Kanton Zürich
Regierungsrat

Allgemeine Informationssicherheits-richtlinie (AISR)

des Regierungsrates für die kantonale Verwaltung

16. April 2025

Abkürzungen

Abkürzung	Beschreibung
AFI	Amt für Informatik
AISR	Allgemeine Informationssicherheitsrichtlinie
BISR	Besondere Informationssicherheitsrichtlinie
CISC	Kantonales Zentrum für Informationssicherheit (ehemals: CCSC)
CSIRT	Computer Security Incident Response Team
DIR	Direktionen
DSB	Datenschutzbeauftragte/r des Kantons Zürich
DSMS	Datenschutz-Managementsystem
FAGIS	Fachgruppe Informationssicherheit
IIA	Institute of Internal Auditors
IKT	Informations- und Kommunikationstechnologie
IntRM	Integrales Risikomanagement
ISID	Informationssicherheitsbeauftragte/r der Direktion oder Staatskanzlei
ISIK	Informationssicherheitsbeauftragte/r des Kantons Zürich
ISMS	Informationssicherheits-Managementsystem
ISSE	Informationssicherheitsservices
ISST	Informationssicherheitsstandards
Kapo	Kantonspolizei
KFO	Kantonale Führungsorganisation
KGC	Kerngruppe Cyber
RFC	Request for Comments
RRZ	Legislaturziele des Regierungsrates
RRB	Regierungsratsbeschluss
SDI	Gremium Steuerung Digitale Verwaltung und IKT
SK	Staatskanzlei

Hinweis: Die Direktionsvorsteherin bzw. der Direktionsvorsteher und die Staatsschreiberin bzw. der Staatsschreiber werden im vorliegenden Dokument unter dem Begriff «Direktionsvorstehende» zusammengefasst.

Inhaltsverzeichnis

1. Einleitung

Die Bedeutung der Informationssicherheit für den Kanton Zürich ist in der kantonalen Cybersicherheitsstrategie (RRB Nr. 676/2022) festgehalten. Gemäss dieser gestaltet und stärkt der Kanton Zürich zusammen mit Bund, Kantonen, Gemeinden und weiteren Partnern die Widerstandsfähigkeit gegenüber Informationssicherheitsrisiken zum Nutzen der Bevölkerung, der Wirtschaft und der eigenen Mitarbeitenden.

Die digitale Transformation als strategischer Schwerpunkt des Regierungsrates setzt Informationssicherheit voraus. Investitionen in die Informationssicherheit sichern die Zukunftsfähigkeit und stärken den Kanton Zürich als qualifizierten und verlässlichen Partner auch in der digitalen Welt.

Deshalb verfolgt der Regierungsrat das Ziel, die Informationssicherheit adäquat und nachhaltig in die Verwaltungsprozesse zu integrieren. Diese Massnahme ist in den Richtlinien der Regierungspolitik 2023–2027 festgehalten (RRB Nr. 871/2023, siehe Legislaturziel und Massnahme RRZ 10g) und soll das Vertrauen in den Staat stärken.

Dabei ist auch der Grundsatz der Wirtschaftlichkeit zu beachten, gemäss dem der Aufwand für Informationssicherheitsmassnahmen in einem angemessenen Nutzen-Aufwand-Verhältnis zu den damit verbundenen Risiken und zur Risikobereitschaft des Kantons bzw. der Direktionen und der Staatskanzlei stehen muss (vgl. Kapitel 3).

Allgemeine Informationssicherheitsrichtlinie

Die vorliegende Allgemeine Informationssicherheitsrichtlinie (AISR) legt den Geltungsbereich der kantonalen Vorgaben, die Ziele und Grundsätze der Informationssicherheit sowie die direktionsübergreifenden Strukturen und Anforderungen fest, die für den Schutz der Informationen und der damit verbundenen Werte in der kantonalen Verwaltung erforderlich sind.

Es handelt sich um eine überarbeitete und auf die aktuelle Bedrohungslage, Legislaturziele (RRB Nr. 871/2023), Cybersicherheitsstrategie (RRB Nr. 676/2022) und Normen ausgerichtete Fassung der 2019 erlassenen AISR (RRB Nr. 795/2019).

Mit dem Erlass der AISR bekräftigt der Regierungsrat seine Verantwortung für die Gewährleistung der Informationssicherheit in der kantonalen Verwaltung und trägt den veränderten Herausforderungen Rechnung.

2. Allgemeines

Die AISR ist eine verbindliche Weisung des Regierungsrates.

2.1 Geltungsbereich

Diese Richtlinie ist die übergeordnete Informationssicherheitsrichtlinie für die kantonale Verwaltung. Der Geltungsbereich umfasst insbesondere alle in der Verantwortung der Direktionen bzw. der Staatskanzlei befindlichen Strukturen, Prozesse, Technologien und Werte (einschliesslich Informationen und Personen).

2.2 Verpflichtung Dritter

Das Bearbeiten von Informationen des Kantons und der Zugriff auf Informatikmittel des Kantons ist Dritten (einschliesslich den übrigen öffentlichen Organen) nur unter der Bedingung erlaubt, dass sie die massgeblichen Vorgaben dieser Richtlinie einhalten oder eine mindestens gleichwertige Informationssicherheit gewährleisten.

