

Projektauftrag

Projektname	Informationssicherheitsmanagementsystem (ISMS) der Verwaltung und der Gerichte des Kantons Solothurn
Autor/-innen	Christof Kramer, Informationssicherheitsbeauftragter ABMH/DBKS a.i. Corinne Felber, Informationssicherheitsverantwortliche und Projektleiterin FD
Auftraggeber-schaft	Regierungsrat und Gerichtsverwaltungscommission (GVK)
Status	genehmigt durch die KoKo am 10.09.2026

Änderungsverzeichnis

Datum	Version	Änderung	Autoren	Reviewer
08.05. – 25.05.2026	0.1 – 0.6	Entwurfsversionen	Corinne Felber Christof Kramer	Samara Ocampo Nathalie Hiemer
26.06.2026	1.0	Finale Version	Corinne Felber Christof Kramer Samara Ocampo Nathalie Hiemer	-
10.09.2026	1.1	Version nach Inputs AIO und KoKo	Samara Ocampo	Nathalie Hiemer Christof Kramer

Inhaltsverzeichnis

Management Summary	2
1 Ausgangslage und Handlungsbedarf	3
2 Projektziele	4
3 Geltungsbereich (Scope) und Abgrenzung	5
4 Rahmenbedingungen und Methodik	5
5 Rechtliche Grundlagen.....	6
6 Projektorganisation und interne Stakeholder	6
7 Vorgehensbeschreibung	7
8 Termine und Meilensteine.....	8
9 Ressourcen und Kosten	9
10 Risikomanagement.....	9
11 Berichtswesen im Projekt.....	10
12 Fachliches ISMS-Berichtswesen	11
13 Freigabe und Genehmigung	11

Management Summary

Die Verwaltung und die Gerichte des Kantons Solothurn bearbeiten im Rahmen ihres Leistungsauftrages Informationen, sei dies in Form von Daten mittels entsprechender (Fach-)Applikationen, in mündlicher oder anderweitig schriftlicher Form (bspw. Bürgerbriefe). Dabei handelt es sich sowohl um (besonders schützenswerte) Personendaten im Sinne des Datenschutzes¹ wie auch um generisch alle anderen Geschäfts- resp. Prozessinformationen (bspw. Medienmitteilungen, Korrespondenz, Finanzdaten). Diese Informationen müssen gemäss ihres Schutzbedarfs geschützt werden. Die Informationssicherheit hat dies als primäre Zielsetzung: Der Schutz von Informationen in ihrer

- Vertraulichkeit,
[Schutz vor unberechtigtem Zugriff (sowohl interne wie externe Zugriffe)]
- Integrität,
[Schutz vor unberechtigter Veränderung/Verfälschung]
- Verfügbarkeit sowie
[Schutz vor unberechtigter Löschung/Vernichtung]
- Nachvollziehbarkeit.
[Schutz vor unberechtigter Verschleierung/Manipulation der Bearbeitungshistorie]

In Anbetracht der fortschreitenden Digitalisierung in der Verwaltung und bei den Gerichten sowie der steigenden Bedrohung durch Cyberrisiken ist ein kantonal übergreifendes Informationssicherheitsmanagementsystem (ISMS) ein zentrales und unabdingbares Instrument zur wirkungsvollen und strukturierten Führung und Steuerung der Informationssicherheit. Es stellt Regeln und Verfahren auf, um Informationssicherheit und Datenschutz dauerhaft zu definieren, zu steuern, zu kontrollieren, aufrechtzuerhalten und fortlaufend zu verbessern. Zur Sicherstellung dieser Vorgaben werden angemessene technische und organisatorische Massnahmen umgesetzt. Ziel ist, eine systematische Basis zu schaffen, um die staatliche Leistungserbringung sowie das Vertrauen der Bevölkerung und Wirtschaft in den Kanton Solothurn dauerhaft zu sichern.

