KANTON AARGAU

DEPARTEMENT
FINANZEN UND RESSOURCEN
Informatik Aargau

2. September 2021

BERICHT

INFORMATIONSSICHERHEITSSTRATEGIE des Kantons Aargau

Dokumentinformation

Klassifikation	INTERN / C2
Autor/-in:	Roger Kamm
Version | Status	1.0 FINAL
Freigabe:	02.09.2021 / GSK-Beschluss vom 30.08.2021
Letzte Änderung:	02.09.2021
Wiedervorlage / Prüfzyklus	Jährlich sowie bei Änderungen
In Kraft seit:	30.08.2021 (GSK)
Dokumenten-Nummer:	

Versionsinformation

Version	Datum	Autor	Kurzzeichen	Beschreibung
1.0	02.09.2021	Roger Kamm	RKC7	Finalisiert nach GSK vom 30.08.2021

Inhaltsverzeichnis

1. Einführung 3

2. Informationssicherheits-Management im Kanton Aargau 4
2.1 Geltungsbereich 4
2.2 Ziele der Informationssicherheitsstrategie 4
2.3 Grundsätze der Informationssicherheitsstrategie 5
2.4 Rechtliche Grundlagen 6
2.4.1 auf Bundesebene 6
2.4.2 auf kantonaler Ebene 6
2.5 Aufbau des Informationssicherheits-Managements 7
2.5.1 Gesetzliche, normative und operative Ebene 7
2.5.2 Informationssicherheits-Management KTAG 9
2.6 Informationssicherheit, IT-Sicherheit und Datenschutz 10

3. Elemente der Informationssicherheit des Kantons Aargau 11
3.1 Informationssicherheits-Management und Informationssicherheits-Management-System 11
3.1.1 Risikomanagement 11
3.1.2 Inventarisierung der Systeme 12
3.1.3 Klassifizierung von Informationen und Feststellung des Schutzbedarfes 12
3.1.4 Informationssicherheit in Projekten 12
3.1.5 Prozess zur Behandlung von Sicherheitsvorfällen 12
3.2 Aufgaben, Kompetenzen, Verantwortung (AKV) 13
3.2.1 Generalsekretärenkonferenz (GSK) 13
3.2.2 Informatikkonferenz (IK) 14
3.2.3 Generalsekretärinnen und Generalsekretäre 14
3.2.4 Chief Information Security Officer (CISO) 15
3.2.5 Informationssicherheitsbeauftragte Person (ISBP) 16
3.2.6 Security- und Cyber-Security Engineer 17
3.2.7 Beauftragte für Öffentlichkeit und Datenschutz (ÖDB) 18
3.2.8 Governance-Modell (Normative und operative Ebene) 18

Abbildungsverzeichnis

Abbildung 1: Gesetzliche, normative und operative Ebene des Informationssicherheits-Managements im KTAG 7
Abbildung 2: Umfang und Einflussfaktoren des Informationssicherheits-Management 9
Abbildung 3: Schnitt- und Teilmengen von Informationssicherheit, IT-Sicherheit und Datenschutz 10
Abbildung 4: Governance Modell 18

1. Einführung

Das Informationssicherheits-Management umfasst alle Planungs- und Lenkungsaufgaben, die notwendig sind, damit angemessene Informationssicherheit im Kanton Aargau im Sinne eines effizienten und effektiven Prozesses etabliert und aufrechterhalten werden kann.

Die rasche und intensive Verbreitung von Informationssystemen hat im Zuge der Digitalisierung und digitalen Transformation – nicht zuletzt durch die Corona-Krise – nochmals an Bedeutung zugenommen und führt im Kanton Aargau in verschiedenen Bereichen zu Problemen, weil die bestehenden Grundlagen und Instrumente nicht mehr zeitgemäss sind. Es liegt daher auf der Hand, dass der wachsenden Risikoexposition mit wirksamen Massnahmen auf der organisatorischen und technischen Ebene entgegengetreten werden muss.

Im Kanton Aargau ist die Informatik Aargau im Rahmen der *Richtlinie der Generalsekretärenkonferenz (GSK) für die Führung und Steuerung der Informatik in der kantonalen Verwaltung* mit der Etablierung, Aufrechterhaltung und Kontrolle der Informationssicherheit – dem Informationssicherheits-Management – beauftragt. Die dafür notwendigen Grundlagen und Instrumente werden durch den Informationssicherheitsbeauftragten (Chief Information Security Officer; CISO) geschaffen und unterhalten. Die Umsetzung der Informationssicherheit erfolgt in Zusammenarbeit zwischen den Departementen mit ihren Abteilungen/Ämtern und der Informatik Aargau (IT AG).

Das Informationssicherheits-Management ist eine mit dem *Datenschutz* verwandte Disziplin und teilt einige gemeinsame, überlappende Themenbereiche. Den Datenschutz betreffende Anliegen werden von der Beauftragten für Öffentlichkeit und Datenschutz vertreten und die gemeinsamen Themenbereiche auf regelmässiger Basis mit dem CISO abgestimmt.

Der Kanton Aargau ist mit seinen vielfältigen Aufgaben zunehmend exponiert und angehalten, seine Informationssicherheit auf die vielfältigen Bedrohungssituationen auszurichten. Zu diesem Zweck wurde die seit 2010 gültige IT-Sicherheitsstrategie grundlegend überarbeitet, neu strukturiert sowie auf das Niveau der *Informationssicherheit* angehoben und entsprechend ausgeweitet. Informationssicherheit beschreibt neben dem Schutz von IKT-Systemen (IT-Sicherheit) auch den Schutz jeglicher Informationen (hinsichtlich der Informationssicherheit synonym zu *Daten*). Die Massnahmen erstrecken sich auf technische und organisatorische Bereiche, also auf Mensch *und* Technik.

Alle diese Massnahmen sind im Informationssicherheits-Management zusammengefasst und werden in *der Informationssicherheitsstrategie*, dem *Informationssicherheitskonzept* und den *Sicherheits-Standards* als gemeinsames Normativ festgelegt. Nicht zuletzt wird mit der Umsetzung solcher Massnahmen erreicht, dass das Verwaltungshandeln – Geschäftsprozesse und Interaktionen des Kantons Aargau mit seinen Einwohnerinnen und Einwohnern sowie den Unternehmen, dem Bund, den Gemeinden und weiteren Stakeholdern – möglichst von Informationssicherheitsvorfällen verschont bleibt und finanzielle Schäden sowie Reputationsverluste ausbleiben.

Fritz A. Zanzerl
Abteilungsleiter Informatik Aargau

Roger Kamm
Chief Information Security Officer (CISO)

2. Informationssicherheits-Management im Kanton Aargau

Das Informationssicherheits-Management umfasst alle Planungs- und Lenkungsaufgaben, die notwendig sind, damit angemessene Informationssicherheit in Kanton Aargau im Sinne eines effektiven Prozesses etabliert und aufrechterhalten werden kann.

Die Informationssicherheitsstrategie und ihre assoziierten Dokumente dienen somit der Definition des angemessenen Schutzes von jeglicher Art von Informationen und sind für sämtliche Aufgabenbereiche im Kanton Aargau verbindlich (vgl. Anhang 1 des Dekrets über die wirkungsorientierte Steuerung von Aufgaben und Finanzen (DAF)). Im Zuständigkeitsbereich des Regierungsrats sind die Departemente und die Staatskanzlei für den Vollzug ihrer Aufgabenbereiche zuständig (vgl. Anhang 1 der Verordnung über die wirkungsorientierte Steuerung von Aufgaben und Finanzen (VAF)). Für die genannten Organisationen bzw. "alle Aufgabenbereiche" wird nachfolgend die Abkürzung *KTAG* verwendet.