2.3 Rechtsgrundlagen

Die Umsetzung der Informationssicherheit in den Direktionen und der Staatskanzlei richtet sich nach den folgenden Gesetzen, Verordnungen und Beschlüssen:

- Bundesgesetz über die Informationssicherheit beim Bund (ISG, SR 128)
- Gesetz über die Organisation des Regierungsrates und der kantonalen Verwaltung (OG RR, LS 172.1)
- Verordnung über die Organisation des Regierungsrates und der kantonalen Verwaltung (VOG RR, LS 172.11)
- Gesetz über die Information und den Datenschutz (IDG, LS 170.4)
- Verordnung über die Information und den Datenschutz (IDV, LS 170.41)
- Verordnung über die Informationsverwaltung und -sicherheit (IVSV)
- Richtlinien der Regierungspolitik 2023–2027 (RRB Nr. 871/2023)
- Kantonale Cybersicherheitsstrategie des Kantons Zürich (RRB Nr. 676/2022)
- Rahmenverträge für den Expertenpool Informationssicherheit (RRB Nr. 811/2021)
- Informationssicherheit, Umsetzung in den Direktionen und der Staatskanzlei (RRB Nr. 1193/2020)
- Kantonale IKT-Strategie (RRB Nr. 383/2018)

2.3.1 Gesetze und Verordnungen

Die Direktionsvorstehenden regeln die Grundsätze der Organisation und der Geschäftsordnung der Direktion, einschliesslich der zur Umsetzung des IDG erforderlichen Regelungen (§ 60 Abs. 1 VOG RR).

Die öffentlichen Organe stellen sicher, dass ihre Verwaltungseinheiten das IDG und die IVSV einhalten. Sie erlassen hierzu Ordnungsvorschriften und schützen Informationen durch angemessene organisatorische und technische Massnahmen.

Das öffentliche Organ bestimmt eine federführende Stelle (Dossiers, § 4 IVSV). Diese beurteilt die Risiken und den Schutzbedarf für die von ihr verwalteten Informationen. Gestützt darauf legt das öffentliche Organ angemessene Massnahmen zum Schutz fest und gibt die Wirkung, die Kosten und die Termine an (§ 12 Abs. 2 IVSV).

Diese Massnahmen richten sich nach der Art der Information, nach Art und Zweck der Bearbeitung, nach dem jeweiligen Stand der Technik (§ 7 Abs. 3 IDG) und den folgenden Schutzzielen:

- **Vertraulichkeit:** Informationen dürfen nicht unrechtmässig zur Kenntnis gelangen (§ 7 Abs. 2. lit. a IDG; § 13 lit. a IVSV)
- **Unversehrtheit** («Integrität»)**:** Informationen müssen richtig und vollständig sein (§ 7 Abs. 2 lit. b IDG; § 13 lit. b IVSV)
- **Verfügbarkeit:** Informationen müssen bei Bedarf vorhanden sein (§ 7 Abs. 2 lit. c IDG; § 13 lit. c IVSV)
- **Zurechenbarkeit**: Informationsbearbeitungen müssen einer Person zugerechnet werden können (§ 7 Abs. 2 lit. d IDG; § 13 lit. d IVSV)
- **Nachvollziehbarkeit:** Veränderungen von Informationen müssen erkennbar und nachvollziehbar sein (§ 7 Abs. 2 lit. e IDG; § 13 lit. e IVSV)

Die öffentlichen Organe prüfen regelmässig die Einhaltung der Vorgaben des IDG und der IVSV sowie die Zweckmässigkeit der getroffenen Massnahmen zum Schutz der Informationen. Werden die Schutzziele gemäss § 7 Abs. 2 IDG nicht erreicht, passt es die Massnahmen an (§ 14 Abs. 2 IVSV).

Zur Sicherstellung der Qualität kann das öffentliche Organ die Umsetzung der Informationssicherheit durch eine unabhängige und anerkannte Stelle prüfen und bewerten lassen (§ 13 Abs. 2 IDG).

Die Ergebnisse der Überprüfungen und Anpassungen der Massnahmen sind durch das öffentliche Organ zu dokumentieren (§ 14 Abs. 3 IVSV).

2.3.2 Beschlüsse des Regierungsrates

Mit der AISR präzisiert der Regierungsrat die Umsetzung der erlassenen Gesetze und Verordnungen zur Informationssicherheit und legt kantonale Strukturen und Anforderungen für die Direktionen und die Staatskanzlei fest.

Ergänzend unterstützt der Regierungsrat mit der kantonalen Cybersicherheitsstrategie (RRB Nr. 676/2022) sein Legislaturziel (RRZ 10g, 2023–2027, RRB Nr. 871/2023: «Die Cybersicherheitsstrategie umsetzen … und die Informationssicherheit in die Verwaltungsprozesse integrieren.») durch den Aufbau kantonaler Informationssicherheitsservices.

Der Regierungsrat unterstützt die Umsetzung der Informationssicherheit zusätzlich mit den im Rahmen der Beschlüsse Nrn. 1193/2020 und 811/2021 bewilligten finanziellen Mitteln.

Die genannten Regierungsratsbeschlüsse gewährleisten einheitliche Anforderungen für alle Direktionen und die Staatskanzlei, fördern die direktionsübergreifende Zusammenarbeit und erleichtern die direktionsinterne Umsetzung der Informationssicherheit. Unabhängig davon verbleibt die Verantwortung für die Umsetzung und Einhaltung der Informationssicherheit bei den einzelnen Direktionen und der Staatskanzlei (§ 60 Abs. 1 VOG RR, § 7 Abs. 1 IDG, § 14 Abs. 1 IVSV).

