KANTON solothurn

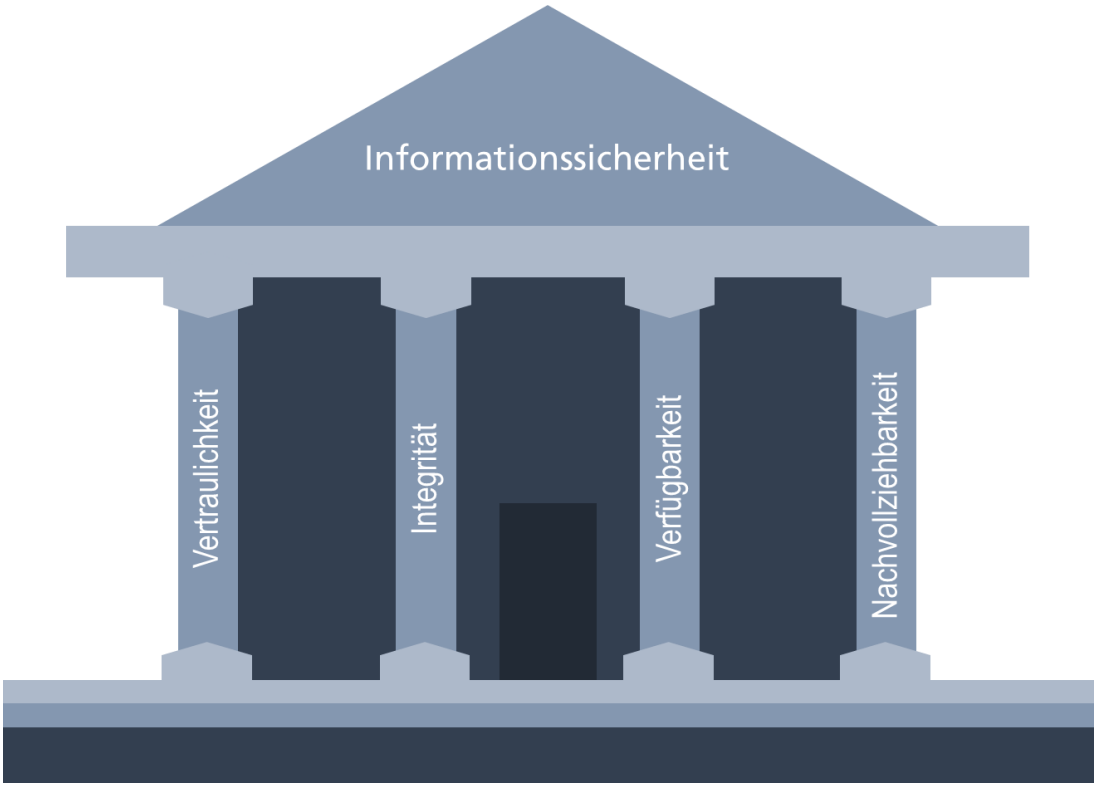

Abbildung 1: Titelbild

Konzept Informationssicherheit der kantonalen Verwaltung, V2.0

Dokumentenhistorie

V1.0	26.04.2022	Ersterstellung
V2.0	21.04.2026	Überarbeitung

Inhaltsverzeichnis

1 Einleitung und Ziel 4
2 Geltungsbereich 4
3 Grundlagen & Anforderungen 4
4 Organisation der Informationssicherheit 5
4.1 Dienststellen 5
4.2 Amt für Informatik und Organisation (AIO) 5
4.3 Informationssicherheitsverantwortliche (ISVs) 6
4.4 ISV-Gremium 6
4.5 IKT-Governance 6
5 Schutzbedarf, Risikoanalyse & ISDS-Konzepte 6
6 IKT-Grundschutz & Ausnahmen 7
7 Behandlung von Sicherheitsvorfällen 7
8 Business Continuity Management (BCM) 8
9 Kommunikation, Schulung und Awareness 8
10 Kontinuierliche Verbesserung & Audit 8
11 Referenzen 8
12 Abbildungsverzeichnis 8

1 Zweck und Zielsetzung

Dieses Konzept konkretisiert die Umsetzung der Leitlinie Informationssicherheit in der kantonalen Verwaltung Solothurn. Es beschreibt die organisatorischen und technischen Grundsätze, Zuständigkeiten sowie die Einbindung der relevanten Gremien und schafft die Grundlage für ein nachhaltiges und wirksames Informationssicherheitsmanagement.