2.1 Geltungsbereich

Der Geltungsbereich der Informationssicherheitsstrategie und ihrer assoziierten Dokumente erstreckt sich auf alle Organisationseinheiten im KTAG. Sie gilt ebenfalls für Geschäftspartner und Dienstleister des KTAG. Bei der Zusammenarbeit mit externen Stellen ist die Durchsetzung der hier festgelegten Grundsätze, soweit wie möglich, vertraglich zu vereinbaren.

Die vorliegende Informationssicherheitsstrategie ersetzt die IT-Sicherheitsstrategie vom 28.06.2010.

2.2 Ziele der Informationssicherheitsstrategie

Die folgenden Ziele gelten für die Informationssicherheitsstrategie des KTAG (und ihrer assoziierten Dokumente):

- Die Informationssicherheit im KTAG wird als Prozess gesteuert und kontinuierlich weiterentwickelt, um sich den ändernden Rahmenbedingungen und Risiken anzupassen. Zur Steuerung der Informationen werden definierte Kennzahlen beigezogen.
- Die Definition und Umsetzung des Informationssicherheits-Managements orientiert sich an den Prämissen des *Entwicklungsleitbildes des Regierungsrats 2021-2030*[1], der *Strategie SmartAargau*[2], der *Open Government Data Strategie 2017-2022*[3] und der *Fachstrategie Informatik 2020-2026*[4].
- Es ist sichergestellt, dass für die Mitarbeitenden des KTAG bei der Bearbeitung von Informationen eine rechtliche Grundlage besteht.
- Es ist sichergestellt, dass die Mitarbeitenden des KTAG im rechtmässigen Umgang und bei der Bearbeitung von Informationen geschult sind.

[1] https://www.ag.ch/de/rr/strategie_rr/entwicklungsleitbild/entwicklungsleitbild.jsp
[2] https://www.ag.ch/de/themen_1/smartaargau/strategie_smartaargau/strategie_smartaargau_1.jsp
[3] https://www.ag.ch/de/weiteres/aktuelles/medienportal/medienmitteilung/medienmitteilungen/mediendetails_77526.jsp#:~:text=Der%20Kanton%20und%20die%20Aargauer,swiss%20zur%20Verf%C3%BCgung.
[4] https://www.ag.ch/media/kanton_aargau/dfr/dokumente_3/ueber_uns_6/organisation_7/191128_ktag_brosch_fachstrategie.pdf

- Die Mitarbeitenden kennen den Wert und die Bedeutung des Datenschutzes und der Informationssicherheit. Sie kennen die gesetzlichen Bestimmungen und internen Weisungen und handeln danach.

2.3 Grundsätze der Informationssicherheitsstrategie

Die folgenden Grundsätze gelten für die Informationssicherheitsstrategie des KTAG (und ihrer assoziierten Dokumente):

- Die Informationen des KTAG sind klassifiziert. Mit der Klassifikation wird der Schutzbedarf der betreffenden Information definiert. Die Klassifikation unterstützt das Sicherheitsbewusstsein der Mitarbeitenden des KTAG im Umgang mit Informationen oder bei der Wahrung des Amtsgeheimnisses. Verantwortlich für die richtige Klassifikation und somit Schutz sind die jeweiligen Dateneigner.
- Die Informationssicherheitsstrategie des KTAG orientiert sich an den Empfehlungen der international anerkannten Sicherheitsstandards gemäss ISO 27001[5] sowie ISO 27002[6] und stellt so sicher, dass der KTAG auf bewährte Best Practices setzt.
- Die Umsetzung der Informationssicherheit erfolgt risikobasiert (vgl. Kapitel 3.1.1). Definition und Umsetzung orientiert sich an etablierten Standards und Best Practices[7]. Restrisiken sind zu bewerten und vom Dateneigner zu tragen.
- Um die Informationssicherheit gewährleisten zu können, werden alle Applikationen und Services im Rahmen der geltenden Prozesse eingeführt und betrieben.
- Alle Applikationen und Services sind so dokumentiert, dass der erforderliche Schutz umgesetzt und überprüft werden kann.
- Alle Informationen und insbesondere Personendaten sind entsprechend ihrem Schutzbedarf geschützt. Sie werden physisch oder elektronisch auf den Systemen des KTAG so gespeichert, bearbeitet und übertragen, dass die Schutzziele (Verfügbarkeit, Vertraulichkeit, Integrität, Authentizität) sichergestellt sind.
- Die Informationssicherheitsmassnahmen werden im KTAG so umgesetzt, dass die Ausgewogenheit zwischen Sicherheitsanforderungen einerseits und Funktionalität, Leistungsfähigkeit, Wirtschaftlichkeit sowie Bedienkomfort andererseits sichergestellt ist.
- Die Wirksamkeit der Informationssicherheitsmassnahmen wird periodisch überprüft. Aus dem Ergebnis der Überprüfung können erforderliche Massnahmen abgeleitet werden. Deren Umsetzung wird im Rahmen des Sicherheitsmanagements überwacht.
- Die Bearbeitung von Störfällen und die Krisenbehandlung werden durch die Notfallorganisationen periodisch geübt. Dabei kommen definierte und dokumentierte Prozesse zum Einsatz.

[5] https://www.iso.org/isoiec-27001-information-security.html
[6] Code of practice for information security controls https://www.iso.org/standard/54533.html
[7] Normen- und Standardorientierung: z.B. ISO/IEC Normen, ITIL und Branchenstandards (z.B. BSI-Standards)

2.4 Rechtliche Grundlagen

2.4.1 auf Bundesebene

Das Bundesrecht sieht für den Kanton lediglich das bundesrechtlich gestützte Bearbeiten von Informationen durch den Kanton als rechtliche Grundlagen vor. Hierbei gilt einerseits die Verordnung über den Schutz von Informationen des Bundes (Informationsschutzverordnung, ISchV) vom 4. Juli 2007 (SAR 510.411) nur, wenn der Kanton klassifizierte Informationen bearbeitet und soweit dies im Bundesrecht vorgesehen ist oder entsprechend vereinbart wurde (Art. 2 lit. c ISchV). Andererseits gelten für das Bearbeiten von Personendaten durch kantonale Organe beim Vollzug von Bundesrecht die Art. 1-11a, 16, 17, 18-22 und 25 Abs. 1-3 des Bundesgesetzes über den Datenschutz (DSG) vom 19. Juni 1992 (SR 235.1), soweit keine kantonalen Datenschutzvorschriften bestehen, die einen angemessenen Schutz gewährleisten (Art. 37 Abs. 1 DSG). Dabei ist zu beachten, dass das DSG ausschliesslich den Schutz der Persönlichkeit und der Grundrechte von natürlichen und juristischen Personen, über die Daten bearbeitet werden, bezweckt, und nicht die Informationssicherheit zum Inhalt hat (vgl. Art. 1 i.V.m. Art. 3 Bst. b DSG).