Der vorliegende Projektauftrag formuliert und konkretisiert das Vorhaben zur nachhaltigen Etablierung (Aufbau und Betrieb) eines ISMS, geltend für die Verwaltung und die Gerichte, durch die Arbeitsgruppe ISMS (AG ISMS). Das Projekt bündelt kantonale Ressourcen, nutzt Synergien aus dem bereits bestehenden ISMS der kantonalen Schulen und schafft einen einheitlichen Sicherheitsstandard. Die elementare Grundlage für das Projekt bildet der entsprechende Beschluss des Regierungsrats und der Gerichtsverwaltungscommission.

¹ Datenschutz bezeichnet den Schutz der Persönlichkeit und der Grundrechte von Personen bei der Bearbeitung ihrer Personendaten. Informationssicherheit geht weiter und umfasst den Schutz sämtlicher Informationen – unabhängig davon, ob es sich um Personendaten handelt oder nicht – hinsichtlich ihrer Vertraulichkeit, Integrität, Verfügbarkeit und Nachvollziehbarkeit. Der Datenschutz versteht sich daher als Teil der Informationssicherheit.

1 Ausgangslage und Handlungsbedarf

1.1 Begriffsklärung

Das ISMS schafft eine klare inhaltliche Abgrenzung zwischen «Informationssicherheit» und «Datenschutz», regelt die Zusammenarbeit an den Schnittstellen und nutzt gezielt Synergien. Beim Aufbau und Betrieb des ISMS werden die Anforderungen des Datenschutzes folglich als Teil der Informationssicherheit berücksichtigt. Der Begriff «Informationssicherheit» beinhaltet entsprechend im weiteren Verlauf dieses Dokuments immer auch den Datenschutz.

1.2 Aktuelle Bedrohungslage

Die fortschreitende Digitalisierung – insbesondere getrieben durch E-Government-Dienste, die flächendeckende digitale Aktenführung sowie die zunehmende Vernetzung von Fachanwendungen – hat die Angriffsfläche der kantonalen Informationslandschaft massiv vergrößert. Als kritische Infrastrukturen im Teilsektor «Parlament, Regierung, Justiz, Verwaltung» gemäss der nationalen Strategie zum Schutz kritischer Infrastrukturen (SKI) tragen die Verwaltung und die Gerichte des Kantons Solothurn eine besondere Verantwortung. Der Aufbau eines kantonsweiten ISMS ist die logische Konsequenz, um der steigenden Bedrohungslage angemessen zu begegnen. Sicherheits- und Datenschutzvorfälle gefährden nicht nur interne Prozesse, sondern bedrohen unmittelbar die staatliche Leistungserbringung sowie das Vertrauen von Bevölkerung und Unternehmen in den Rechtsstaat.

1.3 Rechtliche und strategische Grundlagen

Die rechtlichen Vorgaben auf Bundesebene (Informationssicherheitsgesetz [ISG, SR 128] und Verordnung [ISV, SR 128.1]) sowie die Nationale Cyberstrategie (NCS) verpflichten die Kantone – teilweise direkt, teilweise indirekt – zum aktiven Behandeln der Informationssicherheit und der damit verbundenen Risiken. Im Kanton Solothurn bilden das Informations- und Datenschutzgesetz (InfoDG, BGS 114.1), die zugehörige Verordnung (InfoDV, BGS 114.2) sowie das Gesetz über die Auslagerung von Informatikdienstleistungen (AusG, BGS 114.5) den verbindlichen Rahmen.

Die Leitlinie und das Konzept Informationssicherheit des Kantons Solothurn in der Fassung vom 28.04.2026 (RRB Nr. 2026/800 vom 28. April 2026) stellen weitere Grundlagen für das vorliegende Vorhaben dar.

Mit entsprechendem RRB bzw. GVB werden die Grundsätze des Vorhabens festgehalten und die AG ISMS mit der Ausformulierung der Details durch diesen Projektauftrag beauftragt.

