KANTON AARGAU

REGIERUNGSRAT

24. April 2024

BOTSCHAFT AN DEN GROSSEN RAT **24.135**

Informationssicherheit; Umsetzung Massnahmen Informatik Aargau; Verpflichtungskredit

Inhaltsverzeichnis

Sehr geehrte Frau Präsidentin
Sehr geehrte Damen und Herren

Wir unterbreiten Ihnen die Botschaft Informationssicherheit; Umsetzung Massnahmen Informatik Aargau; Verpflichtungskredit zur Beschlussfassung und erstatten Ihnen dazu folgenden Bericht.

Zusammenfassung

Der rasante Wandel hin zu einer Informationsgesellschaft und die Digitalisierung bergen ungeahnte Chancen, jedoch auch erhebliche Risiken. Die zunehmende Abhängigkeit von Informations- und Kommunikationstechnologie (IKT) macht auch den Kanton Aargau verwundbarer gegenüber Ausfällen, Störungen und Missbräuchen dieser Technologien. Die Angriffe auf Verwaltungssysteme haben stark zugenommen. Um dieser Situation wirksam entgegentreten zu können, ist eine angemessene und effektive Informationssicherheit unerlässlich. Sie umfasst die Gesamtheit aller Anforderungen und Massnahmen, mit denen die Vertraulichkeit, die Verfügbarkeit, die Integrität und die Nachvollziehbarkeit von Informationen gewährleistet werden kann.

In Anbetracht dieser Herausforderungen sind strategische Zielsetzungen für den weiteren Ausbau und die nachhaltige Sicherheit im Kanton Aargau von entscheidender Bedeutung. Der Fokus des Regierungsrats liegt auf der Umsetzung eines abgestuften Plans bis 2026, um dem Minimalstandard an Informations- und Kommunikationstechnologie (IKT-Minimalstandard) des Bundes zu entsprechen und langfristig einen Reifegrad anzustreben, der die Voraussetzung für eine ISO/IEC 27001 Zertifizierung schafft.

Das anvisierte Zielniveau (Kapitel 2) sowie die dazu notwendigen Massnahmen (Kapitel 3) für die gesamte kantonale Verwaltung und die Gerichte Kanton Aargau werden in einem neuen Entwicklungsschwerpunkt 'Informationssicherheit' im Aufgaben- und Finanzplan (AFP) 2025–2028 (Aufgabenbereich 435 'Informatik') aufgenommen. Dieser setzt sich aus verschiedenen Initiativen zusammen, welche über alle Organisationseinheiten ihre Wirkung entfalten sollen. Es handelt sich um organisatorische und technische Massnahmen, welche die Basis für die langfristige Entwicklung der Informationssicherheit im Kanton Aargau bilden. Die Fortschritte werden im jährlichen Rechenschaftsbericht des Chief Information Security Officer (CISO) an die Generalsekretärenkonferenz (GSK) transparent dargestellt. Angesichts der komplexen Lage und der langfristigen Natur der Sicherheitsaufgaben ist eine kontinuierliche Anpassung und Weiterentwicklung der Strategien und Massnahmen unerlässlich.

Um den IKT-Minimalstandard des Bundes und das angestrebte Sicherheitsniveau erreichen zu können, sind substanzielle Investitionen in technische und organisatorische Massnahmen zu tätigen sowie in personeller Hinsicht zusätzliche Stellen zu schaffen. Neben der angemessenen Verstärkung der Fachstelle für Informationssicherheit bedarf es zusätzlicher Ressourcen für die mit ihr eng verbundenen Fachdisziplinen innerhalb der Aargau (IT AG) des Departements Finanzen und Ressourcen, welche mit der Wahrnehmung von informationssicherheitsspezifischen Aufgaben (Cybersecurity-Engineering; sicherheitsrelevante Aufgaben im Rahmen von Entwicklung, Bereitstellung und Betrieb von Applikationen, Plattformen und Infrastrukturen) betraut sind. Die personellen Ressourcen sind im AFP 2025–2028 eingeplant.

Für diejenigen Massnahmen, welche gemäss § 24 Abs. 1 Gesetz über die wirkungsorientierte Steuerung von Aufgaben und Finanzen (GAF) einen Verpflichtungskredit in der Kompetenz des Grossen Rats bedingen, wird dem Grossen Rat die vorliegende Botschaft unterbreitet. Es wird Antrag gestellt, dass für das Vorhaben "Massnahmen Informationssicherheit" ein Verpflichtungskredit für einen einmaligen Bruttoaufwand von 7,2 Millionen Franken und für einen jährlich wiederkehrenden Bruttoaufwand von 4,0 Millionen Franken beschlossen werden.

1. Ausgangslage

Im Jahr 2022 wurde in der Schweiz ein starker Anstieg von Cyber-Security Vorfällen beobachtet. Dieser Trend hat sich im Jahr 2023 fortgesetzt[1]. Inzwischen hat sich die Cyber-Crime-Industrie in spezialisierten Fachbereichen organisiert und steigerte den Jahresumsatz weltweit auf über 1,5 Billionen Franken. Der Schaden in der Schweiz beläuft sich im Jahr 2023 auf über 700 Millionen Franken[2]. Nach wie vor am erfolgreichsten sind Attacken via Phishing E-Mails[3]. Zunehmend wird seitens Angreifer auch künstliche Intelligenz (KI) eingesetzt. Die Geschwindigkeit und Diversität der Angriffe nehmen zu. Entsprechend ist die Bedrohungslandschaft im Cyberbereich für den Kanton Aargau genauso wie für alle anderen Industriezweige und Verwaltungsebenen zunehmend dynamisch und grundsätzlich vielschichtiger geworden.

