags für die Sanierung erfolgte dabei an die Andres Architekten AG in Ettingen.

Ziele der GPK Prüfung

- Vergabeprozess: Anhand der Gemeinderatsbeschlüsse soll beurteilt werden, ob der Vergabeprozess den Vorgaben der Gemeinde entsprochen hat.
- Abstimmung: Abstimmung der Rechnungen mit der Bauabrechnung sowie der Buchhaltung.
- Einhaltung Kredit: Feststellen, wie hoch die effektiven Baukosten ausgefallen sind, ob der genehmigte Kredit ausgereichend war und Einfordern ausgewählter Abnahmeprotokolle.

Verwendete Unterlagen

- Protokoll der Einwohnergemeindeversammlung Nr. 02118 vom 12. Dezember 2018
- Verschiedene sachrelevante GR-Protokolle
- Verträge mit den einzelnen Dienstleistern respektive Handwerker
- Rechnungen der einzelnen Dienstleister respektive Handwerker
- Baukostenschlussabrechnung
- Verpflichtungskreditkontrolle

Sachverhalte der GPK

Die GPK rapportiert die nachfolgenden Sachverhalte:

Vergabeprozess

- Gemäss Auskunft der Gemeinde Ettingen werden Offerten von nicht beauftragter Firmen typischerweise nicht abgelegt. Damit wird ein Nachvollzug der Verordnung zum Beschaffungswesen der Gemeinde Ettingen durch die GPK erschwert respektive verunmöglicht.
- Der Gemeinderat vergab den Auftrag zur Ausarbeitung der Ausführungsplanung und der Bauleitung für die Sanierungsmassnahmen Trakt 4 gemäss Architekturhonorarofferte im Zeitmodell vom 11. Januar 2019 freihändig an das Büro Andres Architekten, Brühlmattweg 1, 4107 Ettingen, zum Betrag von CHF 149'572.00 inkl. Mehrwertsteuer. Dies aufgrund deren Projektkenntnisse durch die im Vorfeld erbrachten Planungsleistungen. Gemäss der Verordnung zum Beschaffungswesen wäre für die Vergabe das Einladungsverfahren vorgesehen.

- Der Gemeinderat genehmigte die Aufträge an die Firmen basierend auf den durchgeführten Submissionen. Im Rahmen der Ausführung der Arbeiten wurden zusätzliche Arbeiten im Rahmen von Nachträgen ausgeführt und verrechnet. Aufgrund fehlender Dokumentation (beispielsweise Gemeinderatsprotokolle, Werkverträge, Nachtragsvereinbarungen) konnten diese Nachträge durch die GPK nicht umfassend nachvollzogen werden.
- Für die übrigen im Rahmen der Sanierung eingesetzten Handwerker wie beispielsweise die GEZE Schweiz AG wurden durch die Gemeinde im Rahmen der Vergabe keine Unterlagen zur Verfügung gestellt. Damit konnte nicht nachvollzogen werden, ob die Verordnung der Gemeinde Ettingen zum Beschaffungswesen eingehalten wurde.

Abstimmung der Rechnungen mit der Bauabrechnung

- Alle Rechnungen, welche Bestandteil unserer Stichprobe waren, konnten mit der Bauabrechnung des Architekten sowie dem Konto 2171.5040.0021 der Buchhaltung abgestimmt werden.

Einhaltung Kredit

- Die Sanierungsarbeiten im Trakt 4 wurden im 2021 abgeschlossen. Trotz formeller Anfrage an die Bauverwaltung Ettingen konnte das Protokoll der Schlussabnahme der Elektroanlagen nicht durch die Gemeinde beschafft werden.
- Der genehmigte Kredit von CHF 1.9 Mio. wurde mit aufgelaufenen Kosten von CHF 1’580’291.20 um insgesamt CHF 319'708.8 unterschritten.
- Die in der Sondervorlage vom 12. Dezember 2018 aufgeführten Förderbeiträge in der Höhe von CHF 70’000 wurden nicht vereinnahmt.

Beurteilung und Empfehlung der GPK

Wir empfehlen die Umsetzung der nachfolgenden Massnahmen:

- Es sollte rechtlich abgeklärt werden, ob auch Offerten von nicht beauftragter Firmen abgelegt werden müssen – nur so können die Vergabeentscheide der Gemeinde umfassend durch die GPK nachvollzogen werden.
- Wie bereits mehrfach von der GPK angemerkt ist die Verordnung zum Beschaffungswesen der Gemeinde Ettingen in der aktuellen Version strikte einzuhalten. Dies gilt auch für sämtlichen Nachträge.
- Für sämtliche im Rahmen der Sanierung eingesetzten Handwerker sind die relevanten Unterlagen vorzuhalten.
- Das Protokoll der Schlussabnahme ist durch die Gemeinde aufzubewahren.
- Es sollte geprüft werden, ob die in der Sondervorlage vom 12. Dezember 2018 aufgeführten Förderbeiträge in der Höhe von CHF 70’000 noch nachträglich vereinnahmt werden können.

4 ZUSAMMENFASSUNG

Die GPK prüfte im 2022/2023 die unten aufgeführten Geschäfte und kam zu folgenden Schlüssen:

Thema 1 / Prüfung IT

Die GPK hat zahlreiche Anmerkungen organisatorischer, konzeptioneller und technischer Natur identifiziert, welche holistisch durch die Gemeinde Ettingen adressiert werden sollten. Dabei sollte insbesondere der präventive und detektive Schutz vor Cyber Angriffen priorisiert adressiert werden. Gemäss den uns vorliegenden Informationen sind die Sachverhalte der Gemeinde Ettingen bereits bekannt und werden nachhaltig adressiert.

Thema 2 / Bauabrechnung Schulhaus «Hintere Matten»: Unterhalts- und Sanierungsarbeiten Trakt 4

Die GPK weist nochmals darauf hin, dass die Verordnung zum Beschaffungswesen der Gemeinde Ettingen strikte einzuhalten ist. Dabei sind sämtliche Dokumente aufzubewahren, die für den Nachvollzug relevanter Entscheidungen notwendig sind. Nachträge sind nach Möglichkeit zu verhindern, und bei ausgewiesenem Bedarf, umfassend zu begründen und entsprechend zu dokumentieren. Zudem sind sämtliche Schlussabnahmen zu dokumentieren, zu unterzeichnen und aufzubewahren. Es sollte geprüft werden, ob die nicht eingeforderten Förderbeiträge nachträglich vereinnahmt werden können.

Die GPK dankt den involvierten Gemeinderätinnen und Gemeinderäten, den Kommissions- und Behördenmitgliedern sowie der Gemeindeverwaltung für die konstruktive Zusammenarbeit in der vergangenen Berichtsperiode.

Wir haben die diesem Bericht aufgeführten Feststellungen und Empfehlungen mit den Betroffenen diskutiert. Wir erachten es als zweckmässig, diesen Bericht – ohne Anhänge – in geeigneter Weise zu veröffentlichen.

Ettingen, 09. Juni 2023

Für die GPK Ettingen

Dieter Baumann

Ralf Hofstetter