1.4 Lehren aus dem Vorfall «Zürcherische Direktion der Justiz und des Innern (JI)»

Der Datensicherheitsvorfall bei der Zürcherischen JI (2002 – 2014)² verdeutlicht die fatalen Folgen struktureller Defizite. Der am 21.11.2025 veröffentlichte Bericht der Parlamentarischen Untersuchungskommission (PUK) stellt ein massives Organisationsversagen fest und enthält insgesamt 50 Empfehlungen zur Behebung systemischer Mängel. Die Kernpunkte der Untersuchung sind:

- Mangelnde Führung: Ungenügende strategische Begleitung und Aufsicht der Informationssicherheit durch den Regierungsrat.

² In den Jahren 2002 bis 2014 ist es dort zu unsachgemässen Entsorgungen von Datenträgern wie Festplatten und USB-Sticks gekommen. Sie enthielten teilweise noch sensitive Daten, die in der Folge an verschiedene Personen im Zürcher Drogen- und Sexmilieu gelangten.

- Isolierte Strukturen: Fehlende kantonale Koordination und ein ausgeprägtes Silo-Denken in den Direktionen.
- Kontrollverlust: Mangelhafte Dokumentation, unzureichende interne Kontrollen und unsachgemässer Umgang mit Datenträgern.
- Fehlendes Bewusstsein: Das Bewusstsein für die Notwendigkeit kantonsweiter, verbindlicher Sicherheitslösungen fehlte über Jahre hinweg.

Diese zentralen Erkenntnisse lassen sich ebenfalls auf den Kanton Solothurn übertragen. Eine zentrale Steuerung der Informationssicherheit und des Datenschutzes fehlt bisher. Dieser Umstand ist, letztendlich im Sinne des Volksauftrages, durch die Etablierung eines ISMS für den Kanton (Verwaltung, Gerichte) zu korrigieren.

1.5 Aktuelle Situation im Kanton Solothurn

Zwar ist das Amt für Informatik und Organisation (AIO) bereits ISO/IEC 27001 (ISMS) zertifiziert, dies deckt jedoch primär die technische Infrastruktur ab (als on-premise³ IKT-Leistungserbringer). Die Verantwortung für die inhaltlichen Geschäftsprozesse und die Etablierung einer Sicherheitskultur verbleibt zwingend bei den einzelnen Dienststellen und Gerichten. Diese setzen Informationssicherheit aktuell allerdings sehr unterschiedlich um. Demzufolge bestehen auch ein unterschiedliches Verständnis zu Umfang, Ausgestaltung, Ziel und Zweck der Informationssicherheit.

2 Projektziele

Das Projekt etabliert einen einheitlichen und systematischen Rahmen für die Informationssicherheit und den Datenschutz, basierend auf drei strategischen Säulen:

Rechtssicherheit und Compliance	Berücksichtigung kantonaler Vorgaben (insbesondere InfoDG, AusG, Leitlinie und Konzept Informationssicherheit) und Bundesvorgaben (ISG, NCS, SKI). Systematische Adressierung der Verantwortung der obersten Führungsebene (Regierungsrat und Gerichtsverwaltungscommission).
Einheitlicher Standard	Schaffung eines kantonal koordinierten, risikobasierten und nutzenbezogenen ISMS mit struktureller Berücksichtigung der zugehörigen Schnittstellen (IKS Internes Kontrollsystem, IRM Integriertes Risikomanagement, ISMS des AIO) und spezifischer Bedürfnisse (Polizei).
Synergien	Transfer und Skalierung von erfolgreich etablierten Konzepten und Verfahren aus den Departementen (bspw. DBKS) auf die kantonale Verwaltung und die Gerichte, um Redundanzen und Kosten zu minimieren.

Methodischer Hinweis: Die Orientierung am internationalen Standard ISO/IEC 27001 (Standard für die Zertifizierung eines ISMS) ist als Referenzrahmen verbindlich. Eine formale Zertifizierung der gesamten Verwaltung und der Gerichte gehört hingegen nicht zum Projektziel.