Die Vorteile der schnell fortschreitenden Digitalisierung von Wirtschaft und Gesellschaft bringen mit immer ausgefeilteren Cyberattacken auch mehr Angriffsflächen und neue Angriffsvektoren mit sich, entsprechend steigen auch die Anforderungen an die Cyber-Sicherheitssysteme. Die unzureichende Sicherung von Netzwerken, Programmen und Daten kann zu unautorisierter Nutzung von vertraulichen Informationen führen, sowohl durch Mitarbeitende als auch vonseiten krimineller Dritter ("Hacker"). Letztere versuchen tagtäglich, Systeme zu kompromittieren, um mittels Exfiltration von Daten Lösegeldforderungen an die Opfer stellen zu können. Der Datenabfluss bei Xplain[4] zeigt, dass diese Bedrohungen eine ernstzunehmende Realität sind und es nur eine Frage der Zeit ist, bis ein Angriff bei der Kantonalen Verwaltung zu erheblichen Beeinträchtigungen führen wird[5].

Die fortschreitende Nutzung von Cloud-Services und hybride Arbeitsmethoden zwingen zum beschleunigten Ausbau von Sicherheitsmassnahmen. Gemäss Gartner Inc. werden im Jahr 2024 die Ausgaben für Sicherheit und Risikomanagement weltweit um über 14 % steigen.[6]

Im Kanton Aargau ist das Informationssicherheits-Management-System, welches sich aus Elementen der Aufbauorganisation und Prozessen und Systemen (Ablauforganisation) zusammensetzt, eine gemeinsame Aufgabe der Departemente, der Staatskanzlei und der Gerichte Kanton Aargau, welche durch den CISO[7] koordiniert wird. Übergeordnet verantwortlich ist die Generalsekretärenkonferenz (GSK), welche die Informationssicherheit im Rahmen der Richtlinie zur Führung und Steuerung der Informatik im Kanton Aargau steuert. Im jährlichen Rechenschaftsbericht informiert der CISO die GSK über den Status und den Fortschritt bei der Massnahmenumsetzung.

Seit 2013 wird "Informationssicherheit" im Kanton Aargau mit der damals verabschiedeten Informationssicherheitsstrategie als eigenständige Disziplin geführt. Die ergriffenen Massnahmen haben sich seither weiterentwickelt, um den stetig steigenden Risiken zu begegnen[8]. Entsprechend wurde das Security Team (CISO Office) in den vergangenen Jahren von 1 auf knapp 3 Vollzeitstellen aufgebaut, um den Umweltbedingungen Rechnung tragen zu können. Neben dem Personalaufbau wurden

---

[1] Gemäss Allianz Risk Barometer 2024 erneut um 50% / "Ransomware claims activity was up by more than 50% year-on-year in 2023" (Quelle: https://commercial.allianz.com/news-and-insights/expert-risk-articles/allianz-risk-barometer-2024-cyber-incidents.html)
Im gleichen Bericht wird auch auf die Zunahme von KI sowie die unablässige Früh-Detektion von Ereignissen hingewiesen.

[2] Zahlen stammen von 2021. Eine aktuelle aber nicht zu verifizierende Quelle "Comparitech" spricht sogar von über 1,5 Milliarden Franken für die Schweiz: https://www.comparitech.com/blog/vpn-privacy/cybercrime-cost/

[3] Eine Phishing-Mail ist eine betrügerische E-Mail, die vorgibt, von einer vertrauenswürdigen Quelle zu stammen, um persönliche Daten wie Passwörter oder Kreditkarteninformationen zu stehlen, indem sie den Empfänger dazu verleitet, auf gefälschte Links zu klicken oder sensible Informationen preiszugeben.

[4] Datenabfluss bei einem IT-Lieferanten der kantonalen Verwaltung

[5] https://www.allianz.com/content/dam/onemarketing/azcom/Allianz_com/press/document/Allianz-Risk-Barometer-2023.pdf

[6] Gartner: https://de.wikipedia.org/wiki/Gartner_Inc.

(nur in englischer Sprache) https://www.gartner.com/en/newsroom/press-releases/2023-09-28-gartner-forecasts-global-security-and-risk-management-spending-to-grow-14-percent-in-2024

[7] Der Chief Information Security Officer ist im Kanton Aargau organisatorisch im Departement Finanzen und Ressourcen, Abteilung Informatik Aargau, verortet. Er ist verantwortlich für die Schaffung, Pflege und Weiterentwicklung der Grundlagen, Instrumente und Prozesse zur Informationssicherheit, insbesondere durch ein Informationssicherheits-Managementsystem.

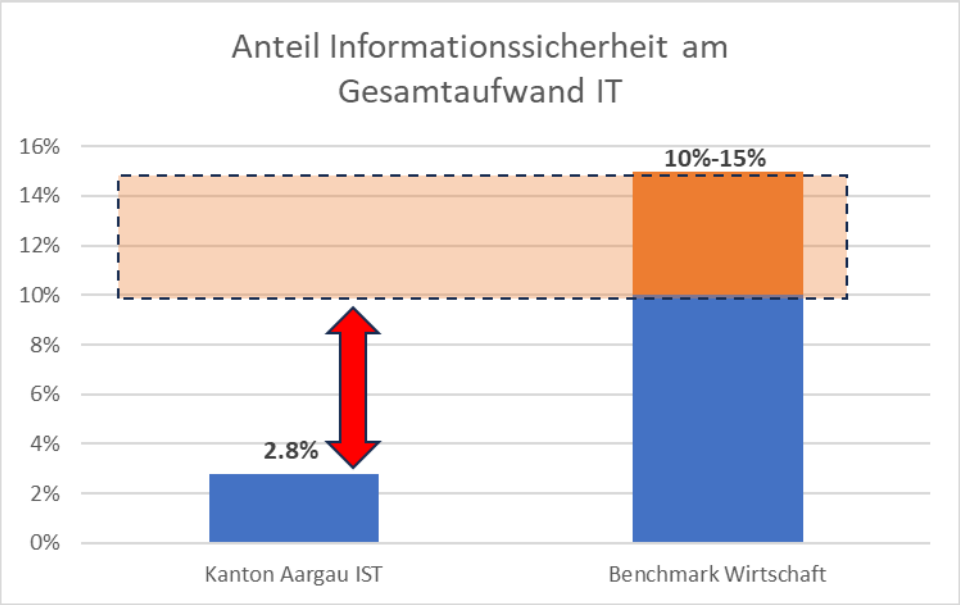
[8] Seit 2019 führt die Informatik Aargau die Informationssicherheit und ihr Teilgebiet Cybersicherheit als grösstes Risiko im Aufgaben- und Finanzplan.