2 Geltungsbereich

Das vorliegende Konzept dient als Grundlage für ein einheitliches Sicherheitsmanagement innerhalb der kantonalen Verwaltung. Das Konzept Informationssicherheit gilt für sämtliche Organisationseinheiten und Mitarbeitenden der kantonalen Verwaltung Solothurn, gemäss IKT-Strategie.

Bei der Zusammenarbeit mit Dritten (Kunden, Partner, Dienstleistungsunternehmen, Lieferanten etc.) müssen die zur Informationssicherheit definierten Sicherheitsstandards so weit als möglich vertraglich eingebunden werden.

3 Grundlagen & Anforderungen

Die Anforderungen beruhen auf:

- dem Informations- und Datenschutzgesetz (InfoDG)
- der Datenschutzverordnung (InfoDV)
- der IKT-Strategie
- Digitalisierungsstrategie
- der IKT-Governance

sowie den Vorgaben aus dem Informationssicherheits-Managementsystem (ISMS) des AIO. Alle Dienststellen richten ihre Massnahmen anhand der Anforderungen aus und tragen die Verantwortung für die Informationssicherheit ihrer eigenen Daten, Anwendungen, Prozesse und Informationsflüsse. Die technische Umsetzung der Informationssicherheit erfolgt durch das AIO oder externe Partner (Betreiber der Services).

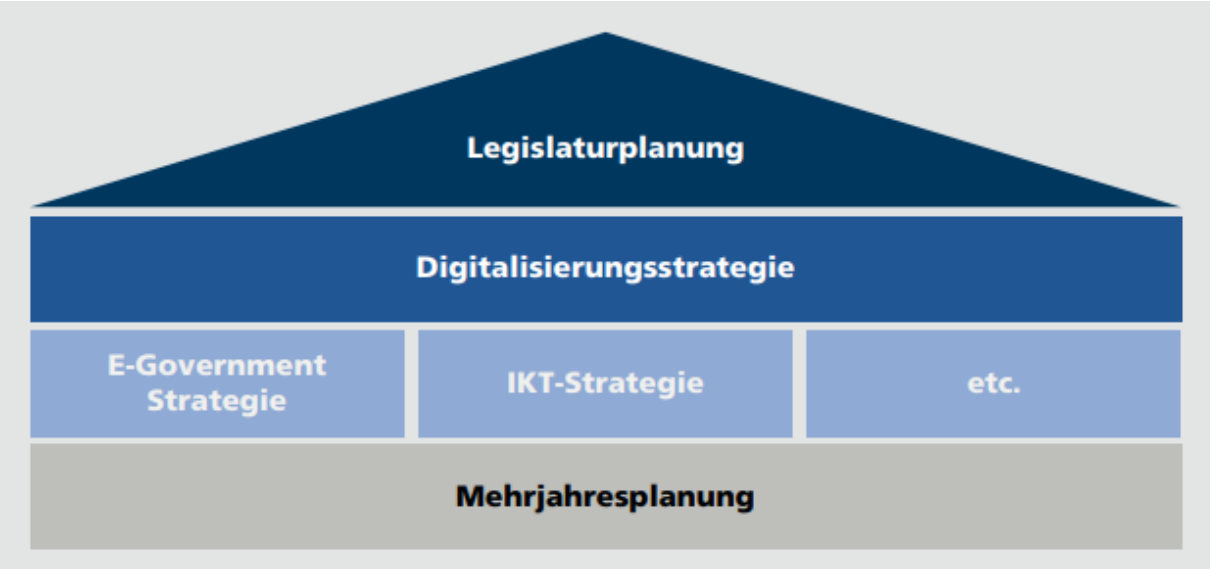

Abbildung 2: Strategieübersicht

4 Organisation der Informationssicherheit

4.1 Dienststellen

Dienststellen sind verantwortlich für den Schutz und die sichere Nutzung ihrer Daten, Informationen, Geschäftsprozesse, Fachanwendungen sowie genutzter Räume und Gebäude. Sie legen den Schutzbedarf ihrer Informationen und Prozesse fest, führen erforderliche Risikoanalysen (bei Bedarf in Zusammenarbeit mit dem AIO) durch und sorgen für die Umsetzung organisatorischer Schutzmassnahmen in ihrem eigenen Verantwortungsbereich. Die Sicherstellung der technischen Schutzmassnahmen der Services erfolgt durch den Betreiber solcher, innerhalb der kantonalen Verwaltung ist dies das AIO oder entsprechende externe Betreiber.