Die Projektziele werden wie folgt formuliert:

Nr.	Kategorie	Beschreibung	Messgrösse	Priorität
1	Sicherheit, Zuverlässigkeit	Resilienz/Sicherheitsniveau der kantonalen Verwaltung und Gerichte steigern	Anzahl Vorfälle ⁴ zur Informationssicherheit / Jahr	Hoch

³ Daten/Systeme werden in der eigenen Infrastruktur betrieben, nicht extern/cloudbasiert.

⁴ Etablierte IKT-Sicherheitskennzahlen des AIO sind hierbei angemessen zu berücksichtigen.

Nr.	Kategorie	Beschreibung	Messgrösse	Priorität
2	Effektivität, Qualität, Fehlerreduktion	Zentral gesteuertes, überwachtes und messbares ISMS (strategisch, taktisch, operativ) für die kantonale Verwaltung und die Gerichte	Zeitgerecht und nachgewiesen erfolgreich (Nachweis der entsprechenden Verbesserungen inkl. Nutzen) abgeschlossene PDCA ⁵ -Zyklen	Mittel
3	Effizienz, Wirtschaftlichkeit	Synergien-Nutzung durch Integration in bestehende Strukturen und Standardisierungen	Anzahl etablierter, kantonsweit standardisierter Prozesse zur Informationssicherheit (Abdeckungsgrad)	Hoch

3 Geltungsbereich (Scope) und Abgrenzung

Der Geltungsbereich umfasst die gesamte kantonale Verwaltung (Departemente, Staatskanzlei) sowie die Gerichte des Kantons Solothurn. Vom Geltungsbereich ausgenommen sind die Solothurner Spitäler AG, die FHNW, selbständige öffentlich-rechtliche Anstalten und der Informatikeinsatz in Schulen für Unterrichtszwecke.

Abgrenzung gemäss IKT-Grundschutz

Die Verantwortlichkeiten richten sich im Grundsatz nach dem «IKT-Grundschutz Kanton Solothurn», der zwischen Leistungserbringer und Leistungsbezüger differenziert:

- Amt für Informatik und Organisation (AIO): ISO/IEC 27001 zertifiziert, Wissensträger für ISMS sowie Cyber-Sicherheit und damit verantwortlich für den Schutz der IKT-Infrastruktur und die Bereitstellung technischer Sicherheitsdienste.
- Kantonale Verwaltung (Departemente inkl. Staatskanzlei) und Gerichte: Verantwortung für die Informationssicherheit und den Datenschutz innerhalb der Fachprozesse. Dies umfasst die verbindliche Festlegung von Vorgaben zur Informationssicherheit sowie die Sicherstellung der konformen und praktikablen Umsetzung in der Organisation – und somit der Festigung und Verankerung des ISMS in den Dienststellen. Dafür wird im Rahmen dieses Projekts eine anforderungsgerechte Tool-Unterstützung evaluiert und den Dienststellen bereitgestellt. Die Finanzierung der Investition sowie der Betriebskosten ist im Kontext der Tool-Evaluation festzulegen.

4 Rahmenbedingungen und Methodik

Folgende Rahmenbedingungen gelten:

- 1) HERMES: Das Projekt wird analog der kantonalen Projektmethodik HERMES geführt. HERMES bildet den verbindlichen Rahmen für Projektsteuerung, Rollen, Entscheide, Phasenplanung, Reporting und Lieferergebnisse.
- 2) Hybrides Vorgehen: Die Projektsteuerung erfolgt formal nach HERMES. Die Erarbeitung der ISMS-Grundlagen und deren spätere Umsetzung erfolgen jedoch dort, wo es

⁵ PDCA – Plan, Do, Check, Act: Vorgehen resp. Prozess zur Sicherstellung einer kontinuierlichen Verbesserung eines Systems, Prozesses oder einer Organisation. Ziele, Verfahren, Vorhaben werden geplant (Plan), durchgeführt (Do), überprüft (Check) und anschliessend verbessert (Act).

zweckmässig ist, iterativ und ressourcenorientiert. Damit wird ein hybrides Vorgehen gewählt: formale Phasenführung nach HERMES, schrittweise Erarbeitung und Einführung der ISMS-Bausteine in Konzept- und Umsetzungsphase.