auch Investitionen in die Systeme zur präventiven und prädiktiven Erkennung von Cyberbedrohungen sowie in die klassischen Schutzsysteme getätigt.

Bis anhin vermochten die getätigten Informationssicherheitsmassnahmen den Kanton Aargau zu schützen, so dass er bisher von grossen Schäden verschont blieb. Mit der fortschreitenden Entwicklung zu einer Informationsgesellschaft und der stark wachsenden Cyber-Crime-Industrie wurden die Bedrohungen für Informationen und IKT-Mittel aber komplexer und dynamischer, weshalb ihnen inskünftig noch integraler und professioneller begegnet werden muss. Der systematische Auf- und Ausbau von Informationssicherheitsmassnahmen auf technischer und organisatorischer Stufe muss weiter vorangetrieben werden.

Trotz den bisherigen Investitionen in Personal und Technik zeigt ein Quervergleich, dass die kantonale Verwaltung derzeit mit einem jährlichen Aufwand für Informationssicherheit von knapp 3 % des gesamten Informatik-Budgets mit dem privatwirtschaftlichen Vergleichswert (10–15 %[9]) um den Faktor 3–5 weniger in die Informationssicherheit investiert:

Abbildung 1: Prozentualer Anteil der Informationssicherheit an den IT-Ausgaben (Status quo; 2023), mit Benchmark



Es ist angezeigt, die notwendigen Massnahmen zur Gewährleistung der Informationssicherheit in einem neuen Entwicklungsschwerpunkt der Informatik Aargau (IT AG) zu orchestrieren. Dies mit dem Ziel, das gesamte Informationssicherheits-Managementsystem unter Einbezug der Departemente, der Staatskanzlei und der Gerichte Kanton Aargau auf ein der Situation angemessenes Niveau zu erhöhen, damit die Informationssicherheit und der Datenschutz in der kantonalen Verwaltung nachhaltig sichergestellt werden können.

2. Handlungsbedarf

Den zunehmenden Herausforderungen im Bereich der Informationssicherheit und des Datenschutzes, welche sich angesichts der fortschreitenden Digitalisierung und der steigenden Bedrohungen durch Cyberangriffe ergeben, ist alternativlos etwas entgegenzusetzen, wenn die Systeme und Daten der kantonalen Verwaltung auch künftig angemessen geschützt sein sollen. Nicht zuletzt haben

[9] Siehe Zusammenfassung aus dem Abschnitt "Cybersecurity and Risk Management Growth in 2024" (Englisch) auf Webseite https://www.splunk.com/en_us/blog/learn/it-tech-spending.html , welcher auf den "2023 Security Budget Benchmark Report" by IANS Research and Artico Search verweist. Der umfassende IANS Bericht von 2023 (in Englisch) kann bei der Informatik Aargau angefragt werden.

der Vorfall bei Xplain sowie nachweisbare Artefakte von versuchten Angriffen auf Systeme der kantonalen Verwaltung die reale Gefahr von Datenlecks und Angriffen auf die IT-Infrastruktur unterstrichen.

Für den angemessenen Schutz müssen durch den Kanton Aargau einerseits die Vorgaben des Bundes im Rahmen des Bundesgesetzes über die Informationssicherheit beim Bund (Informationssicherheitsgesetz, ISG) eingehalten werden[10]. Der Bund hat dazu einen entsprechenden Minimalstandard verfasst[11], welcher als Richtschnur für die IKT-Resilienz dient. Andererseits bieten international anerkannte, branchenübliche Standards (zum Beispiel ISO/IEC 27001[12] oder NIST Cybersecurity Framework[13]) eine gute Referenz zur Definition von Massnahmen zur Sicherstellung der Informationssicherheit und dem Datenschutz. Eine entsprechende Kontrollgrösse sind die im Zusammenhang mit den technischen und organisatorischen Massnahmen getätigten Ausgaben im Verhältnis zu den gesamten IT-Ausgaben. Hierzu bestehen verschiedene Referenzwerte und Benchmarks, die in der Fachpresse und -literatur veröffentlicht wurden und deren Bandbreiten teilweise erheblich variieren. Allen Benchmarks gleich ist der Umstand, dass die aktuell im Kanton Aargau getätigten Ausgaben für die Informationssicherheit ein Mehrfaches unter diesen Referenzwerten liegen und so die Notwendigkeit für zusätzliche Investitionen – abgestimmt auf das angestrebte Sicherheitsniveau – offensichtlich und angemessen ist (vgl. Abbildung 1). Welche notwendigen Massnahmen und welche Investitionen damit verbunden sind, ergibt sich aus dem Minimalstandard, welcher der Kanton Aargau als Minimalziel definiert hat. Dieser IKT-Minimalstandard richtet sich zwar insbesondere an die Betreiber von kritischen Infrastrukturen, er ist aber auch für jedes Unternehmen und die öffentliche Hand auf allen Ebenen zur eigentlichen Richtschnur und zum gemeinsamen Nenner in Bezug auf das anzustrebende Sicherheitsniveau geworden. Um diesem Mindeststandard nachkommen zu können, sind substanzielle Investitionen in technische und organisatorische Massnahmen zu tätigen.