2.4 Inhalte

Die AISR legt Folgendes fest:

- **Grundsätze** der Informationssicherheit in der kantonalen Verwaltung (Kapitel 3)
- Abgestuftes **Modell:** Gemeinsame Basis, individuelle Umsetzung (Kapitel 4)
- Betrieb des **ISMS** in der jeweiligen Direktion und der Staatskanzlei (Kapitel 5)
- **Beurteilung** der Wirksamkeit: Metriken, Prüfungen, Berichte (Kapitel 6)
- **Kantonale Organisationsstrukturen** und Verantwortlichkeiten (Kapitel 7)
- **Schnittstellen** zu weiteren Fachthemen (Kapitel 8)

3. Grundsätze der Informationssicherheit

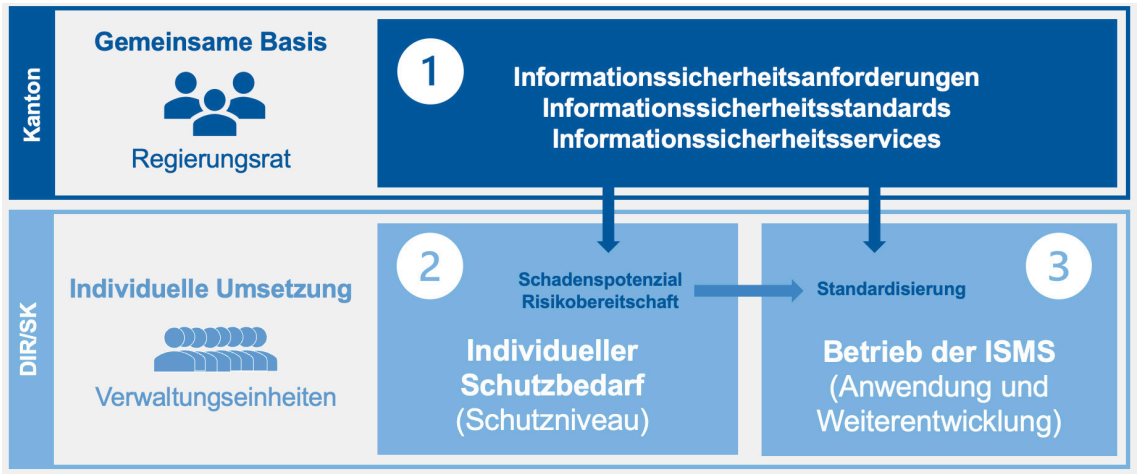
In der kantonalen Verwaltung gelten die folgenden Informationssicherheitsgrundsätze:

- **Rechtmässigkeit:** Gesetzliche und vertragliche Vorschriften werden eingehalten.
- **Schutz:** Alle Informationen, unabhängig ihrer Form (z.B. digital oder physisch), sind durch die verantwortlichen Stellen über ihren gesamten Lebenszyklus hinweg angemessen zu schützen (Vertraulichkeit, Integrität, Verfügbarkeit, Zurechenbarkeit, Nachvollziehbarkeit).
- **Normierung:** Die Informationssicherheit der kantonalen Verwaltung stützt sich auf den aktuellen Stand der ISO/IEC-27000-Normreihe, gängigen Industriestandards (OWASP usw.) und verfügbaren Best Practices (IIA, ISACA usw.) ab.
- **Managementsystem:** Jede Direktion und die Staatskanzlei setzt zusammen mit ihren Verwaltungseinheiten ein angemessenes und wirksames ISMS eigenverantwortlich um.
- **Ausrichtung:** Die Informationssicherheit ist auf die Richtlinien der Regierungspolitik und die Legislaturziele des Regierungsrates ausgerichtet und innerhalb der kantonalen Verwaltung abgestimmt.
- **Befähigung:** Führungsorgane befähigen (mit Kenntnissen und Mitteln) ihre Verwaltungseinheiten in Bezug auf die Informationssicherheit und beauftragen sie mit der angemessenen und wirksamen Umsetzung der Anforderungen.
- **Funktionstrennung:** Aufgaben und Verantwortlichkeiten werden ausreichend getrennt, um potenzielle Interessenkonflikte zu vermeiden.
- **Förmlichkeit:** Aufgaben, Kompetenzen und Verantwortlichkeiten sind eindeutig festgelegt. Informationssicherheitsmassnahmen werden formell geplant und plangemäss umgesetzt.
- **Wirtschaftlichkeit:** Der Aufwand für Informationssicherheitsmassnahmen steht in einem angemessenen Nutzen-Aufwand-Verhältnis zu den damit verbundenen Risiken und zur Risikobereitschaft des Kantons bzw. der Direktionen und der Staatskanzlei.
- **Zusammenarbeit:** Die Umsetzung der Informationssicherheit ist eine Gemeinschaftsaufgabe der kantonalen Verwaltung. Durch übergreifende Strukturen und einen regelmässigen Austausch werden Synergien genutzt.
- **Einbindung:** Die Informationssicherheit wird angemessen in den Verwaltungsstrukturen, Verwaltungsprozessen und Infrastrukturen verankert.
- **Austausch:** Die Verantwortlichen pflegen einen funktions- und stufengerechten Erfahrungsaustausch innerhalb des Kantons Zürich, mit anderen Kantonen, mit dem Bund und mit Interessen- und Berufsverbänden sowie in spezialisierten Foren.
- **Auswertung:** Die Angemessenheit und Wirksamkeit der Informationssicherheit wird regelmässig überprüft und verbessert.