- 3) ISO/IEC 27001: Dieser Standard dient als verbindliche methodische Referenz für den Aufbau und Betrieb des ISMS. Eine formelle Zertifizierung ist derzeit kein Ziel.
- 4) Ressourcen- und Risikoorientierung: Massnahmen werden nicht nach dem Prinzip der formalen Vollständigkeit, sondern nach dem konkreten Schutzbedarf und dem identifizierten Risiko priorisiert. Dies stellt sicher, dass Ressourcen dort investiert werden, wo die grösste Wirkung erzielt wird.
- 5) Schnittstellen: Es erfolgt eine enge Abstimmung mit bestehenden Systemen wie dem Integrierten Risikomanagement (IRM), dem Internen Kontrollsystem (IKS) und dem ISMS des AIO.
- 6) Toolunterstützung: Im Rahmen des Projekts wird ein ISMS-Tool beschafft und eingeführt, den vorgegebenen Prozessen folgend (IKT-Teilprojekt zu diesem Vorhaben). Das Tool unterstützt insbesondere die strukturierte Erfassung und Bewirtschaftung von Schutzobjekten, Schutzbedarfen, Risiken, Massnahmen, Verantwortlichkeiten und Informationen für das Berichtswesen.

5 Rechtliche Grundlagen

Es wird auf die entsprechende Rechtsgrundlagenanalyse verwiesen. Das Vorhaben stützt sich primär auf folgende Grundlagen:

- WoV-G (§ 25): Verpflichtung zur Unterhaltung zeitgemässer Führungs- und Organisationsinstrumente
- InfoDG / InfoDV: Pflicht zur Umsetzung angemessener technischer und organisatorischer Massnahmen zum Datenschutz
- Geschäftsreglement der Gerichtsverwaltung: Explizites Vorsehen eines ISMS für die Gerichte
- Leitlinie und Konzept Informationssicherheit: Strategische Vorgaben des Regierungsrats (RRB Nr. 2026/800 vom 28. April 2026)

6 Projektorganisation und interne Stakeholder

Regierungsrat: Strategische Gesamtverantwortung und Genehmigungsinstanz für die Verwaltung

Gerichtsverwaltungscommission (GVK): Strategische Gesamtverantwortung und Genehmigungsinstanz für die Gerichte

Koordinationskommission (KoKo): Übergeordnetes Steuerungs- und Berichterstattungsorgan (Steuerungsausschuss)

Arbeitsgruppe ISMS (AG ISMS): Operative Projektleitung und Erarbeitung der Fachgrundlagen. Die Arbeitsgruppe – bestehend aus Vertreterinnen und Vertretern der internen Stakeholder – setzt sich wie folgt zusammen:

- Informationssicherheitsverantwortliche (ISV) der Departemente, der Staatskanzlei und der Gerichte
- Vertretung des AIO
- Beauftragte/r für Information und Datenschutz (IDSB), beratend (ohne Stimm- und Antragsrecht)

Die operative Projektleitung wird durch die ISV FD wahrgenommen; die Stellvertretung wird bei der Konstitution der Arbeitsgruppe festgelegt.

7 Vorgehensbeschreibung

Das Projekt orientiert sich am HERMES-Phasenmodell. Die klassischen Phasen Realisierung und Einführung werden für dieses Vorhaben zu einer gemeinsamen Umsetzungsphase zusammengefasst. Dadurch kann der Aufbau des kantonal übergeordneten ISMS praxisnah, ressourcenorientiert und schrittweise erfolgen.

7.1 Initialisierung

Die Initialisierungsphase wird mit der Genehmigung des vorliegenden Projektauftrags abgeschlossen. In dieser Phase wurden die wesentlichen Grundlagen für die Projektfreigabe erarbeitet. Dazu gehören insbesondere:

- Rechtsgrundlagenanalyse
- Schutzbedarfsanalyse
- Projektauftrag (Klärung der Grundsätze zu Geltungsbereich, Governance, Rahmenbedingungen und Vorgehen)
- Entwurf Regierungsratsbeschluss

Mit dem Abschluss der Initialisierung und nach entsprechendem Regierungsrats- und Gerichtsverwaltungs-kommissionsbeschluss wird die Grundlage geschaffen, um das Projekt in die Konzeptphase zu überführen.