Die geplante Intensivierung des Dispositivs im Bereich der Informations- und Cybersicherheit unterstreicht dann auch die klare Strategie zur diesbezüglichen Stärkung in der kantonalen Verwaltung. Die durch den CISO und die IT AG vorgeschlagenen Massnahmen bilden dabei einen ganzheitlichen Ansatz, welcher in allen Verwaltungseinheiten und den Justizbehörden zum Einsatz kommen soll. Zwar sind von diesen Massnahmen nicht alle gleichermassen betroffen, der zusätzliche Sicherheitsgewinn ist aber ein kollektiver Mehrwert.

Die Erhebung durch den CISO (Stand November 2023) unterstreicht den Optimierungsbedarf in verschiedenen Bereichen des Reifegradmodells des IKT-Minimalstandards zur Erreichung des vom Bund geforderten Sicherheitsniveaus.

2.1 Strategischer Ausblick

Der weitere Aufbau, die Umsetzung und Aufrechterhaltung der Informationssicherheit im Kanton Aargau ist eine langfristige Aufgabe. Es braucht eine Vielzahl von technischen und organisatorischen

[10] https://www.fedlex.admin.ch/eli/fga/2020/2696/de; Artikel 3: Die Kantone müssen gleichwertige Informationssicherheit gewährleisten, wenn sie auf Informationen und Informatikmittel des Bundes zugreifen.

[11] Der IKT-Minimalstandard dient zur Verbesserung der IKT-Resilienz, speziell bei Betreibern kritischer Infrastrukturen, ist jedoch grundsätzlich für jede Organisation anwendbar. Er besteht aus Empfehlungen und Richtlinien in drei Teilen: Grundlagen mit Hintergrundinformationen zur IKT-Sicherheit, einem Framework mit 106 konkreten Massnahmen gegliedert in die Bereiche „Identifizieren", „Schützen", „Detektieren", „Reagieren" und „Wiederherstellen", und einem Self-Assessment mit Bewertungstool für Organisationen zur Selbstprüfung des Umsetzungsstands der Massnahmen. Ziel ist es, die Resilienz gegenüber Cyber-Bedrohungen durch einen risikobasierten Ansatz und angepasste Schutzniveaus zu verbessern.

[12] ISO/IEC 27001 ist ein international anerkannter Standard für Informationssicherheits-Managementsysteme (ISMS), der Anforderungen für die Etablierung, Implementierung, Aufrechterhaltung und kontinuierliche Verbesserung eines ISMS definiert. Der Standard legt den Schwerpunkt auf die Bewertung und Behandlung von Informationssicherheitsrisiken im Kontext der spezifischen Risikoumgebung einer Organisation.

[13] Das NIST Cybersecurity Framework ist ein Leitfaden, der von der US-amerikanischen National Institute of Standards and Technology entwickelt wurde. Es bietet Organisationen aller Branchen eine Struktur für die Verbesserung ihrer Cybersecurity durch Identifizierung, Schutz, Erkennung, Reaktion und Wiederherstellung von Informationssystemen vor Cyberbedrohungen.

Massnahmen im Verantwortungsbereich der IT AG wie auch bei den Departementen, der Staatskanzlei, dem Parlamentsdienst und den Gerichten Kanton Aargau, um die Resilienz nachhaltig zu erhöhen und auf diesem Niveau halten zu können.

Die Planung sieht ein abgestuftes Vorgehen vor. Zunächst soll bis ca. 2026 der IKT-Minimalstandard des Bundes erreicht werden. Als strategische Zielsetzung wird bis 2028 ein Reifegrad angestrebt, welcher die Voraussetzung für eine Zertifizierung gemäss ISO/IEC 27001 bildet.

Zur Erreichung des Reifegrads sind eine Reihe von in Initiativen zusammengefassten, priorisierten Massnahmen in verschiedenen Teildisziplinen des Informationssicherheits-Managements geplant.

Es handelt sich dabei um technische und organisatorische Massnahmen, welche auf allen Verwaltungsstufen umgesetzt werden müssen. Aus Gründen der Vertraulichkeit werden die Details zu den Massnahmen in der Botschaft nicht detailliert erläutert, weil damit auch identifizierte Schwachstellen offengelegt und somit potenziellen Angreifern offenbart würden (Details im vertraulichen Bericht zuhanden der grossrätlichen Fachkommission). Die Gesamtkoordination dieser Massnahmen erfolgt durch den CISO, die departementale Koordination und Umsetzung erfolgt durch die informationssicherheitsbeauftragten Personen (ISBP) der Departemente, der Staatskanzlei und der Gerichte Kanton Aargau. Die Umsetzungsplanung erfolgt iterativ und orientiert sich periodisch neu anhand der aktualisierten Bedrohungsanalyse (jährlich) und dem erreichten Fortschritt der Massnahmen. Die Berichterstattung der Fortschritte erfolgt im Rahmen des jährlichen Rechenschaftsberichts des CISO an die GSK.

Als übergeordnetes und zentrales Element der strategischen Zielsetzungen ist ab dem AFP 2025–2028 ein Entwicklungsschwerpunkt 'Informationssicherheit' im Aufgabenbereich der IT AG (Aufgabenbereich 435 'Informatik') vorgesehen (vgl. Kapitel 3).