4. Kantonales Modell

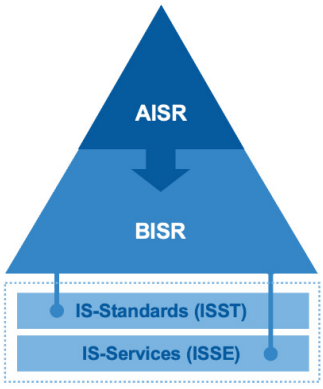
4.1 Zweistufiger Governance-Ansatz

Für die Ausgestaltung der Informationssicherheit ist dem mehrstufigen Aufbau des Kantons Zürich sowie den Besonderheiten der einzelnen Direktion und der Staatskanzlei Rechnung zu tragen. Damit wird sichergestellt, dass die Governance- und Management-Strukturen einen nachhaltigen, d.h., angemessenen und wirksamen Schutz gewährleisten. Deshalb wird ein zweistufiger Ansatz verfolgt, der Synergien nutzt, die Zusammenarbeit fördert, ein durchgängiges Sicherheitsniveau sicherstellt und gleichzeitig die Autonomie und Handlungsfähigkeit der Direktionen und der Staatskanzlei bei der individuellen Umsetzung gewährleistet.



4.2 Gemeinsame Basis

Der Regierungsrat legt die Anforderungen an die Informationssicherheit und die Strukturen der Zusammenarbeit fest. Ergänzend werden von und für die Verwaltungseinheiten kantonale Informationssicherheitsservices bereitgestellt. Seine steuernde Funktion nimmt der Regierungsrat mit dem kantonalen Regelwerk wahr, das den gleichen Geltungsbereich wie diese Richtlinie abdeckt (vgl. Kapitel 2.1) und auf folgenden Elementen aufbaut:



Allgemeine Informationssicherheitsrichtlinie
Die AISR legt die Rahmenbedingungen für die Informationssicherheit, den Aufbau der kantonalen Anforderungen sowie der organisatorischen Strukturen auf kantonaler Stufe fest.

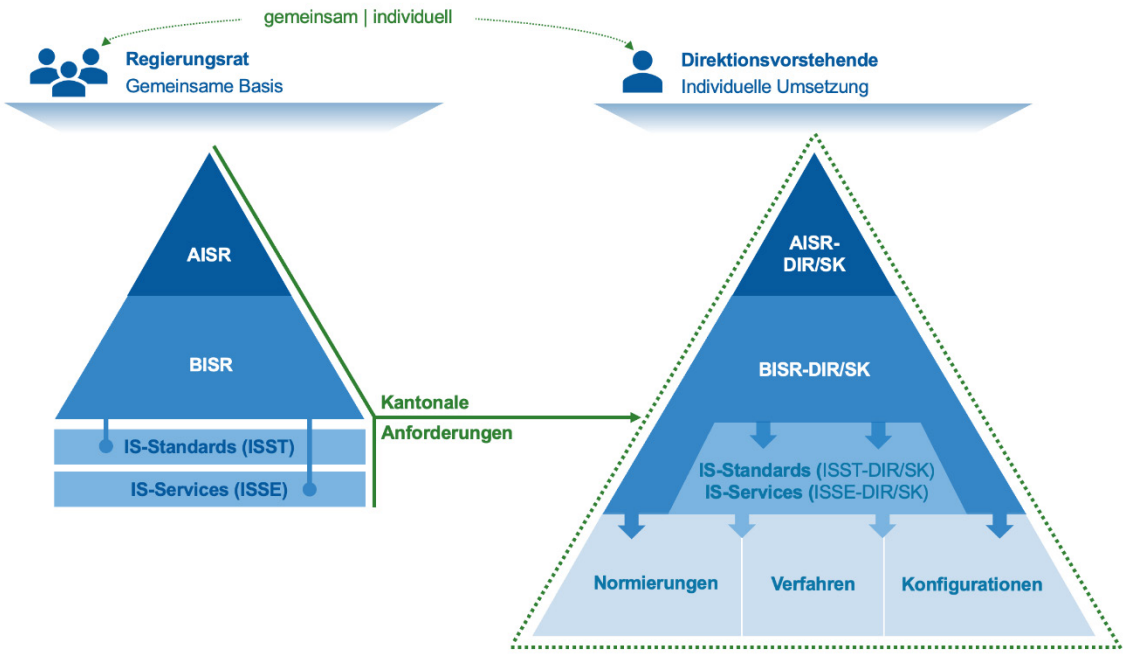
Besondere Informationssicherheitsrichtlinien (BISR)
Die BISR legen die kantonalen Anforderungen («Was») an die Informationssicherheit gestützt auf die Umsetzungshinweise der ISO/IEC-27002-Norm sowie die kantonal bereitgestellten Informationssicherheitsstandards und -services fest.

Kantonale Informationssicherheitsstandards (ISST)
Unter Berücksichtigung stark verzahnter Themenfelder oder besonderer Bedrohungslagen können für alle Verwaltungseinheiten verpflichtende Standards («Wie», «Wer») definiert werden, welche die Umsetzung der BISR regeln.

Kantonale Informationssicherheitsservices (ISSE)
Bereitgestellte Services sollen die Direktionen und die Staatskanzlei bei der Umsetzung der kantonalen Anforderungen in Bezug auf die Informationssicherheit unterstützen.

4.3 Individuelle Umsetzung

Die Umsetzung der Informationssicherheit im Einklang mit der gemeinsamen Basis (kantonales Regelwerk: AISR, BISR, ISST, ISSE) sowie den spezifischen Schutzbedarfsanforderungen innerhalb der Verwaltungseinheiten erfolgt in den Direktionen und der Staatskanzlei. Hierzu muss das kantonale Regelwerk auf den individuellen Bedarf ausgerichtet werden.