7.2 Konzept

In der Konzeptphase werden die zentralen Grundlagen für das kantonal übergeordnete ISMS gemeinsam durch die AG ISMS erarbeitet. Die Arbeiten orientieren sich methodisch an ISO/IEC 27001 und werden auf die Bedürfnisse der kantonalen Verwaltung und der Gerichte angepasst. Zusätzlich wird in dieser Phase eine Software (ISMS-Tool) evaluiert und beschafft, um das ISMS sachgerecht betreiben zu können.

Die Konzeptphase umfasst insbesondere folgende Ergebnisse:

- Konkretisierung des Zielbilds für das kantonal übergeordnete ISMS
- Präzisierung des Geltungsbereichs und der Abgrenzungen
- Festlegung des Rollen-, Aufgaben-, Kompetenzen-, Verantwortlichkeits- und Zusammenarbeitsmodells
- Definition der strategischen, taktischen und operativen ISMS-Ebenen: Die strategische Ebene wird zu Beginn durch die AG ISMS ausgearbeitet und durch Regierungsrat und Gerichtsverwaltungs-kommission freigegeben. Die taktische Ebene wird laufend an rechtliche, technische und fachliche Entwicklungen angepasst. Die operative Umsetzung liegt bei den Departementen, der Staatskanzlei und den Gerichten.
- Erarbeitung der Regelwerksstruktur, inkl. der erforderlichen Grundlagendokumente
- Festlegung der Methodik für Schutzobjekte, Schutzbedarfe, Risiken und Massnahmen
- Definition des Berichtswesens und des Eskalationsmodells
- Klärung der Schnittstellen zu IRM, IKS, AIO, IDSB sowie bestehenden kantonalen Vorgaben

- Definition der Anforderungen an das ISMS-Tool, inkl. Klärung der Kosten und Finanzierung
- Vorbereitung und Durchführung der Toolbeschaffung
- Planung der Umsetzungsphase

Die Konzeptphase schafft damit die verbindlichen Grundlagen, welche anschliessend in den Departementen, der Staatskanzlei und den Gerichten angewendet werden.

7.3 Umsetzung

Die Umsetzungsphase umfasst die Realisierung und Einführung des ISMS. Sie erfolgt nicht über einzelne Pilotdienststellen, sondern kantonsweit auf Basis der in der Konzeptphase gemeinsam erarbeiteten Grundlagen.

Die konkrete Aufnahme und Bewirtschaftung von Schutzobjekten, deren Schutzbedarf, Risiken und Massnahmen erfolgt innerhalb der Departemente, der Staatskanzlei und der Gerichte. Die jeweiligen ISVs nehmen dabei eine Schlüsselfunktion ein. Sie wirken einerseits als Mitglieder der AG ISMS an der strategischen Führung und Weiterentwicklung des ISMS mit und koordinieren andererseits die Umsetzung in ihrem Zuständigkeitsbereich.

Die Umsetzungsphase umfasst insbesondere:

- Einführung des ISMS-Tools
- Einrichtung von Rollen, Berechtigungen und Grundstrukturen im Tool
- Schulung und Befähigung der ISVs und weiterer Schlüsselpersonen zum ISMS-Tool und allgemeiner Führung des ISMS-Rahmenwerks
- Aufnahme und Pflege von Schutzobjekten in den Departementen, der Staatskanzlei und den Gerichten
- Durchführung von Schutzbedarfs- und Risikoanalysen gemäss gemeinsamer Methodik
- Erfassung und Nachverfolgung von Massnahmen
- Aufbau eines Berichtswesens durch die Departemente, Staatskanzlei und Gerichte an die AG ISMS
- Aufbau eines Berichtswesens der AG ISMS via KoKo an Regierungsrat und Gerichtsverwaltungskommission
- Bei Bedarf Anpassung der strategischen Vorgaben
- Vorbereitung des Übergangs in den regulären Betrieb inkl. separatem RRB bzw. GVB