2.4.2 auf kantonaler Ebene

Das Gesetz über die Information der Öffentlichkeit, den Datenschutz und das Archivwesen (IDAG) vom 24. Oktober 2006 (SAR 150.700) regelt die amtliche Information der Öffentlichkeit und den Zugang zu amtlichen Dokumenten, das Archivwesen sowie den Umgang mit Personendaten durch öffentliche Organe (§ 1 IDAG). Das IDAG stellt dabei zwar nur den Schutz von Personendaten sicher, also von Daten, die sich auf eine bestimmte oder bestimmbare natürliche Person beziehen (vgl. § 1 Abs. 1 lit. b i.V.m. § 3 Abs. 1 lit. d IDAG). In Bezug auf alle anderen Informationen beziehungsweise auf die Informationssicherheit finden sich jedoch – mit Ausnahme der Vorgaben für das Archivwesen (vgl. § 43 ff. IDAG) – keine rechtlichen Grundlagen im kantonalen Recht.

2.5 Aufbau des Informationssicherheits-Managements

2.5.1 Gesetzliche, normative und operative Ebene

Die normative Ebene in der Pyramide des Informationssicherheits-Managements besteht aus den Elementen der *Informationssicherheitsstrategie*, dem *Informationssicherheitskonzept* und den *Sicherheits-Standard*s.

Das vorliegende Dokument beschreibt die Informationssicherheitsstrategie. Das Informationssicherheitskonzept sowie die Sicherheits-Standards sind als eigenständige Dokumente verfasst und gehen aus der Informationssicherheitsstrategie hervor.

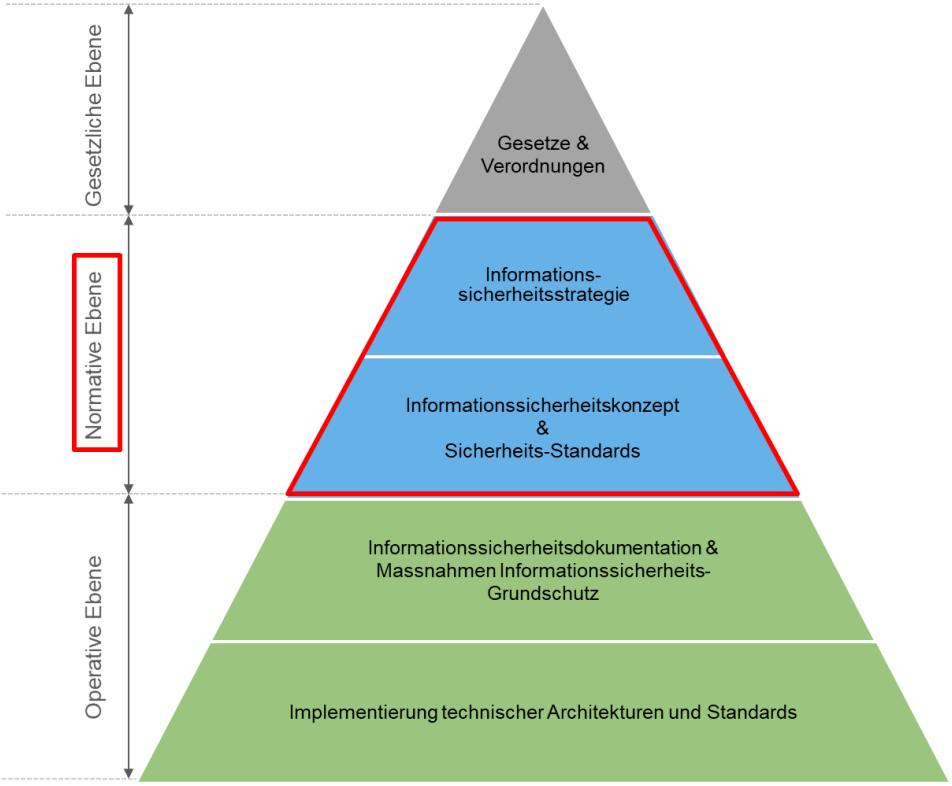

Abbildung 1: Gesetzliche, normative und operative Ebene des Informationssicherheits-Managements im KTAG

Gesetzliche Ebene:
Gesetze und Verordnungen gemäss Kapitel *2.4.1* und Kapitel *2.4.2* definieren den Rahmen für die Informationssicherheit im KTAG.

Normative Ebene
Die normative Ebene beschreibt die grundlegenden Elemente des Informationssicherheits-Managements im KTAG. Sie besteht aus den Elementen Informationssicherheitsstrategie, Informationssicherheitskonzept und Sicherheits-Standards.

- Die *Informationssicherheitsstrategie* beschreibt Ziele, Grundsätze und Organisation im Sinne einer Charta (*Was* bedeutet Informationssicherheit im KTAG?). Die Informationssicherheitsstrategie ist langfristig ausgerichtet und erfährt wenig Änderungen und wird jährlich überprüft und gegeben falls aktualisiert.

- Das *Informationssicherheitskonzept* beschreibt die taktischen Massnahmen und Handlungsfelder (im Sinne von Themenbereichen bspw. dem Schutz von Objekten) zur Erreichung von Zielen und zur Einhaltung von Grundsätzen der Informationssicherheitsstrategie (*Wie/Womit* wird Informationssicherheit erreicht?). Das Informationssicherheitskonzept ist mittelfristig ausgerichtet und erfährt periodische Anpassungen. Dabei orientiert es sich an den technologischen Entwicklungen und neuen Bedrohungssituationen.
- Die *Sicherheits-Standards* beschreiben konkrete Handlungsanweisungen, welche von allen Organisationsteilnehmenden einzuhalten sind, indem sie die im Informationssicherheitskonzept definierten taktischen Massnahmen und Handlungsfelder operationalisieren (bspw. der Sicherheits-Standard *Datenklassifikation*). Sicherheitsstandards ändern sich hinsichtlich Anzahl und Inhalt laufend – Änderungen werden regelmässig kommuniziert.

Operative Ebene

Auf der operativen Ebene des Informationssicherheits-Managements erfolgt die Umsetzung der Informationssicherheit durch die Organisationseinheiten mit entsprechenden *Informationssicherheitsdokumentation* respektive *Implementierungen von technischen Architekturen- und Standards* anhand der normativen Vorgaben.

- Mit den der *Informationssicherheitsdokumentation* (Schutzbedarfsanalyse (Schuban), ISDS-Konzept, Risikoanalyse und, wenn erforderlich, Datenschutzfolgeabschätzung (DSFA)) werden alle relevanten Informationen erfasst und die Risiken identifiziert/dokumentiert. Diese Informationen werden zur Beurteilung des Schutzbedarfs und der Festlegung von Schutzmassnahmen herangezogen, damit die Risiken auf ein annehmbares Restrisiko reduziert werden.
- Mit der Implementierung technischer Architekturen und Standards wird der Grundschutz oder auch erweiterte Schutzniveaus der Schutzobjekte sichergestellt. Dabei orientieren sich diese Massnahmen an in den Sicherheits-Standards festgelegten Handlungsanweisungen (Konfigurationen; Implementierung).

Die Segregation auf drei Ebenen und die Dokumentenhierarchie innerhalb der normativen Ebene vereinfachen das Informationssicherheits-Management in mehrfacher Hinsicht:

- Klare Trennlinie hinsichtlich der Verantwortung für die verschiedenen Ebenen (v.a. auf der normativen und der operativen Ebene) und somit Reduktion von Missverständnissen.
- Die Dokumentenhierarchie lässt flexible und schnelle Anpassung des Informationssicherheits-Managements zu, wenn neue technologische Entwicklungen oder Bedrohungen dies notwendig machen.
- Änderungen beziehungsweise Anpassungen an Dokumenten der normativen Ebene werden stufengerecht im Rahmen der Prozesse und Kompetenzen bestehender Richtlinien der Generalsekretärenkonferenz resp. der Informatikkonferenz beurteilt und verabschiedet.