4.2 Amt für Informatik und Organisation (AIO)

Das AIO betreibt die zentralen IT-Services und Fachanwendungen der kantonalen Verwaltung. Es ist verantwortlich für das Informationssicherheits-Managementsystem (ISMS) nach ISO 27001 für die eigenen Services und stellt die Einhaltung und Weiterentwicklung der verbindlichen Sicherheitsstandards (z.B. IKT-Grundschutz) sicher. Das AIO definiert die Sicherheitspolitik, organisiert und führt zentrale Awarenesskampagnen und Schulungen durch, stellt Prozesse, Richtlinien und Hilfsmittel zur Verfügung und berät sowie unterstützt die Dienststellen und Informationssicherheitsverantwortlichen (ISV) in Fragen der Informationssicherheit.
Im operativen Security Bereich betreibt das AIO umfangreiche Security Operations Tätigkeiten. Massnahmen im Informationssicherheitsbereich werden Risikobasiert definiert. Ebenfalls betreibt das AIO ein Business Continuity Management (BCM) für definierte Services in seinem Bereich.

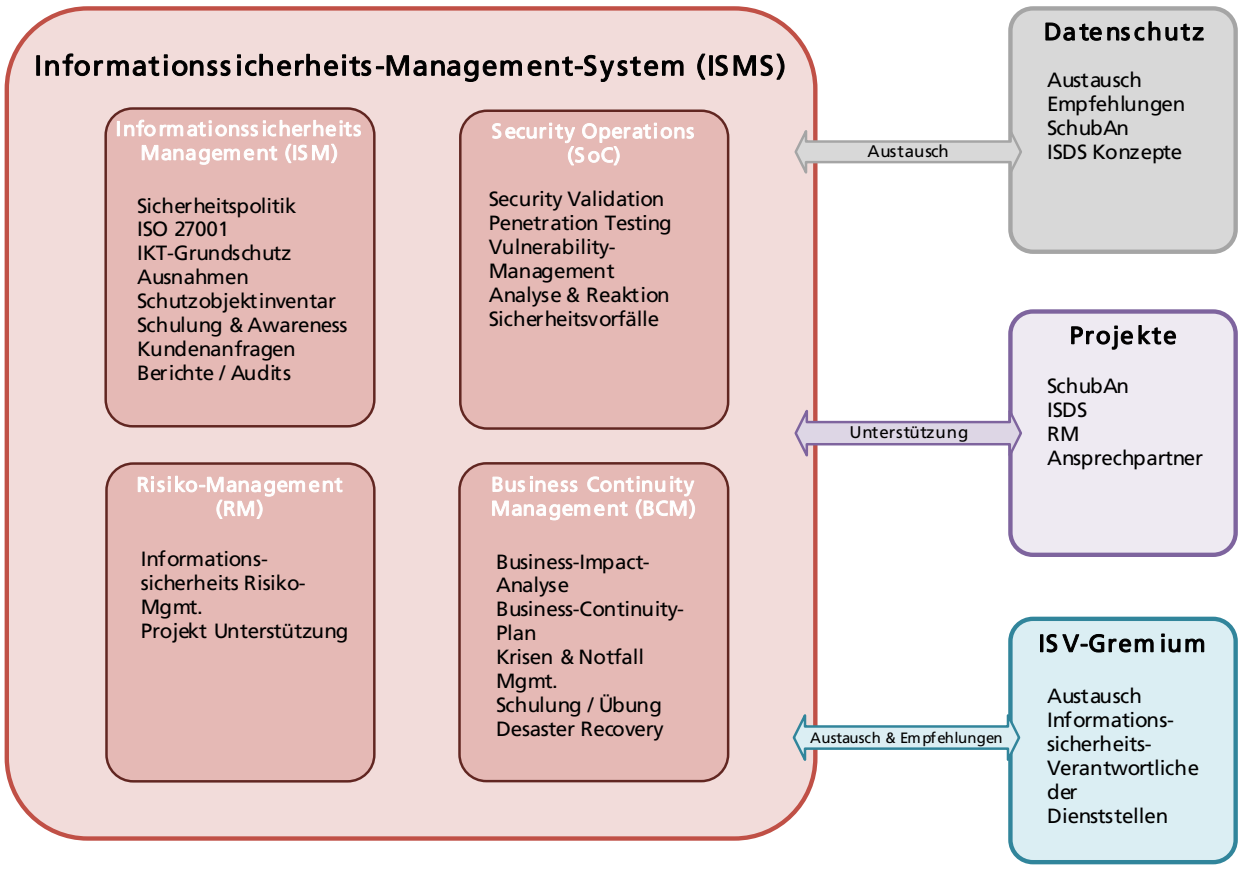

Abbildung 3: ISMS des AIO

4.3 Informationssicherheitsverantwortliche (ISVs)

Die Informationssicherheitsverantwortlichen (ISV) fungieren als zentrale Ansprechperson für alle Fragen zur Informationssicherheit und Business Continuity Management (BCM) innerhalb der Dienststelle. Die ISVs sensibilisieren und unterstützen die Mitarbeitenden der Dienststellen, geben Empfehlungen, sind Bindeglied zum AIO und vertreten die Dienststellen im ISV-Gremium. Sie unterstützen in ihrem Bereich sowohl in täglichen- wie auch in Projektbezogenen Tätigkeiten im Bereich Informationssicherheit.