Mit Abschluss der Umsetzungsphase wird das ISMS in den regulären Betrieb überführt. Die AG ISMS bleibt weiterhin als strategisches Gremium für die Führung, Weiterentwicklung und Überprüfung des kantonal übergeordneten ISMS zuständig. Auch der Regierungsrat, die Gerichtsverwaltungskommission und die KoKo behalten ihre Rollen, wie unter «Projektorganisation und interne Stakeholder» beschrieben.

8 Termine und Meilensteine

Meilenstein	Termin
Projektfreigabe durch Regierungsrat und Gerichtsverwaltungskommission, inkl. RRB und GVB	September 2026 (RRB) / Oktober 2026 (GVB)
Projektstart	November 2026

Meilenstein	Termin
Abschluss Konzeptphase	Q2 2027
Evaluation und Einführung ISMS-Tool	separate Planung
Umsetzungsphase (inkludiert die Aufnahme des operativen Betriebs des ISMS) in den Departementen, der Staatskanzlei und den Gerichten, durch die AG ISMS begleitet. Die Leitung, Planung und Durchführung der ISMS-Umsetzung hat im vorgegebenen Zeitrahmen in Verantwortung des ISV zu erfolgen.	ab Q3 2027 bis Q1 2029
Projektabschluss	Q1 2029

9 Ressourcen und Kosten

Für die Durchführung des Projekts sind folgende Ressourcen budgetiert:

Personalaufwand

Die Projektarbeiten erfolgen durch die AG ISMS bzw. deren Mitglieder unter Beizug weiterer Personen (intern/extern) im Rahmen ihres heutigen Aufgaben- und Verantwortungsbereiches. Die Planung (inkl. Ressourcenplanung) obliegt der AG ISMS und wird gemäss obgenanntem Zeitplan koordiniert und festgelegt. Gemäss Schätzung liegt der Stellenprozentaufwand in der Konzeptphase bei 40–50 % und steigt in der Umsetzungsphase weiter an. Der effektive Aufwand kann sich im Zuge des Projekts volatil entwickeln. Die Departemente, die Staatskanzlei sowie die Gerichte haben die Verfügbarkeit dieser Ressourcen sicherzustellen.

Die Einführung des ISMS in den Departementen, der Staatskanzlei und den Gerichten erfolgt unter der Leitung und Verantwortung des jeweiligen ISVs.

Kosten (CHF)

Phase	Geplante Kosten (ohne MwSt.)
Initialisierung	CHF 10'000
Konzept	Es erfolgt eine Evaluation des begleitenden Dienstleisters, im Einladungsverfahren (Kostendach maximal CHF 250'000). Kostenteilung auf die Departemente, die Staatskanzlei sowie die Gerichte gemäss separatem RRB bzw. GVB
ISMS-Tool	Teilprojekt (Vorhabensantrag ODI), separate Ausweisung der Kosten
Umsetzung	Die Einführung und der Betrieb des ISMS in den Departementen, der Staatskanzlei und den Gerichten erfolgt unter der Leitung und Verantwortung des jeweiligen ISVs.

10 Risikomanagement

Die Bewertung der Risiken erfolgt nach dem Schema Wahrscheinlichkeit (W) x Auswirkung (A).