Aufgaben, Kompetenzen und Verantwortung des Informationssicherheits-Managements auf der normativen und der operativen Ebene sind im Kapitel 3.2ff detailliert beschrieben.

2.5.2 Informationssicherheits-Management KTAG

Die folgende Abbildung stellt den Umfang und die Einflussfaktoren des Informationssicherheits-Managements im KTAG dar. Dieses umfasst alle Planungs- und Lenkungsaufgaben, die notwendig sind, damit angemessene Informationssicherheit in Kanton Aargau im Sinne eines effektiven Prozesses für IKT- und nicht-IKT-Systeme respektive für digitale und analoge Informationen etabliert und aufrechterhalten werden kann (vgl. Kapitel 2f).

Aus den kantonalen Strategien, Gesetzen, Standards & Best Practices sowie den kantonalen Informatikvorgaben leiten sich die in den Kapiteln 2.2 und Kapitel 2.3 formulierten Ziele bzw. Grundsätze der Informationssicherheitsstrategie ab. Diese wiederum determinieren den Inhalt des Informationssicherheits-Konzepts sowie den Sicherheits-Standards:

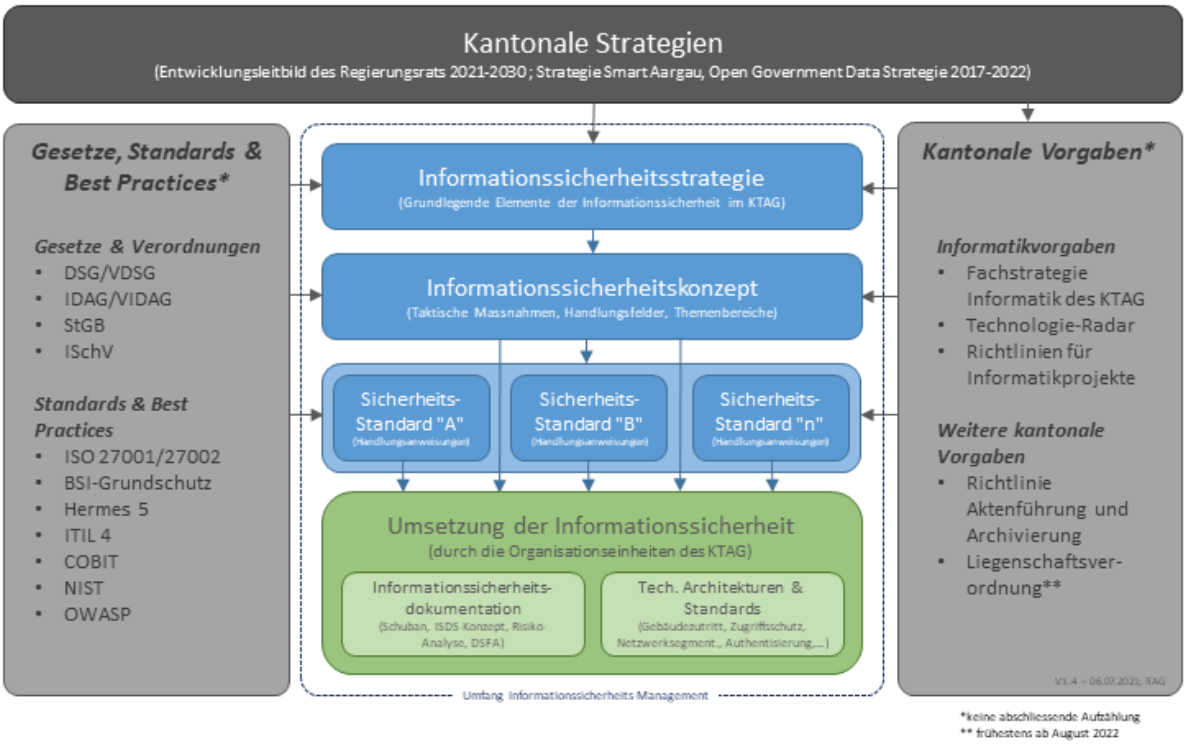

Abbildung 2: Umfang und Einflussfaktoren des Informationssicherheits-Management

2.6 Informationssicherheit, IT-Sicherheit und Datenschutz

Informationssicherheit und Datenschutz sind verwandte, sich in einigen Bereichen überlappende Themenbereiche. IT-Sicherheit wiederum ist eine Teilmenge der Informationssicherheit. Die nachfolgende Grafik veranschaulicht die Beziehungen der verschiedenen Themenbereiche und deren assoziierte Rollen zur Definition notwendiger Grundlagen und Rahmenbedingungen auf der normativen Ebene:

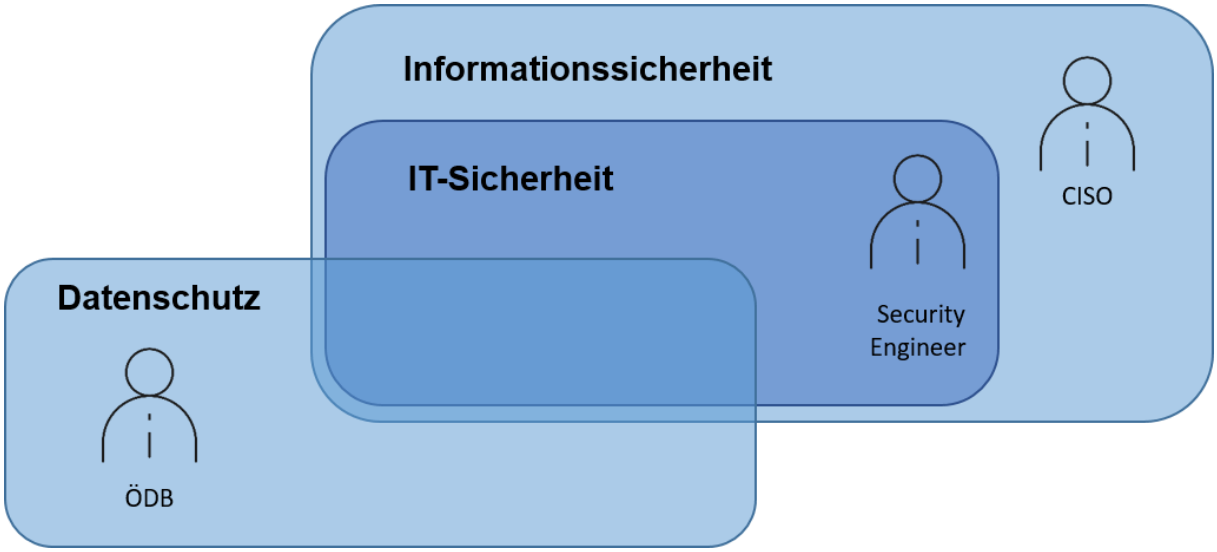

Abbildung 3: Schnitt- und Teilmengen von Informationssicherheit, IT-Sicherheit und Datenschutz

Informationssicherheit:
Die Informationssicherheit befasst sich mit dem Schutz von Informationen im Kontext ihres Schutzbedarfs, unabhängig davon, ob es sich dabei um Personendaten oder andere Informationen handelt. Die Informationssicherheit begegnet den Risiken, indem sie die Information vor Manipulation, Verlust oder unberechtigter Offenlegung schützt. Dabei ist es unerheblich, ob es sich um digitale oder analoge Informationen handelt. Die Definition und Unterhalt der Grundlagen und Instrumente für den Bereich der Informationssicherheit obliegt dem CISO.