Die Ausgestaltung der jeweiligen Weisungsstrukturen (Regelwerke der Direktionen oder Staatskanzlei) erfolgt im Auftrag der Direktionsvorstehenden.

- **AISR der Direktionen und der Staatskanzlei (AISR-DIR/SK)**
  Analog und unter Berücksichtigung der kantonalen AISR, werden hiermit die individuellen Informationssicherheitsziele, -anforderungen, -strukturen und -prozesse der jeweiligen Direktion bzw. der Staatskanzlei festgelegt.
- **BISR der Direktionen und der Staatskanzlei (BISR-DIR/SK)**
  Die Direktionen und die Staatskanzlei können optional die kantonalen BISR verschärfen und präzisieren. Die Einhaltung anwendbarer (ISO/IEC-27001:2022-Klausel 6.1.3d) kantonaler Anforderungen muss gewährleistet sein.
- **ISST und ISSE der Direktionen und der Staatskanzlei (ISST/E-DIR/SK)**
  Unter Berücksichtigung der gemeinsamen Basis liegt es in der Verantwortung der Direktionen bzw. der Staatskanzlei, zweckmässige Standards und Services auszugestalten, die eine nachhaltige, angemessene und wirksame Operationalisierung der Informationssicherheit in ihrem Verantwortungsbereich ermöglichen.
- **Normierungen, Verfahren, Konfigurationen**
  Es handelt sich um Schritt-für-Schritt-Anleitungen oder spezifische Standards, Normen, Protokolle, Werte usw., welche die Operationalisierung unterstützen können.

Technische Rahmenbedingungen: Bei der Ausgestaltung der Weisungsstrukturen bzw. der Umsetzung von Informationssicherheitsmassnahmen sind die massgeblichen Zuständigkeiten und die damit verbundenen Steuerungsprozesse zu berücksichtigen (vgl. z.B. RRB Nr. 383/2018, IKT-Strategie).

Abgesehen von den Anforderungen in der gemeinsamen Basis (kantonales Regelwerk, siehe Kapitel 4.2) und unter Berücksichtigung der technischen Rahmenbedingungen sind die Direktionen und die Staatskanzlei frei in der Ausgestaltung der operativen Umsetzung. Dies umfasst auch die Entscheidung, ob die Umsetzung der Informationssicherheit in den Verwaltungseinheiten mit einem einheitlichen zentralen oder einem individuellen dezentralen Ansatz erfolgen soll. Eine solche Entscheidung kann:

- von der Grösse der Ämter,
- der Kritikalität der Verwaltungsprozesse oder
- der Komplexität der Strukturen

abhängen und sowohl einzelne Verwaltungseinheiten als auch spezifische Teilbereiche betreffen.

4.4 Ausgestaltung des Regelwerks

Um die Informationssicherheit fortlaufend zu gewährleisten, muss das Regelwerk regelmässig an die aktuellen Bedürfnisse der kantonalen Verwaltung angepasst werden (kontinuierlicher Verbesserungsprozess).

Kantonales Regelwerk | Gemeinsame Basis
Für die fortlaufende Überprüfung, Erarbeitung, Beantragung und den Erlass der kantonalen Regelungen gelten die folgenden Zeiträume und Zuständigkeiten:

- **Allgemeine Informationssicherheitsrichtlinie**
  Die AISR wird regelmässig (mindestens alle vier Jahre) durch die oder den ISIK auf ihre Angemessenheit überprüft, bei Bedarf unter Einbezug der relevanten Gremien und Fachgruppen überarbeitet und auf Antrag der Finanzdirektion und unter Vorberatung durch das SDI vom Regierungsrat erlassen.
- **Besondere Informationssicherheitsrichtlinien**
  Die BISR werden regelmässig (mindestens alle zwei Jahre) durch die oder den ISIK auf ihre Angemessenheit überprüft, bei Bedarf unter Einbezug der relevanten Fachgruppen überarbeitet und auf Antrag der FAGIS vom SDI erlassen.
- **Kantonale Informationssicherheitsstandards**
  Die kantonalen Informationssicherheitsstandards werden durch Fachgruppen erstellt, regelmässig (mindestens alle zwei Jahre) durch die oder den ISIK auf deren Angemessenheit überprüft, bei Bedarf überarbeitet und von den relevanten Gremien erlassen.

Regelwerk der Direktionen oder Staatskanzlei | Individuelle Umsetzung
Die Zuständigkeiten für das Regelwerk der Direktionen und der Staatskanzlei werden von den Direktionsvorstehenden erlassen und in der AISR-DIR/SK festgehalten. Die Angemessenheitsprüfung der jeweiligen Regelwerke wird analog zum kantonalen Regelwerk durchgeführt (AISR-DIR/SK analog zu AISR, BISR-DIR/SK analog zu BISR, ISST-DIR/SK analog zu ISST). Normierungen, Verfahren und Konfigurationen der Direktionen und der Staatskanzlei sind ebenfalls regelmässig (mindestens alle zwei Jahre) zu prüfen und bei Bedarf anzupassen.

Kommunikation des Regelwerks
Die Richtlinien (AISR-DIR/SK und BISR-DIR/SK) werden zielgruppengerecht den Mitarbeitenden der kantonalen Verwaltung elektronisch mitgeteilt und im Intranet publiziert. Die Mitteilung wird jeweils von der Direktion bzw. Staatskanzlei veranlasst, der die Stelle angehört, welche die Dokumente erlassen hat. Im Bereich des kantonalen Regelwerks erfolgt sie durch die oder den ISIK.