3. Umsetzung

Die notwendigen Massnahmen werden im Aufgabenbereich '435 Informatik' in einem neuen Entwicklungsschwerpunkt 'Informationssicherheit' im AFP 2025–2028 gebündelt. Dieser setzt sich aus verschiedenen Initiativen zusammen, welche über alle Organisationseinheiten ihre Wirkung entfalten. Es handelt sich um organisatorische und technische Massnahmen, die das Rahmenwerk und die Basis für die langfristige Entwicklung der Informationssicherheit im Kanton Aargau bilden. Die notwendigen Massnahmen sind folgenden Initiativen zuzuordnen:

1. Zero-Trust (Sicherheitskonzept zur Autorisierung von Akteuren und Systemen)
2. Security Operations Center (SOC; Einheit zur Überwachung, Analyse und Schutz vor Cyberbedrohungen)
3. Datenklassifizierung und Datenkategorisierung
4. IAM NextGen (Identitäts- & Zugriffsverwaltung)
5. DevSecOps (Sicherheitsorientierte Entwicklung & IT-Betriebsführung)
6. ISO/IEC 27001 Strategie
7. Security Awareness

Detaillierte Informationen zu den Massnahmen werden in einem vertraulichen Bericht zuhanden der Fachkommission des Grossen Rats erläutert. Die personellen und finanziellen Auswirkungen, welche mit diesen Initiativen einhergehen, werden im Kapitel 5 und Kapitel 7.1 detailliert dargestellt und erläutert.

4. Rechtsgrundlagen

Der Kanton betreibt seit Jahrzehnten Informatik und damit in einem engen Konnex stehend auch Informatiksicherheit. Die gesetzliche Grundlage basiert auf § 5 Abs. 1 des Gesetzes über die Organisation des Regierungsrates und der kantonalen Verwaltung (Organisationsgesetz), wonach der Regierungsrat im Rahmen dieses Gesetzes eine zweckmässige Verwaltungsorganisation schafft, soweit diese nicht durch andere gesetzliche Bestimmungen festgelegt ist. Informatik ist eine Querschnittsaufgabe, die mit allen gesetzlichen Aufgaben des Kantons in Zusammenhang steht. Denn ohne den entsprechenden Support können alle anderen staatlichen Aufgaben nicht erfüllt werden. Die Informationssicherheit wurde bisher als Informatiksicherheit verstanden und fiel deshalb unter dieselbe Rechtsgrundlage wie die Informatik. Die neueste Entwicklung zeigt, dass Informationssicherheit über die Informatiksicherheit hinausgeht. Aus diesem Grund werden diesbezüglich auch neue Rechtsgrundlagen geschaffen (vgl. Anhörungsvorlage Gesetz über die Informationssicherheit [InfoSiG] vom 24. April 2024). Die Sofortmassnahmen sind jedoch Massnahmen zur Verbesserung der Informatiksicherheit und fallen folglich unter § 5 Abs. 1 Organisationsgesetz.

5. Finanzielle Auswirkungen

5.1 Einmaliger Aufwand

Für die Umsetzung der Massnahmen Informationssicherheit, bestehend aus den sieben Initiativen, werden folgende finanzielle Mittel benötigt:

Tabelle 1: Einmaliger Aufwand

Einmaliger Aufwand		
Vorleistungen 2024 (Konzept, Studie & Submission für Teilprojekt SOC)		Fr. 340'000.–
Teilprojekt Zero Trust (Externe Unterstützung Evaluation & Implementation)		Fr. 560'000.–
Teilprojekt SOC (Server-Hardware, Sensoren)		Fr. 150'000.–
Teilprojekt Datenklassifikation (Externe Unterstützung Analyse & Detailkonzepte)		Fr. 480'000.–
Teilprojekt IAM NextGen		Fr. 2'650'000.–
Projektleitung	Fr. 450'000.–	
Externe Fachunterstützung (Konzept, Detailstudie, Systemarchitektur, Einführungskonzept)	Fr. 400'000.–	
Externe Fachunterstützung (Systementwicklung, Installation, Migration, Rückbau)	Fr. 1'800'000.–	
Teilprojekt ISO Zertifizierung		Fr. 1'850'000.–
Projektleitung	Fr. 700'000.–	
Externe Fachunterstützung (Entwicklung Risk Assessment, Auditprogramm etc.)	Fr. 700'000.–	
Zertifizierungskosten	Fr. 250'000.–	
Anpassungen Swiss GRC Tool (Dokumentationsmanagement)	Fr. 200'000.–	
Reserve für Unvorhergesehenes (20 %)		Fr. 1'138'000.–
Total einmaliger Aufwand (erforderlicher Verpflichtungskredit)		**Fr. 7'168'000.–**

Die einmaligen Aufwände beinhalten vorwiegend Projektleistungen (Leitung, Entwicklung und Umsetzung durch externe Fachexperten und zu einem kleinen Anteil Neuanschaffungen [Server, Tool-Erweiterungen]). Aufgrund der Dringlichkeit wurden konzeptuelle Arbeiten beim Teilprojekt SOC bereits im Jahr 2023 gestartet und der aufgelaufene Aufwand des Jahrs 2024 wird als Vorleistung ausgewiesen. Zudem wird aufgrund von Planungsrisiken bei IT-Projekten eine Reserve für Unvorhergesehenes von 20 % addiert. Diese ist bewusst hoch angesetzt und begründet sich durch mehrere Faktoren: Einerseits ist am IT-Markt mit Unsicherheiten und hohen Kostensteigerungen zu rechnen, und die benötigten Submissionen müssen erst noch geplant werden. Andererseits macht die Komplexität und die Neuartigkeit der Vorhaben die Aufwandsschätzung vor Projektbeginn schwierig. Es ist damit zu rechnen, dass sich der Gesamtaufwand erst mit der Konzeptphase der Teilprojekte eingrenzen lässt.