4.4 ISV-Gremium

Das Gremium der Informationssicherheitsverantwortlichen (ISV), unter der Leitung des AIO, ist das zentrale Organ für den bereichsübergreifenden Austausch und die Koordination der Informationssicherheitsthemen in der kantonalen Verwaltung. Es setzt sich aus Vertretenden des Informationssicherheitsteams des AIO sowie den verantwortlichen Personen der Dienststellen zusammen. Das Gremium fördert die Harmonisierung, behandelt bereichsübergreifende Fragestellungen und unterstützt die Dienststellen in ihrer Aufgabe.

4.5 IKT-Governance

Die Steuerung der Digitalisierungs- sowie der IKT-Strategie der kantonalen Verwaltung ist integraler Bestandteil der IKT-Governance des Kantons Solothurn. Die operative und strategische Führung erfolgt durch die zuständigen Gremien ODI und SDI im Kontext der digitalen Transformation. Strategische übergeordnete Informationssicherheitsthemen werden ebenfalls unter dem Kontext der IKT-Governance verwaltet.

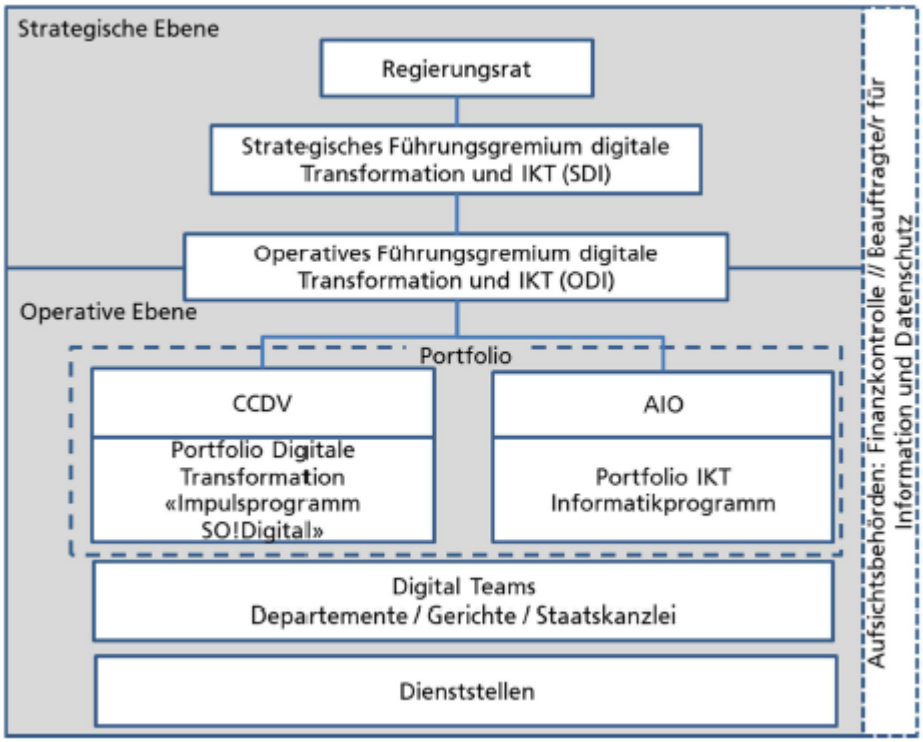

Abbildung 4: Übersicht Governance

5 Schutzbedarf, Risikoanalyse & ISDS-Konzepte

Die Dienststellen bestimmen den Schutzbedarf ihrer Informationen, Daten, Anwendungen und Prozesse. Bei Fragen zur Bestimmung des Schutzbedarfs unterstützen in erster Linie die ISVs. Alle Dienststellen führen auf den Schutzbedarf basierend die erforderlichen Risikoanalysen in enger Abstimmung mit den ISVs und in Zusammenarbeit mit dem AIO durch, wo dieses die Rolle des Betreibers innehat oder wo Schnittstellen von externen Services zu Systemen im AIO vorhanden sind.