IT-Sicherheit:
Die IT-Sicherheit ist als Teilbereich innerhalb der Informationssicherheit verortet und befasst sich mit dem Schutz von IKT-Systemen und den darin gespeicherten Informationen. Die Definition der IT-Sicherheit im Sinne von den technischen Möglichkeiten und Entwicklungen angepasste Architekturen, Standards und Implementationen wird in enger Zusammenarbeit zwischen CISO, (Cyber-) Security Engineers sowie internen und externen Fachspezialisten vorgenommen.

Datenschutz:
Der Datenschutz beschreibt im Gegensatz zur Informationssicherheit ausschliesslich den Schutz der Privatsphäre einer Person (Personendaten). Der Datenschutz garantiert jeder Person ein Recht auf informationelle Selbstbestimmung und schützt sie vor missbräuchlicher Verwendung ihrer Daten. Die Verantwortung für den Bereich des Datenschutzes obliegt der Beauftragten für Öffentlichkeit und Datenschutz.

3. Elemente der Informationssicherheit des Kantons Aargau

3.1 Informationssicherheits-Management und Informationssicherheits-Management-System

Informationssicherheits-Management resultiert durch das Zusammenspiel von Vorgaben und Definitionen auf der normativen Ebenen und deren Umsetzung und Kontrolle im Sinne von konkreten Aktivitäten und Massnahmen auf der operativen Ebene (vgl. Abbildung 1, Seite 7 und Abbildung 2, Seite 9).

Zu diesem Zweck betreibt der KTAG ein Informationssicherheits-Managementsystem (ISMS[8]), in welchem die Sicherheitsorganisation, alle geltenden Vorgaben, Massnahmen und strategischen Prozesse im Bereich Informationssicherheit dokumentiert, koordiniert und an die unternehmensspezifischen Anforderungen angepasst werden. Weiter werden im ISMS Kennzahlen und Bewertungsgrundlagen definiert und abgebildet, welche für das Reporting und die Kommunikation der Informationssicherheit notwendig sind.

Das ISMS wird vom Chief Information Security Officer der Informatik Aargau (CISO) verantwortet, betrieben und aktuell gehalten.

Effektivität und Effizienz der Sicherheitsmassnahmen werden laufend überprüft und bei Bedarf verbessert. Zusätzliche Massnahmen werden für kritische Informationen und Systeme in Abhängigkeit von ihrem Schutzbedarf und ihren Bedrohungen definiert.

3.1.1 Risikomanagement

Die Massnahmen zur Wahrung der Informationssicherheit basieren auf der Risikoabschätzung in Bezug auf das Schutzobjekt. Das Risikomanagement ist entsprechend *der* zentrale Prozess der Informationssicherheit.

Die Datenklassifikation, identifizierte Risiken und resultierende Massnahmen werden in der Schutzbedarfsanalyse (Schuban), der Risikoanalyse und im ISDS-Konzept festgehalten und im ISMS sowie, gegebenenfalls in der Datenschutzfolgeabschätzung, dokumentiert. Allfällige Restrisiken werden im Sinne der Güterabwägung von der zuständigen fachverantwortlichen Organisationseinheit (siehe oben Kapitel 2, Absatz 2) bewusst akzeptiert, der entsprechende Entscheid wird schriftlich dokumentiert.

Informationen müssen für *alle* informationstragenden und informationsverarbeitenden *Systeme* (IKT und nicht IKT) erhoben werden und dokumentiert sein. Bei der Erstellung neuer Systeme oder bei Änderungsanträgen (Change Requests) werden die Informationen entlang des Projekt- resp. Change-Prozesses erhoben und dokumentiert. Bei sich im Betrieb befindlichen IKT und nicht IKT-Systemen ohne vorliegende Informationssicherheits-Dokumentation ist diese zu erarbeiten und nachzureichen.

Gleichermassen wird das Risikomanagement auch hinsichtlich der Risiken der *Informationssicherheit* angewendet. Die Risiken werden nach dem selben Prozess systematisch identifiziert, bewertet und überwacht.
Die Risikoanalyse wird regelmässig durchgeführt, um die Risiken und Gefährdungspotentiale im Bereich der Informationssicherheit festzuhalten. Mit der Risikobewertung wird bestimmt, ob die Risikobehandlung erforderlich ist oder das Restrisiko akzeptiert wird. Die identifizierten Risiken werden im Risikobehandlungsplan festgehalten.

Dieser enthält folgende Informationen:

[8] ISMS https://www.iso.org/isoiec-27001-information-security.html

- die eindeutige Beschreibung der Risiken
- die definierten Massnahmen zur Behebung oder Abschwächung der Risiken
- die Umsetzungstermine der definierten Massnahmen
- die für die Umsetzung der Massnahmen verantwortlichen Organisationseinheiten und Personen

3.1.2 Inventarisierung der Systeme

Alle informationstragenden und verarbeitenden Systeme (IKT und nicht IKT) werden im Inventar des ISMS erfasst (vgl. Kapitel 3.1). Die Inventarisierung neuer Objekte / Services erfolgt während verschiedenen Projektphasen, indem die Informationssicherheitsdokumentation (Schutzbedarfsanalyse, ISDS-Konzept und Risikoanalyse) erarbeitet wird. Fehlt die Informationssicherheitsdokumentation für Services, ist diese nach Abschluss des Projektes zu erstellen und nachzureichen. Die Informationen der Inventarisierung werden in der Configuration Management-Database (CMDB) gespeichert.

3.1.3 Klassifizierung von Informationen und Feststellung des Schutzbedarfes

Die Klassifikation von Informationen ist ein wesentliches Element, damit die Erfüllung der Informationssicherheit sichergestellt werden kann. Auf Basis der Klassifikation der Information wird das Schutzniveau festgestellt.
Die Klassifikation und Feststellung des Schutzbedarfes werden während der Ausarbeitung der Informationssicherheitsdokumentation (vgl. Kapitel 2.5.1; *Operative Ebene*) durchgeführt, im ISMS festgehalten und periodisch überprüft. Änderungen an Services führen zu einer Neubeurteilung des Schutzniveaus und ziehen – wo angezeigt – Aktualisierungen der Informationssicherheitsdokumentation nach sich (vgl. auch Kapitel 3.1.1).

3.1.4 Informationssicherheit in Projekten

Informationssicherheit wird als eigenständiges, nicht-funktionales Projektziel betrachtet.
Entsprechend werden die Anliegen der Informationssicherheit neben den Zielkategorien "Funktionalität" und "Leistungsfähigkeit" bei der Konzeption, Realisierung, Umsetzung und Einführung von informationsverarbeitenden Systemen berücksichtigt. Dabei macht es keinen Unterschied, ob Projekte nach der klassischen Wasserfall-Methode oder nach agilen Prinzipien umgesetzt werden.
Die Ausarbeitung der Elemente der Informationssicherheitsdokumentation in den verschiedenen Projektphasen ist in den *Richtlinien zum Vorgehen im IT-Projektmanagement* [9] verankert und festgehalten. Fehlt die Informationssicherheitsdokumentation für Objekte / Services, welche bereits vom Projekt in den ordentlichen Betrieb überführt wurden, ist diese nachzureichen und im Inventar aufzunehmen (vgl. Kapitel 3.1.2).