Risiko	W	A	Massnahme
fehlendes Wahrnehmen der Verantwortung und somit feh-	H	H	explizites Mandat des Regierungsrates und der GVK; regelmässige Berichterstattung

Risiko	W	A	Massnahme
lende Unterstützung des Vorhabens auf oberster Führungsebene			
unzureichende Ressourcen AG ISMS (Fachpersonal nicht vorhanden oder keine Kapazitäten)	M	H	frühzeitige Abstimmung; ggf. Anpassung des Projektzeitplans
Widerstand gegen übergeordnete, einheitliche und verbindliche Vorgaben	M	M	Einbezug der internen Stakeholder von Beginn an; klare Kommunikation des Nutzens der Bündelung und der vorhandenen Spielräume sowie der Risiken und Folgen bei fehlenden übergeordneten, einheitlichen und verbindlichen Vorgaben
unklare politische Trägerschaft nach Wechsel der obersten Führungsebene oder Umstrukturierung	T	H	formeller RRB und GVB als Projektgrundlage; Verankerung in den kantonalen Grundlagen
zu breiter Geltungsbereich (Scope) von Beginn an	M	M	konsequentes Scope-Management im Projekt; ggf. mit stufenweisem Ausbau
Personalausfälle bei internen und externen Schlüsselrollen	T	H	Stellvertretungsregelungen; Wissenstransfer sicherstellen
Verzögerungen durch konkurrierende Projekte und Priorisierungskonflikte	M	M	explizite Priorisierung durch Regierungsrat und GVK

W = Wahrscheinlichkeit, A = Auswirkung / H = hoch, M = mittel, T = tief

Sämtliche Risiken führen bei Eintritt letztendlich zu einer fehlenden oder verzögerten Umsetzung des ISMS. Dies kann zu einem kantonsweiten Schaden resp. einer Beeinträchtigung der Schutzziele führen.

11 Berichtswesen im Projekt

Während des Projekts rapportiert die AG ISMS an die KoKo als Steuerungsausschuss. Die KoKo nimmt die Berichterstattung entgegen, entscheidet über wesentliche Richtungsfragen und bereitet bei Bedarf Entscheide zuhanden des Regierungsrats und der Gerichtsverwaltungskommission vor. Die Projekt-Berichterstattung umfasst insbesondere:

- Projektstatus
- Fortschritt je Phase
- wesentliche Ergebnisse
- Risiken und Massnahmen
- Ressourcen- und Kostenentwicklung
- Abhängigkeiten und Entscheidbedarf
- Eskalationen

12 Fachliches ISMS-Berichtswesen

In der Konzept- und insbesondere in der Umsetzungsphase rapportieren die Departemente, die Staatskanzlei und die Gerichte über ihre ISVs an die AG ISMS. Diese Berichterstattung umfasst insbesondere:

- Stand der Aufnahme von Schutzobjekten
- Stand der Schutzbedarfs- und Risikoanalysen
- wesentliche Risiken
- geplante und laufende Massnahmen
- Umsetzungsfortschritt
- offene Punkte und Unterstützungsbedarf
- Erkenntnisse für die Weiterentwicklung des ISMS

Die AG ISMS konsolidiert diese Informationen und bereitet sie für die Projektsteuerung bzw. später für den regulären Betrieb auf.

13 Freigabe und Genehmigung

Mit der Genehmigung des vorliegenden Projektauftrags sowie mit entsprechendem Regierungsrats- und Gerichtsverwaltungscommissionsbeschluss wird die Initialisierungsphase abgeschlossen und das Projekt zur Durchführung der Konzept- und Umsetzungsphase freigegeben.

Die Genehmigung umfasst insbesondere:

- Bestätigung des Geltungsbereichs
- Bestätigung des Vorgehens nach HERMES mit hybrider Lösungsentstehung
- Einsetzung der KoKo als Projektausschuss im Auftrag von Regierungsrat und Gerichtsverwaltungscommission
- Bestätigung der AG ISMS als strategisches Projektgremium
- entsprechender RRB und GVB
- Freigabe zur Erarbeitung der ISMS-Grundlagen nach ISO/IEC 27001
- Freigabe zur Vorbereitung des Teilprojekts zur Evaluation, Beschaffung und Einführung eines ISMS-Tools
- Auftrag an Departemente, Staatskanzlei und Gerichte, die Umsetzung in ihrem Zuständigkeitsbereich über die ISVs sicherzustellen und an die AG ISMS zu rapportieren