Die Ergebnisse von Schutzbedarf und Risikoanalyse dienen als Grundlage für die Auswahl und Umsetzung geeigneter Schutzmassnahmen. Jedes vom AIO betriebene System befindet sich im Kontext des IKT-Grundschutzes des AIOs (mehr dazu im Kapitel 6). Dadurch sind die Schutzmassnahmen des zentralen Informationssicherheits-Managementsystem (ISMS) nach ISO 27001 für diese Services und entsprechende Vorgaben, Prozesse und Hilfsmittel standardmässig sichergestellt. An denen können sich die Dienststellen orientieren.

Wird bei einer Schutzbedarfsanalyse ein erhöhter Schutzbedarf festgelegt, muss in den Sicherheitsanforderungen mit Hilfe der Risikoanalyse geprüft werden, ob die Standardmassnahmen den Anforderungen genügen oder zusätzliche Massnahmen definiert werden müssen. Bei erhöhtem Schutzbedarf wird entsprechend jeweils ein Informationssicherheits- und Datenschutz (ISDS) Konzept erstellt.

Die Verantwortung zur Erstellung von Risikoanalysen und ISDS-Konzepte sowie die Umsetzung der darin definierten Massnahmen liegt bei den jeweiligen Dienststellen mit Hilfe der ISVs. Technische Massnahmen werden durch den Betreiber eines Systems (AIO oder externe Partner) definiert und sichergestellt.

6 IKT-Grundschutz & Ausnahmen

Der IKT-Grundschutz des Kantons Solothurn bildet den verbindlichen Basisschutz für alle zentral durch das AIO betriebenen Anwendungen, Systeme und Services. Er umfasst die minimal erforderlichen organisatorischen und technischen Massnahmen, um die Informationssicherheit angemessen und nachhaltig zu gewährleisten.
Wenn Dienststellen Anwendungen über das AIO betreiben lassen, so fallen diese automatisch unter den IKT-Grundschutz des AIO.

Das AIO ist verantwortlich für die Definition, Pflege, regelmässige Aktualisierung und Umsetzung des IKT-Grundschutzes für die zentral betriebenen Services. Dienststellen sind verantwortlich für die Sicherheit ihrer eigenen Daten, Informationsflüsse und Prozesse, die auf diesen Services laufen, sowie für zusätzliche Schutzmassnahmen, sofern erforderlich. Bei Betrieb von Services durch externe Dritte (Cloud, SaaS etc.) tragen Dienststellen die Gesamtverantwortung für die Sicherstellung der erforderlichen Sicherheit.

Sollen einzelne Anforderungen des Grundschutzes aus organisatorischen, technischen oder wirtschaftlichen Gründen unterschritten werden, gilt dies als Ausnahmefall. Ausnahmen sind schriftlich zu begründen, von der zuständigen Stelle im AIO zu dokumentieren und bedürfen einer formellen Bewilligung durch das AIO. Das AIO verwaltet die Ausnahmen daraufhin und überprüft, beendet oder verlängert diese fortlaufend.

Das ISV-Gremium wirkt bei der Evaluation, Diskussion und Harmonisierung von Grundschutz-Anpassungen in den Bereichen, wo die Zuständigkeit bei Dienststellen ausserhalb des AIO liegt mit und kann Empfehlungen aussprechen.

7 Behandlung von Sicherheitsvorfällen

Sicherheitsvorfälle werden durch die betroffenen Dienststellen oder das AIO erkannt und initial behandelt. Werden diese durch betroffene Dienststellen erkannt, ist der/die jeweilige ISV beizuziehen und bei schwerwiegenden oder bereichsübergreifenden Vorfällen unverzüglich das AIO zu involvieren. Zur Behandlung der Vorfälle im AIO (als Betreiber der Services) gibt es den Security Incident Response Plan (SIRP). Bei Services, welche extern betrieben werden wird ebenfalls das AIO involviert, um mit den entsprechenden Betreibern ein Vorfall zu bearbeiten.