5.2 Wiederkehrender Aufwand

Der jährlich wiederkehrende Aufwand betrifft einerseits Lizenz- und Software-Wartungskosten für neue Sicherheits-Anwendungen und andererseits die Betriebsunterstützung durch Dienstleister.

Tabelle 2: Jährlich wiederkehrender Aufwand

Jährlich wiederkehrender Aufwand		
Teilprojekt Zero Trust (Tool-Lizenzen)		Fr. 1'450'000.–
Teilprojekt SOC		Fr. 1'170'000.–
Tool-Lizenzen	Fr. 650'000.–	
Externe Betriebsdienstleistungen (24/7 Support)	Fr. 520'000.–	
Teilprojekt DevSecOps (Tool-Lizenzen)		Fr. 300'000.–
Teilprojekt ISO-Zertifizierung (Externe Dienstleistung Lieferanten-Audits)		Fr. 250'000.–
Teilprojekt Awareness (Plattform-Lizenzen)		Fr. 100'000.–
Reserve für Unvorhergesehenes (20 %)		Fr. 654'000.–
Total wiederkehrender Aufwand (erforderlicher Verpflichtungskredit)		**Fr. 3'924'000.–**

Der wiederkehrende Aufwand ab 2027 beträgt rund 3,9 Millionen Franken pro Jahr. Auch hier begründet sich die bewusst hoch angesetzte Reserve von 20 % mit den Unsicherheiten im IT-Markt und bei der Planung (vgl. Kapitel 5.1 Einmaliger Aufwand).

5.3 Folgeaufwand

Der einmalige Aufwand von 7,2 Millionen Franken wird mit einem jährlichen Betrag rund 2,4 Millionen Franken über drei Jahre (2029–2031) abgeschrieben:

Tabelle 3: Folgeaufwand (Abschreibungen)

Anlagekategorie	Nutzungsdauer	Abschreibung total	Abschreibung pro Jahr	Geplanter Nutzungsbeginn
Informatik	3 Jahre	Fr. 7'168'000.–	Fr. 2'389'000.–	1. Januar 2029

5.4 Verhältnis zur mittel- und langfristigen Planung

Das Vorhaben hat für die Informationssicherheit der kantonalen Verwaltung eine hohe Bedeutung; es wird deshalb im Aufgaben- und Finanzplan (AFP) als Entwicklungsschwerpunkt im Aufgabenbereich 435 'Informatik' aufgenommen.

5.4.1 Aufgaben- und Finanzplan (AFP) 2024–2027

Die Aufwände sind als zusätzlicher Bedarf zu betrachten, wobei ein Anteil von rund 3,9 Millionen Franken wiederkehrender Natur ist und somit auch nach dem Jahr 2028 anfallen wird (Lizenzen & Systembetrieb). Aufgrund der Dringlichkeit werden einige der Themen bereits im Jahr 2024 lanciert, unter anderem eine Konzeptstudie und die Submissionsplanung für das Teilprojekt SOC.

Die Aufwände für dieses Vorhaben waren im AFP 2024–2027 im Aufgabenbereich 435 'Informatik' noch nicht eingestellt:

Tabelle 4: AFP 2024–2027

in Tausend Franken	Budget 2024	Plan 2025	Plan 2026	Plan 2027	Plan 2028	2029ff.	Total 2024–2029
AFP 2024–2027	**0**	**0**	**0**	**0**	**0**	**0**	**0**
Globalbudget (FB 150)	0	0	0	0	0	0	0
Investitionsrechnung (FB 350)	0	0	0	0	0	0	0
Finanzbedarf gemäss aktuellem Projektstand	**340**	**3'492**	**4'224**	**4'980**	**5'568**	**3'924**	**18'604**
Globalbudget (FB 150)	0	1'764	2'844	2'904	3'924	3'924	11'436
Investitionsrechnung (FB 350)	340	1'728	1'380	2'076	1'644	0	7'168
Abweichung	**340**	**3'492**	**4'224**	**4'980**	**5'568**	**3'924**	**18'604**

in Tausend Franken	Budget 2024	Plan 2025	Plan 2026	Plan 2027	Plan 2028	2029ff.	Total 2024–2029
Globalbudget (FB 150)	0	1'764	2'844	2'904	3'924	3'924	11'436
Investitionsrechnung (FB 350)	340	1'728	1'380	2'076	1'644	0	7'168

Anmerkung: (+) Aufwand/Verschlechterung; (-) Ertrag/Verbesserung,

Der Finanzbedarf wird im AFP 2025–2028 gemäss effektiver Planung eingestellt. Der Mehrbedarf im Budget 2024 wird innerhalb des Departements Finanzen und Ressourcen kompensiert.