3.1.5 Prozess zur Behandlung von Sicherheitsvorfällen

Als Sicherheitsvorfälle im Bereich der Informationssicherheit gelten einerseits absichtliche oder unabsichtliche Zuwiderhandlung der geltenden normativen Vorgaben und Definitionen (vgl. Kapitel 2.5.1*; normative Ebene*). Andererseits sind damit Ereignisse gemeint, welche potentiellen oder realen Schaden an Schutzobjekten verursachen können respektive verursacht haben.

[9] https://inka.ag.ch/a-bis-z/geschaefte-projekte/projektmanagement?sectionId=section94759&accordId=0

Bei Eintritt von Ereignissen muss im Sinne der Schadensbegrenzung schnell und konsequent reagiert werden. Sicherheitsvorfälle sind dem CISO unter Angabe der vorliegenden Informationen und Ansprechpersonen in der betroffenen Organisationseinheit zu melden. Durch die Meldung von Sicherheitsvorfällen wird der Prozess zur Behandlung des vorliegenden Sicherheitsvorfalles initiiert.

Dieser Prozess umfasst im ersten Schritt die Analyse und Bewertung des Sicherheitsvorfalles durch den CISO (und ggf. weiteren Stakeholdern), anschliessend werden notwendige Sofortmassnahmen definiert und zur Umsetzung beauftragt. Je nach Auswirkung kann die Eskalation/Kommunikation zu weiteren Stellen und/oder eine Ausweitung der Massnahmen erfolgen.

Notfallmassnahmen sind in einem separaten *Business Continuity Management* (BCM) Konzept festgehalten und sind in der Verantwortung der jeweiligen Organisationseinheit. Ziel von BCM ist es, auch bei einem Systemausfall kritische Geschäftsprozesse aufrecht erhalten zu können sowie die Verfügbarkeit der ausgefallenen Systeme innerhalb einer tolerierbaren Zeitspanne wiederherzustellen.

Dokumentationen und Informationen zum Prozess bei Sicherheitsvorfällen und zum BCM sind im ISMS sowie in InKA und Confluence zu finden. Sie werden laufend aktualisiert und gemäss den neuesten Erkenntnissen angepasst.

3.2 Aufgaben, Kompetenzen, Verantwortung (AKV)

3.2.1 Generalsekretärenkonferenz (GSK)

Die Generalsekretärenkonferenz beauftragt die ITAG in der *Richtlinie der Generalsekretärenkonferenz für die Führung und Steuerung der Informatik in der kantonalen Verwaltung*[10] zur Ausarbeitung und zum Unterhalt der Grundlagen und Instrumente zur Informationssicherheit. Diese Grundlagen umfassen die im Kapitel 2.5.1 beschriebenen Elemente der normativen Ebene des Informationssicherheits-Managements.

Änderungen bzw. Ergänzungen der *Informationssicherheitsstrategie* werden der GSK unterbreitet. Sie verabschiedet diese je nach Kompetenz oder äussert sich mitberichtsweise zuhanden des Regierungsrats.

Neuauflagen, Änderungen beziehungsweise Ergänzungen des *Informationssicherheitskonzeptes* und der *Sicherheits-Standards* werden der GSK zur konferenziellen Behandlung vorgelegt, wenn sich vorgängig unter den ordentlichen Mitgliedern der Informatikkonferenz bzw. ihren Vertretern keine Einigkeit erzielen lässt.

Die GSK erlässt zur Steuerung und Entwicklung der Informationssicherheit im KTAG Kennzahlen. Kennzahlen und Entwicklungsschritte werden im Sinne von Vorschlägen durch die ITAG/CISO formuliert und der GSK zur Verabschiedung vorgelegt. Ziel- und Messwerte werden in periodischen Abständen (in der Regel jährlich) zur Beratung vorgelegt, wenn notwendig werden daraus Massnahmen abgeleitet.

[10] https://inka.ag.ch/media/a-bis-z/ueber-uns/interdepartementale-gremien/gsk-richtlinie-fuehrung-steuerung-informatik.pdf

3.2.2 Informatikkonferenz (IK)

Die Informatikkonferenz unterstützt die Generalsekretärenkonferenz in der Erfüllung ihrer Aufgaben bei der strategischen und operativen Führung der Informatik in der kantonalen Verwaltung im Rahmen der Kompetenzregelung im *Reglement für die Informatikkonferenz*[11].

Änderungen bzw. Ergänzungen der *Informationssicherheitsstrategie* werden den Mitgliedern der IK vor der Behandlung und Verabschiedung durch die GSK zur Beurteilung und Stellungnahme vorgelegt.

Neuauflagen, Änderungen beziehungsweise Ergänzungen des *Informationssicherheitskonzeptes* und der *Sicherheits-Standards* werden den Vertretern der Departemente, GKA und SK durch die Informatik Aargau (CISO) zur Stellungnahme und Beurteilung vorgelegt.

Lässt sich über neue oder geänderte beziehungsweise ergänzte Elemente unter den ordentlichen Mitgliedern der Informatikkonferenz bzw. ihren Vertretern keine Einigkeit erzielen, wird das Geschäft zur konferenziellen Bereinigung der GSK vorgelegt.

3.2.3 Generalsekretärinnen und Generalsekretäre

Die Generalsekretärinnen und Generalsekretäre sind für die Umsetzung der Informationssicherheit innerhalb ihres Zuständigkeitsbereiches rechenschaftspflichtig. Sie sorgen für die notwendigen Rahmenbedingungen (personell und finanziell), die organisatorischen Regelungen und stellen so sicher, dass die Umsetzung der Informationssicherheit gemäss den Vorgaben erfolgen kann.

Die Generalsekretärinnen und Generalsekretäre delegieren die operative Umsetzung des Informationssicherheits-Managements an die Informationssicherheitsbeauftrage Personen (ISBP, vgl. Kapitel 3.2.5) im Sinne der Ausführungsverantwortung.

Verantwortung:

- Rechenschaftspflicht für die Umsetzung der Informationssicherheit im eigenen Verantwortlichkeitsbereich (vgl. Abbildung 1 und Abbildung 2, grüner Bereich)
- Sicherstellung der personellen und finanziellen Ressourcen zur Umsetzung der Informationssicherheit

Aufgaben:

- Periodischer Review des Informationssicherheitsberichtes für den eigenen Verantwortlichkeitsbereich
- Periodische Abstimmung mit der ISBP zur Definition von notwendigen Massnahmen und Entwicklungsschritten im eigenen Verantwortlichkeitsbereich.
- Anhörung der Beauftragten für Öffentlichkeit und Datenschutz bei Massnahmen, die für das Öffentlichkeitsprinzip und den Datenschutz erheblich sind (§ 31 Abs. 1 lit. c IDAG).