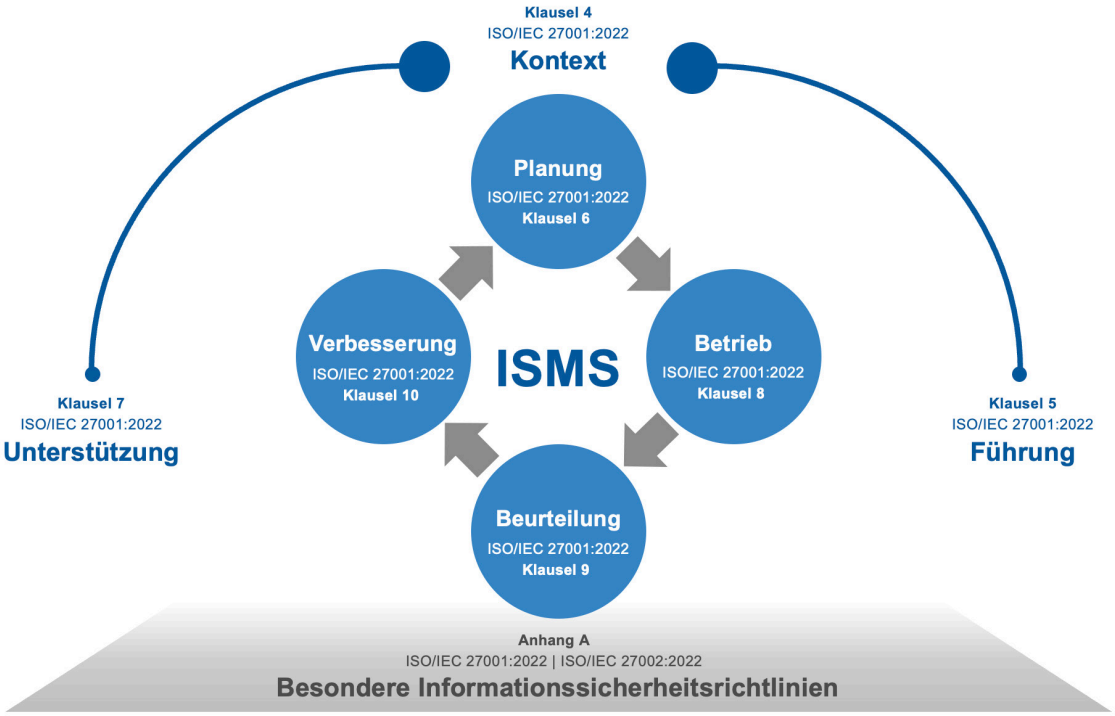
5. Betrieb des ISMS

Die Direktionen und die Staatskanzlei betreiben ein ISMS nach den Grundsätzen des kantonalen Regelwerks, der aktuellen ISO/IEC-27001-Norm und ihren individuellen Bedürfnissen. Durch das ISMS wird sichergestellt, dass der Schutz der Informationen und damit verbundener Werte in ihrem Zuständigkeitsbereich (Anhang 1 und 2 VOG RR) angemessen und wirksam umgesetzt wird.

5.1 Anforderungen an das ISMS

Ein ISMS ist gemäss ISO/IEC 27001:2022 die Aufstellung von Verfahren und Regeln innerhalb einer Organisation, die dazu dienen, die Informationssicherheit ganzheitlich, effektiv und nachhaltig zu definieren, zu steuern, zu kontrollieren, aufrechtzuerhalten und fortlaufend zu verbessern.

Das folgende Schaubild zeigt die grundlegenden Anforderungen an ein ISMS:



Besondere Informationssicherheitsrichtlinien
Die BISR bilden das zentrale Steuerelement zur Gewährleistung eines angemessenen Schutzniveaus. Sie orientieren sich an den Informationssicherheitsmassnahmen des Anhangs A der aktuellen ISO/IEC-27001-Norm sowie der dazugehörigen ISO/IEC-27002-Umsetzungshinweise.

Dabei müssen die thematisch aufgebauten BISR alle Informationssicherheitsmassnahmen des Anhangs A abdecken. Die Zugehörigkeit der Informationssicherheitsmassnahmen zu der jeweiligen BISR ist transparent auszuweisen (vgl. Anhang). Anforderungen innerhalb der BISR sind zu gewichten (z.B. anhand der Terminologie *muss, sollte, kann* in Anlehnung an RFC 2199) und entlang des abgestuften Modells den Umsetzungspartnern (Kanton, DIR/SK, Individuum) zuzuweisen.

5.2 Ausgestaltung des ISMS

Die Ausgestaltung des ISMS richtet sich nach dem individuellen Kontext der Direktionen und der Staatskanzlei. Für die Festlegung der Grundstrukturen und des Handlungsbedarfs wird folgendes Vorgehen empfohlen:

1. Ermitteln der relevanten Einflussfaktoren für das ISMS (Kontext)
2. Festlegen der Ausprägung für das ISMS (zentral, dezentral, hybrid)
3. Festlegen der Richtlinien (Kapitel 4), einschliesslich begründeter Anwendbarkeit der BISR
4. Ermitteln des Umsetzungsstandes in der jeweiligen Direktion oder der Staatskanzlei
5. Bewertung der Defizite und Ableiten des risikobasierten Handlungsbedarfs

5.3 Informationssicherheitsstrategie und -programm

Die Informationssicherheitsstrategie dient als Planungsinstrument zur Umsetzung der Informationssicherheit und beschreibt, wie und in welchem Zeitraum der Soll-Zustand entlang des priorisierten Handlungsbedarfs erreicht werden soll:

- **Kantonale Informationssicherheitsstrategie**
  Die Cybersicherheitsstrategie (für die künftig die Bezeichnung «Kantonale Informationssicherheitsstrategie» geplant ist) wird in einem Turnus von vier Jahren durch den Regierungsrat festgesetzt. Der Fokus liegt auf der Bereitstellung der gemeinsamen Basis, insbesondere der Ausgestaltung des kantonalen Regelwerks, der Bereitstellung ausgewählter ISSE und der Bestimmung der Prüfqualität (Einhalteprüfung) in den Direktionen und der Staatskanzlei. Die Strategie beschreibt die direktionsübergreifenden Massnahmen. Die benötigten finanziellen und personellen Mittel werden in einer Umsetzungsplanung ausgewiesen.
- **Kantonales Informationssicherheitsprogramm**
  Die Umsetzung der kantonalen Informationssicherheitsstrategie wird durch den Regierungsrat beauftragt und im Rahmen des jährlichen Steuerungsmeetings (vgl. Kapitel 6.4) kontrolliert. Die oder der ISIK stellt die Umsetzung der Massnahmen im Rahmen des kantonalen Informationssicherheitsprogramms durch das kantonale Zentrum für Informationssicherheit (CISC) sicher.
- **Informationssicherheitsstrategien der Direktionen und der Staatskanzlei**
  Die Direktionen und die Staatskanzlei sind verpflichtet, jeweils eine angemessene Strategie für die individuelle Umsetzung der Informationssicherheit (einschliesslich ISMS) in ihrem Verantwortungsbereich zu definieren, zu dokumentieren und zu erlassen. Die Informationssicherheitsstrategien der Direktionen und der Staatskanzlei beschreiben die direktionsinternen Massnahmen und stellt die notwendigen finanziellen und personellen Mittel in diesem Verantwortungsbereich sicher.
- **Umsetzung in den Direktionen und der Staatskanzlei**
  Die Umsetzung der Informationssicherheitsstrategien in den Direktionen und der Staatskanzlei wird durch die jeweiligen Direktionsvorstehenden in Auftrag gegeben und im Rahmen der jährlichen Steuerungsmeetings (vgl. Kapitel 6.4) kontrolliert.

5.4 Kontinuierliche Verbesserung

Die Umsetzung der Informationssicherheit sowie relevante Veränderungsfaktoren (Kontext, Organisation, Technologie, Anforderungen) werden überwacht und von den verantwortlichen Stellen regelmässig bewertet. Darauf aufbauend stellen die Direktionsvorstehenden die gezielte und systematische Verbesserung der Angemessenheit und Wirksamkeit der Informationssicherheit sowie des zugrunde liegenden ISMS sicher.

6. Beurteilung der Wirksamkeit

Die erfolgreiche Umsetzung der Informationssicherheit wird anhand von Metriken (kurzfristige Trends) sowie internen und externen Prüfaktivitäten gemessen. Die daraus gewonnenen Erkenntnisse werden in der kantonalen Berichterstattung konsolidiert und an den Steuerungsmeetings beurteilt.

Das Vorgehen orientiert sich an dem ISACA-Praxisleitfaden für Kennzahlen (Metriken), den Vorgaben der ISO/IEC-27000-Normreihe (Ausgestaltung und Periodizität der Prüfaktivitäten) sowie den Best Practices der IIA für interne Audits (Durchführung der Prüftätigkeiten).

6.1 Metriken

Um den Fortschritt der Informationssicherheit direktionsübergreifend messen und beurteilen zu können, werden kantonale Metriken einschliesslich deren kontextueller Beschreibung durch das SDI erlassen. Die Direktionen, die Staatskanzlei und das CISC stellen sicher, dass die Metriken in den vorgesehenen Zeitabständen in ihrem Zuständigkeitsbereich erhoben und in der geforderten Form durch die ISID der oder dem ISIK für die Berichterstattung zuhanden des SDI zur Verfügung gestellt werden.

6.2 Interne Prüfaktivitäten

Die Überprüfung der im Rahmen des Regelwerks erlassenen Anforderungen erfolgt in einem zweistufigen Verfahren. Zusätzlich zu den Anforderungen der ISO/IEC-27001-Norm werden die Ergebnisse der Einhalteprüfung auf kantonaler Ebene hinsichtlich ihrer Qualität überprüft.

- **Einhalteprüfung**
  Die Direktionen und die Staatskanzlei überprüfen mindestens jährlich anhand eines risikobasierten Ansatzes (Stichproben) und gemäss den Vorgaben der ISO/IEC-27001-Klausel 9.2, ob die festgelegten Anforderungen an die Informationssicherheit (ISMS, A/BISR[-DIR/SK], ISST[-DIR/SK]) eingehalten und die Informationssicherheitsmassnahmen angemessen und wirksam umgesetzt wurden.
- **Qualitätssicherung**
  Im Auftrag des SDI überprüft die oder der ISIK jährlich nach einem festgelegten und nachvollziehbaren Verfahren mittels eines risikobasierten Ansatzes (Stichproben) die durchgeführten Einhalteprüfungen hinsichtlich der Objektivität bzw. Genauigkeit der Prüfergebnisse. Dies kann bei Bedarf (z.B. Versäumnisse, kantonale Aggregationsrisiken oder ISSE) auch eigenständige Einhalteprüfungen innerhalb der Direktionen und der Staatskanzlei umfassen.