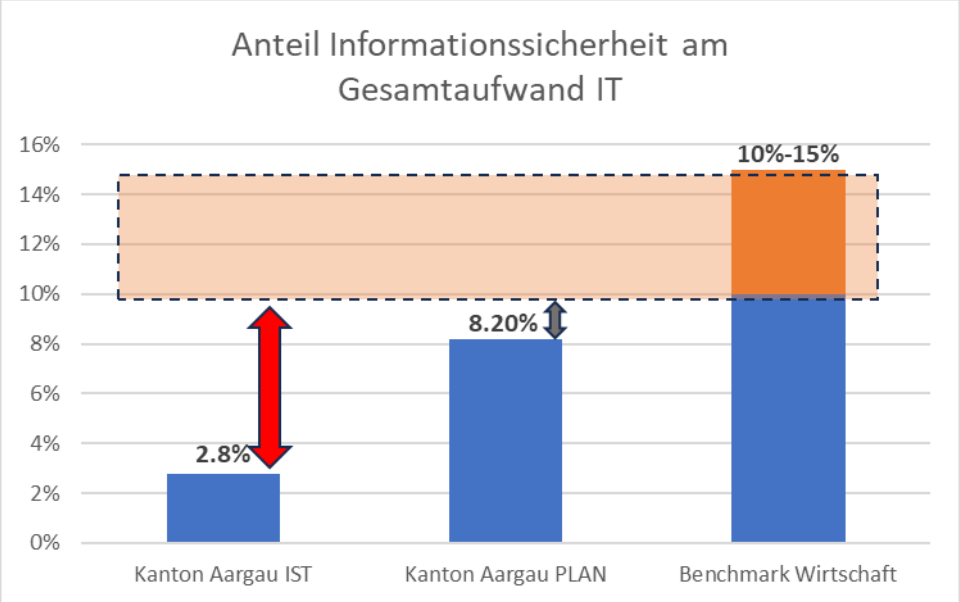
5.5 Verpflichtungskredit

Gemäss vorstehendem Kostenvoranschlag (vgl. Kap. 5.1) ist für das Vorhaben "Massnahmen Informationssicherheit" die Bewilligung eines Verpflichtungskredits nach § 24 Abs. 1 GAF erforderlich. Der Verpflichtungskredit ist als Rahmenkredit ausgestaltet (§ 25 Abs. 1 GAF) und wird als gemischter Verpflichtungskredit sowohl im Globalbudget als auch in der Investitionsrechnung geführt. Mit einer Kreditkompetenzsumme von Fr. 46'408'000.– (einmaliger Bruttoaufwand zuzüglich dem mit Faktor 10 multiplizierten neuen jährlich wiederkehrenden Bruttoaufwand) liegt die Zuständigkeit für die Bewilligung beim Grossen Rat (§ 28 Abs. 5 GAF).

5.6 Kosten-Nutzen-Beurteilung

Die untenstehende Abbildung 2 veranschaulicht den mutmasslichen Effekt der zu ergreifenden Massnahmen auf die kantonale Verwaltung. Mit Blick auf den prozentualen Anteil der Informationssicherheit an den gesamten kantonalen IT-Ausgaben zeigt sich, dass der Benchmark-Bereich der Privatwirtschaft von 10–15 % auch mit diesen Massnahmen noch nicht erreicht wird (vgl. Abbildung 2):

Abbildung 2: Prozentualer Anteil Informationssicherheit Kanton Aargau nach Umsetzung Entwicklungsschwerpunkt (Schätzung, ab 2025)



Insofern kommen die IT AG und der CISO zum Schluss, dass die Initiativen aus der finanziellen Perspektive als angemessen und wirtschaftlich sinnvoll zu beurteilen sind. Zweifellos führen sie auch zur

Verbesserung der Informationssicherheit und des Datenschutzes im Kanton Aargau – und sind daher auch diesbezüglich "angemessen".

Die Umsetzung der Initiativen sind anspruchsvolle technische und organisatorische Projekte. Es gilt daher, diese umsichtig und unter Einbezug aller Stakeholder zu planen und umzusetzen. Die Fortschrittsmessung erfolgt im Rahmen des jährlichen Reportings zur Informationssicherheit durch den CISO respektive im Rahmen des Portfolio-Managements – bei beidem handelt es sich um Steuerungsinstrumente der GSK.

Insgesamt demonstriert der Entwicklungsschwerpunkt die klare Absicht, die Informationssicherheit im Kanton Aargau vor dem Hintergrund der veränderten Umweltbedingungen proaktiv und umfassend zu definieren und umzusetzen sowie auch in dieser Disziplin Standards zu setzen.

6. Ausgabenreferendum

Gemäss § 63 Abs. 1 lit. d der Verfassung des Kantons Aargau unterstehen Beschlüsse des Grossen Rats über neue einmalige Ausgaben von mehr als 5 Millionen Franken oder über neue jährlich wiederkehrende Ausgaben über Fr. 500'000.– der fakultativen Volksabstimmung respektive dem Ausgabenreferendum. Die Berechnung des Umfangs des Vorhabens, welches dem Ausgabenreferendum unterliegt, erfolgt nach dem Nettoprinzip. Massgebend ist folglich der Betrag der Nettobelastung des Kantons nach Abzug der im Zeitpunkt der Beschlussfassung feststehenden Leistungen Dritter. Fallen bei einem Vorhaben einmalige und wiederkehrende Ausgaben an, werden die wiederkehrenden mit dem Faktor 10 multipliziert und zu den einmaligen Ausgaben gezählt (§ 31 Abs. 2 GAF).

Gemäss § 30 Abs. 2 GAF gilt eine Ausgabe als neu, wenn in Bezug auf den damit verfolgten Zweck, den Umfang, den Zeitpunkt ihrer Vornahme oder andere wesentliche Modalitäten eine verhältnismässig grosse Handlungsfreiheit besteht.