Kompetenzen:

- Delegation der Ausführungsverantwortung für die operative Umsetzung der Informationssicherheit im eigenen Zuständigkeitsbereich an die ISBP
- Anordnung von Massnahmen zur Einhaltung der Informationssicherheit innerhalb des eigenen Zuständigkeitsbereiches

[11] https://inka.ag.ch/media/a-bis-z/ueber-uns/interdepartementale-gremien/reglement-informatikkonferenz.pdf

3.2.4 Chief Information Security Officer (CISO)

Der Chief Information Security Officer ist in der Informatik Aargau angestellt und für den Bereich der Informationssicherheit des KTAG verantwortlich, indem Grundlagen und Instrumente zur Sicherstellung angemessener Informationssicherheit geschaffen, unterhalten und weiterentwickelt werden (vgl. Abbildung 1 und Abbildung 2; blauer Bereich). Die Beauftragung erfolgt durch die GSK, welche die Informationssicherheit im KTAG aufgrund definierte Kennzahlen steuert und entwickelt.

Beim Schaffen der Grundlagen und Instrumente werden die Ausgewogenheit zwischen Sicherheitsanforderungen einerseits und Funktionalität, Leistungsfähigkeit, Wirtschaftlichkeit sowie Bedienkomfort anderseits, gleichermassen sichergestellt.

Änderungen beziehungsweise Ergänzungen der *Informationssicherheitsstrategie* sowie Neuauflage, Änderungen beziehungsweise Ergänzungen des *Informationssicherheitskonzeptes* und der *Sicherheits-Standards* werden den Vertretern der Departemente, GKA und SK an der IK durch die Informatik Aargau (CISO) zur Kenntnis gebracht. Dabei werden auch Informationen aufbereitet, die den Hintergrund der technologischen Entwicklung oder vorhandener respektive potentieller Bedrohungsszenarien erläutern und begründen.

Verantwortung:

- Definition, Dokumentation und Unterhalt von Grundlagen und Instrumenten zur Sicherstellung angemessener Informationssicherheit im KTAG, insbesondere der Informationssicherheitsstrategie, dem Informationssicherheitskonzept und den Sicherheitsstandards hinsichtlich der geltenden Ziele, Grundsätze und Vorgaben (vgl. Kapitel 2.2f und Kapitel 2.5.2).
- Definition, Messung und Aufbereitung von Kennzahlen (KPIs, Referenzmodell *Capability Maturity Integration Model*, CMMI) zur Informationssicherheit im Kanton Aargau.
- Aufbau, Betrieb und Weiterentwicklung des Informationssicherheits-Managementsystems (ISMS) des KTAG.
- Koordination angemessener Informationssicherheit zwischen den Stakeholdern im KTAG (Fachbereiche, Informatik Aargau, Lieferanten); Abstimmung und Koordination der Informatiknotfallorganisation und der kantonalen Krisenorganisation.
- Vertretung des KTAG für alle Themen der Informationssicherheit in externen Gremien und Ausschüssen.
- Unterstützung und Kontaktperson für die Informationssicherheitsbeauftragten Personen im KTAG in allen Belangen der Informations- und Informatiksicherheit.

Aufgaben:

- Transparente, periodische Berichterstattung zur Informationssicherheit im Kanton Aargau zu Handen der Generalsekretärenkonferenz und der Informatikkonferenz.
- Erstellung von Jahresplanungen hinsichtlich geplanter Änderungen und Aktualisierungen der Definitionen auf der normativen Ebene.
- Bewertung von Meldungen über Informationssicherheitsvorfälle und Beurteilung von Notfallsituationen.

- Erarbeitung und Durchführung von Schwachstellen- und Risikoanalysen; Bewertung und Prüfung der Notwendigkeit entsprechender Massnahmen (unter Hinzuziehung von betroffenen Organisationen, Fachstellen Spezialisten und ggf. externen Dritten).
- Bearbeitung von Ausnahmegesuchen durch die Informationssicherheitsbeauftragte Person (ISBP), wenn geltenden Vorgaben, Massnahmen und Prozesse im Bereich Informationssicherheit nicht eingehalten werden können.
- Beratung von Informatikleistungserbringern hinsichtlich sicherheitsrelevanter Massnahmen zur Minderung von Informatikrisiken.
- Initiierung, Erarbeitung und Koordination von Awareness-Kampagnen und Schulungsmassnahmen zur Informationssicherheit.
- Überwachung angemessener Ressourcen im Bereich der Informationssicherheit.
- Zusammenarbeit mit Finanzkontrolle und der Beauftragten für Öffentlichkeit und Datenschutz (ÖDB).
- Hinzuziehung und Aktivierung der zuständigen Verantwortlichen bei Informationssicherheitsvorfällen und Aktivierung der Notfallorganisation in Krisenfällen.

Kompetenzen:

- Neuauflage, Änderungen beziehungsweise Ergänzungen von Elementen der normativen Ebene (vgl. Kapitel 2.5.1) unter Wahrung der vorgesehenen konferenziellen Information und Traktandierung (vgl. Kapitel 3.2.1 und Kapitel 3.2.2).
- Anordnung von Sofortmassnahmen in Not- und Krisenfällen unter Einbezug beratender Gremien und Spezialisten.
- Anordnung von Massnahmen zur Wiederherstellung oder Wahrung der Informationssicherheit in enger Zusammenarbeit betroffener Organisationen, Fachstellen Spezialisten und ggf. externen Dritten.

3.2.5 Informationssicherheitsbeauftragte Person (ISBP)

Die Ausführungsverantwortung für die operative Umsetzung des Informationssicherheits-Managements (vgl. Abbildung 1 und Abbildung 2) obliegt der ISBP. Die Rolle der ISBP wird in der Regel durch die Informatikbeauftragten der Departemente, GKA und SK wahrgenommen, entsprechend hat jeder Aufgabenbereich eine ISBP. Die Delegation dieser Rolle an andere Personen innerhalb des Zuständigkeitsbereiches ist möglich und dem CISO im Sinne effektiver Kommunikation zu melden (vgl. Kapitel 3.2.3).

Die ISBP stellt innerhalb des eigenen Zuständigkeitsbereiches sicher, dass die Umsetzung der Informationssicherheit auf der operativen Ebene anhand der dafür vorgesehenen Prozesse und Vorgaben erfolgt und dient als Ansprechpartner für den CISO.

Verantwortung:

- Ansprechperson für den CISO und die Fachbereiche sowie Koordinationsstelle für Informationssicherheit betreffende Themen im eigenen Zuständigkeitsbereich.
- Ansprechperson und Koordinationsstelle bei Notfällen und in Krisensituationen im eigenen Zuständigkeitsbereich.

Aufgaben:

- Sicherstellung der Umsetzung von geltenden Grundsätzen und Massnahmen zur Einhaltung der Informationssicherheit entlang der Anforderungen aus der Informationssicherheitsstrategie, Informationssicherheitskonzept und den Sicherheits-Standards (vgl. Abbildung 2) im KTAG innerhalb der eigenen Organisationseinheit.
- Beantragung von Ausnahmegesuchen, wenn geltenden Vorgaben, Massnahmen und Prozesse im Bereich Informationssicherheit nicht eingehalten werden können.

Kompetenz:

- Entscheidet in Abstimmung mit der jeweiligen Organisationeinheit über die Massnahmen zur Einhaltung der Informationssicherheit und definiert die Akzeptanzkriterien der unvermeidbaren Restrisiken.
- Anordnung von Massnahmen zur Einhaltung der Informationssicherheit im eigenen Zuständigkeitsbereich.

3.2.6 Security- und Cyber-Security Engineer

Der Security- respektive Cyber-Security-Engineer ist in der Informatik Aargau (im Security Team, zusammen mit dem CISO) angestellt und für den Bereich IT-Sicherheit verantwortlich, indem Grundlagen und Instrumente zur Sicherstellung angemessener IT-Sicherheit geschaffen, unterhalten und weiterentwickelt werden. Im Wesentlichen handelt es sich um Beiträge im Informationssicherheitskonzept und den Sicherheits-Standards.