Die strukturierte Nachbearbeitung und Ursachenanalyse erfolgen in Zusammenarbeit zwischen AIO und betroffenen Dienststellen nach definierten Prozessen.

8 Business Continuity Management (BCM)

Jede Dienststelle ist verantwortlich für die Sicherstellung der Fortführung ihrer geschäftskritischen Prozesse und organisatorischen Abläufe. Das AIO verantwortet BCM-Massnahmen für zentrale IKT-Services, welches es betreibt. Abstimmungen erfolgen im Rahmen von Projekten und im ISV-Gremium. Aus Sicht der Dienststelle, betreibt das AIO für die Services ein Service-Continuity Management (SCM) welches den Wiederanlauf und die Zurverfügungstellung der IKT-Services sicherstellt. Die Wiederaufnahme der Geschäftsprozesse bzw. das Sicherstellen der kritischen Prozesse auch im Falle einer Nichtverfügbarkeit von IKT-Services liegt in der Verantwortung der jeweiligen Dienststellen.

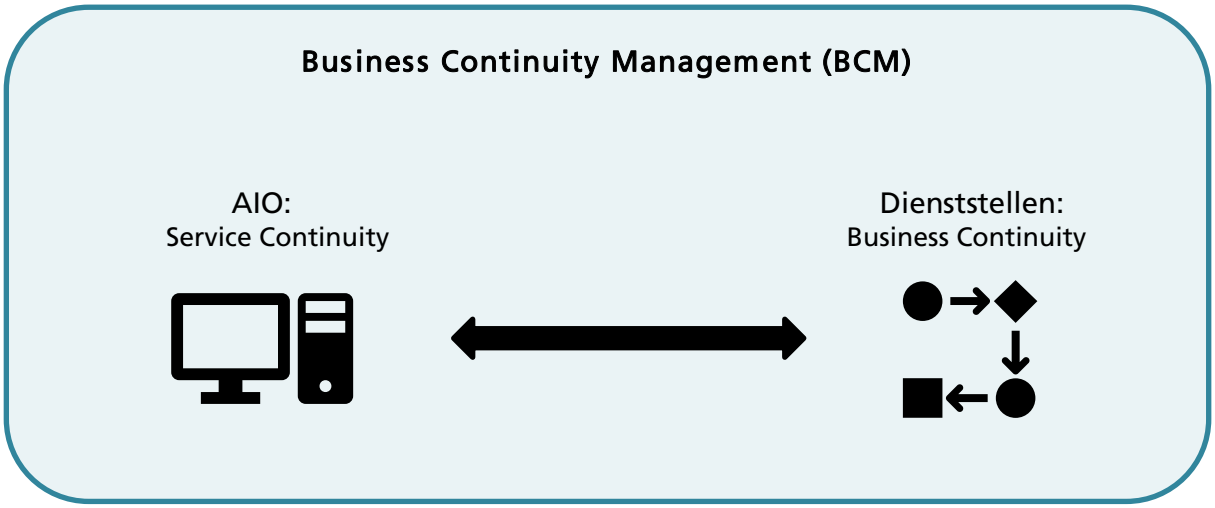

Abbildung 5: Business Continuity Verantwortlichkeiten

9 Kommunikation, Schulung und Awareness

Das AIO organisiert und führt zentrale Awarenesskampagnen und Schulungen für die Mitarbeitenden der Verwaltung durch. Die ISVs unterstützen die Umsetzung in den Dienststellen, beraten Mitarbeitende in Informationssicherheitsfragen und fördern das Bewusstsein für die Sicherheitsanforderungen im Alltag. Regelmässige Informationen, Austauschplattformen und Schulungsangebote sichern die kontinuierliche Sensibilisierung.

10 Kontinuierliche Verbesserung & Audit

Alle Massnahmen der Informationssicherheit werden regelmässig überprüft, bewertet und weiterentwickelt. Interne und externe Audits, die Auswertung von Vorfällen sowie gemeinsame Reviews im ISV-Gremium fördern die nachhaltige Verbesserung der Sicherheitskultur.

11 Referenzen

InfoDG, InfoDV
ISO/IEC 27001:2022
IKT-Strategie Kanton Solothurn
IKT-Governance (ODI/SDI)
AIO IKT-Grundschutz

12 Abbildungsverzeichnis

Abbildung 1: Titelbild 1
Abbildung 2: Strategieübersicht 4
Abbildung 3: ISMS des AIO 5
Abbildung 4: Übersicht Governance 6
Abbildung 5: Business Continuity Verantwortlichkeiten 8