Im vorliegenden Fall wird die betragsmässige Limite für das Ausgabenreferendum überschritten. Hingegen handelt es sich nicht um eine neue Ausgabe. Art. 3 Abs. 1 ISG hält fest, dass die Bestimmungen über klassifizierte Informationen und über die Sicherheit beim Einsatz von Informatikmitteln auch für die Kantone gelten, soweit sie klassifizierte Informationen des Bundes bearbeiten beziehungsweise auf Informatikmittel des Bundes zugreifen. Mit dieser Regelung gibt der Bund den Kantonen einen Mindestsicherheitsstandard vor. Der Bund hat nicht rechtsetzerisch festgehalten, wie dieser Standard einzuhalten ist. Aber er hat mit den von ihm als Empfehlungen herausgegebenen "Minimalstandard zur Verbesserung der IKT-Resilienz" (IKT-Minimalstandard, Version Mai 2023; vgl. Kapitel 2) eine Richtschnur in Bezug auf das Sicherheitsniveau geschaffen. Diese Vorgaben des Bundes zur Erreichung und Einhaltung eines Mindeststandards an Informationssicherheit erfordern die unter Kapitel 3 beschriebene Umsetzung und die entsprechenden finanziellen Mittel. Es besteht diesbezüglich kein wesentlicher Handlungsspielraum.

Der Grosse Rat ist somit abschliessend zuständig, so dass auch die öffentliche Anhörung entfällt.

7. Auswirkungen

7.1 Personelle und finanzielle Auswirkungen des Entwicklungsschwerpunkts 'Informationssicherheit' in der IT AG

Die finanziellen Auswirkungen für den Kanton sind in Kapitel 5 dargestellt. Zusätzlich wird das interne Team der Sicherheitsexperten im CISO Office sowie in verschiedenen Betriebs- und Entwicklungsbereichen personell aufgestockt. Diese neuen Mitarbeitenden werden jedoch nur zum Teil in den Themenbereichen des ESP engagiert. Die nachfolgenden Stellen wurden im Rahmen des regulären AFP-Prozesses vom Regierungsrat bewilligt und ab Budgetjahr 2025 im AB 435 'Informatik' eingestellt.

Tabelle 5: Stellenbedarf

Stellenbedarf	FTE
Security-Architect; Informatik Aargau Sektion TLE, Gruppe TM (Projektbeizug zu ZeroTrust)	1.0
SOC Tier 3 Analyst; Informatik Aargau; Gruppe: CISO Office	1.0
DLP Engineer; Informatik Aargau; Sektion SB; Gruppe WPM (Teilbezug zu Datenklassifikation)	1.0
Security Engineer; Informatik Aargau; Sektionen SB/TLE; diverse Gruppen (Teilbezug zu DevSecOps)	5.0
Security Comms & Training Specialist; Informatik Aargau; Sektion: KSM, Gruppe: IT-Bildung (Teilbezug zu Security Awareness)	0.5
Total	8.5

7.2 Auswirkungen auf die Wirtschaft und Gesellschaft

Wo immer mit sensiblen Daten gearbeitet wird, ist vor dem Hintergrund der sich akzentuierenden Bedrohungslage im Bereich der Cyberkriminalität eine zeitgemässe Informationssicherheit mit einem effektiven Security-Dispositiv von zentraler Bedeutung: Dies trifft nicht nur auf den Kanton Aargau, sondern auch auf seine Stakeholder und letztlich auf die Einwohnerinnen und Einwohnern zu. Daten des Kantons Aargau und seine Interessensgruppen können mit einer gut aufgestellten Informationssicherheit angemessen geschützt werden.

7.3 Auswirkungen auf Umwelt und Klima

Keine.

7.4 Auswirkungen auf die Gemeinden und auf die Beziehungen zum Bund und anderen Kantonen

Aufgrund der vielfältigen digitalen Verknüpfungen zwischen den föderalen Ebenen profitieren vor allem auch die Gemeinden von einem stabilen und sicheren Informatikumfeld. Sie beziehen auf diesem Weg Dienstleistungen von der Verwaltung und stellen ihre Behördenleistungen zum Teil über das kantonale Smart-Service-Portal auf ag.ch zur Verfügung.

8. Wirkungsprüfung

Im jährlichen Rechenschaftsbericht informiert der CISO die GSK über den Status und den Fortschritt bei der Massnahmenumsetzung. Da es sich hierbei um sensible Informationen handelt, werden diese lediglich verwaltungsintern kommuniziert.

Für die Öffentlichkeit werden im Rahmen des AFP respektive des Jahresberichts verschiedene Kennzahlen zur Informationssicherheit publiziert. Diese geben Aufschluss über die Tätigkeiten, ohne damit Schwachstellen oder geplante Aktivitäten offen zu legen.

9. Weiteres Vorgehen

Die einzelnen Teilprojekte sollen in den folgenden Zeitabschnitten umgesetzt werden. Aufgrund der Dringlichkeit wurde bei einzelnen Teilprojekten bereits mit Vorarbeiten begonnen.

Tabelle 6: Weiteres Vorgehen

Security Operations Center (SOC; Einheit zur Überwachung, Analyse und Schutz vor Cyberbedrohungen)	Q1 2024 bis Q4 2025
DevSecOps (Sicherheitsorientierte Entwicklung & IT-Betriebsführung)	Q1 2024 bis Q4 2025
IAM NextGen (Identitäts- und Zugriffsverwaltung)	Q1 2024 bis Q3 2028
Security Awareness	Q2 2024 bis Q2 2025
ISO/IEC 27001 Strategie	Q2 2024 bis Q4 2028
Datenklassifizierung und Datenkategorisierung	Q2 2024 bis Q4 2027
Zero-Trust (Sicherheitskonzept zur Autorisierung von Akteuren und Systemen)	Q2 2024 bis Q4 2029

Antrag

Für das Vorhaben "Informationssicherheit; Umsetzung Massnahmen Informatik Aargau" wird ein Verpflichtungskredit für einen einmaligen Bruttoaufwand von Fr. 7'168'000.– und für einen jährlich wiederkehrenden Bruttoaufwand von Fr. 3'924'000.– beschlossen.

Regierungsrat Aargau