Beim Schaffen dieser Grundlagen und Instrumente werden die Ausgewogenheit zwischen Sicherheitsanforderungen einerseits und Funktionalität, Leistungsfähigkeit, Wirtschaftlichkeit sowie Bedienkomfort anderseits, gleichermassen sichergestellt.

Aufgaben:

- Aufbau, Konzept und Realisierung der IT-Sicherheitsinfrastruktur im KTAG, bspw. (nicht abschliessend): Security Information and Event-Management (SIEM), Intrusion Detection System (IDS), Data Loss Prevention (DLP), Advanced Threat Protection (ATP).
- Fachliche Führung und Koordination des Computer Security Response Team (CSIRT) IT AG bei sicherheitsrelevanten Ereignissen (Cyber-Vorfälle).
- Technische und beratenden Unterstützung des CISO und der Fachbereiche bei der Ausarbeitung von Grundlagen und Instrumenten sowie bei Sicherheitsvorfällen.
- Nachbearbeitung und Analyse von Sicherheitsvorfällen sowie Schwachstellensuche (Vulnerability-Management).

- Definition und Messung und Aufbereitung von Kennzahlen zur IT-Sicherheit, Überwachung der Kennzahlen in enger Zusammenarbeit mit den Fachbereichen und dem CISO.
- Stellvertretungsfunktion des CISO bei Abwesenheiten.

3.2.7 Beauftragte für Öffentlichkeit und Datenschutz (ÖDB)

Die Verfassung des Kantons Aargau garantiert jeder Person das Recht auf Schutz der Privatsphäre bei der Bearbeitung personenbezogener Daten sowie das Recht auf Einsicht in amtliche Dokumente (Öffentlichkeitsprinzip).

Diese verfassungsmässigen Rechte sind im Gesetz über die Information der Öffentlichkeit, den Datenschutz und das Archivwesen (IDAG) vom 24. Oktober 2006 näher geregelt. Dem Gesetz unterstehen alle öffentlichen Organe auf kantonaler und kommunaler Ebene.

Für Aufsicht, Beratung und Auskunft ist die beauftragte Person für Öffentlichkeit und Datenschutz zuständig. Sie nimmt Datenschutz-Folgenabschätzungen entgegen und führt Vorab-Konsultationen sowie unabhängige Kontrollen durch[12].

3.2.8 Governance-Modell (Normative und operative Ebene)

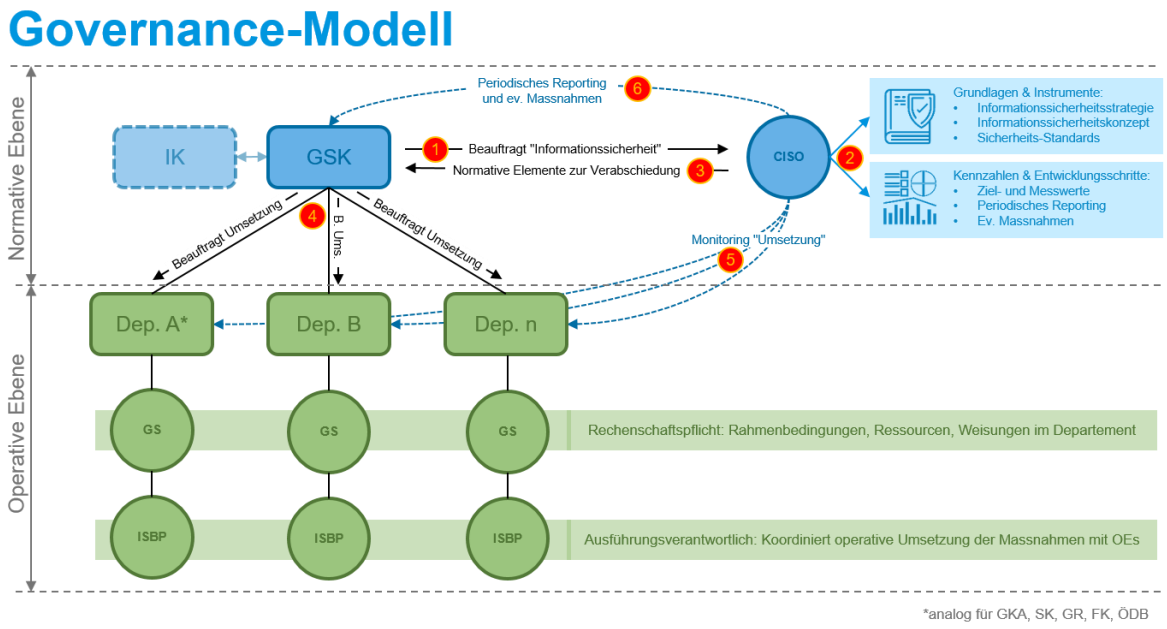

Abbildung 4: Governance Modell

[12] Weitere Informationen: https://www.ag.ch/de/dvi/ueber_uns_dvi/organisation_dvi/generalsekretariat/beauftragte_fuer_oeffentlichkeit_und_datenschutz/beauftragte_fuer_oeffentlichkeit_und_datenschutz.jsp

Ebene	Rolle / Gremium / Instanz	Beschreibung	RACI
Normativ	GSK	Rechenschaftspflichtig (Accountable): Die GSK stellt die Informationssicherheit im KTAG sicher, indem sie die Schaffung von entsprechenden Rahmenbedingungen (normative Ebene) in Auftrag gibt und verabschiedet (per GSK-Entscheid). Zur Ausarbeitung der Grundlagen und dem Monitoring (gesamter KTAG) wird die IT AG / CISO beauftragt. Mit dem periodischen Monitoring und abgeleiteten Massnahmen steuert die GSK die Informationssicherheit im KTAG.	A
Normativ	IT AG / CISO	Ausführungsverantwortlich (Responsible): IT AG / CISO erarbeitet die Rahmenbedingungen per Mandat GSK und ist somit ausführungsverantwortlich, dass die notwendigen Elemente (Grundlagen, Instrumente, Reporting) der normativen Ebene geschaffen sind und für die Umsetzung der Informationssicherheit auf der operativen Ebene zur Verfügung stehen.	R
Normativ	IK	Konsultiert (Consulted): Die Elemente der normativen Ebene werden der IK zur Beratung vorgelegt; das Beratungsergebnis fliesst in die Elemente der normativen Ebene ein.	C
Operativ	Generalsekretär/in (GS)	Rechenschaftspflichtig (Accountable): Für den Zuständigkeitsbereich (Departement, GKA, SK, GR, FK) stellt der oder die GS stellt sicher, dass die Rahmenbedingungen im eigenen Zuständigkeitsbereich geschaffen sind und die Vorgaben der normativen Ebene umgesetzt werden können. Damit die Umsetzung erfolgt, beauftragt die oder der GS die Abteilungen und Ämter entsprechend. Anhand von periodischen Reporting wird die Informationssicherheit im eigenen Bereich gesteuert.	A
Operativ	ISBP	Ausführungsverantwortlich (Responsible): Koordiniert als Ansprechperson der Abteilungen und Ämter die Umsetzung auf der operativen Ebene (Erstellung Informationssicherheitsdokumentation durch Projektleiter, Applikationsverantwortliche, Datenverantwortliche, etc.).	R