Die oder der ISIK koordiniert zusammen mit den Direktionen und der Staatskanzlei den jährlichen Prüfplan hinsichtlich der zeitlichen Abwickelung der kantonalen Qualitätssicherung. Dieser ist jeweils zu Jahresbeginn zu finalisieren und durch das SDI freizugeben.

6.3 Externe Prüfaktivitäten

Ab 2027 wird die Umsetzung der Informationssicherheit alle vier Jahre durch eine unabhängige, qualifizierte Zertifizierungsstelle (ISO/IEC 27001) anhand eines risikobasierten Ansatzes (Stichproben) auf Angemessenheit und Wirksamkeit geprüft. Es besteht keine Zertifizierungspflicht, die Verwendung der Zertifizierungsstelle dient einzig der Vergleichbarkeit der Ergebnisse aus den jeweiligen Verwaltungseinheiten.

- **Gemeinsame Basis:** Der oder die ISIK veranlasst im Auftrag des SDI eine Überprüfung des kantonalen Regelwerks (AISR/BISR), einschliesslich der kantonal erstellten bzw. betriebenen Informationssicherheitsstandards und -services (ISST/ISSE).
- **Individuelle Umsetzung:** Die Direktionen und die Staatskanzlei veranlassen eine Überprüfung des ISMS einschliesslich der daraus abgeleiteten Vorgaben, Verfahren und Informationssicherheitsmassnahmen.

Identifizierte Abweichungen zu Vorgaben (u.a. Gesetze, Verordnungen, Regelwerk, ISO/IEC 27001/2) sind innert nützlicher Frist zu beheben und die Behebung ist innert Jahresfrist durch eine Nachprüfung zu bestätigen.

6.4 Steuerungsmeetings

Der Stand der Informationssicherheit wird durch den Regierungsrat bzw. die Führungsorgane der Direktionen und der Staatskanzlei anhand des Steuerungsmeetings kontrolliert.

- **Kantonales Steuerungsmeeting**
  Unter der Leitung der oder des Vorsitzenden des SDI und der Mitwirkung der oder des ISIK wird jährlich ein Steuerungsmeeting zur Informationssicherheit mit dem Regierungsrat durchgeführt. Im Rahmen dieses Meetings wird der aktuelle Stand der Informationssicherheit aufgezeigt, die Ziele für das laufende Jahr bestimmt und bei Bedarf weiterführende Massnahmen festgelegt.
- **Steuerungsmeeting der Direktionen und der Staatskanzlei**
  Unter der Leitung der oder des zuständigen ISID wird jährlich ein Steuerungsmeeting zur Informationssicherheit mit den Führungsorganen der Direktionen bzw. der Staatskanzlei durchgeführt. Das Steuerungsmeeting ist gemäss den kantonalen Vorgaben zu protokollieren (vgl. Kapitel 6.5). Die Protokolle sind den Teilnehmenden des Steuerungsmeetings sowie der oder dem ISIK zur Verfügung zu stellen.

Die Steuerungsmeetings können eigenständig aufgesetzt oder als spezifisches, nachvollziehbares Traktandum in eine bereits bestehende Sitzungsagenda aufgenommen werden.

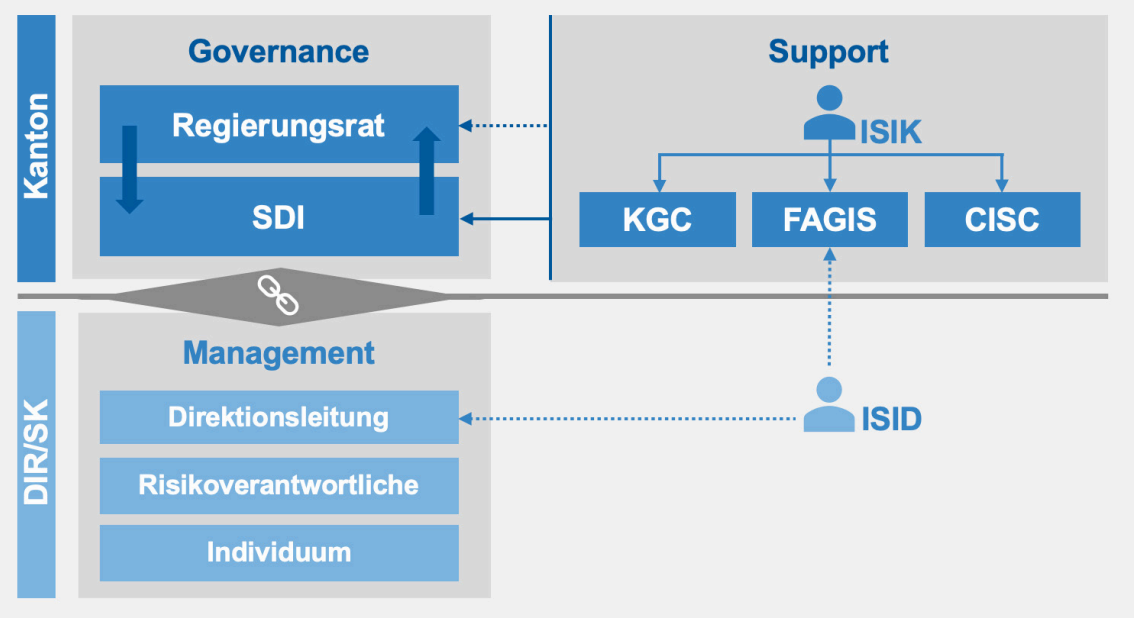
6.5 Kantonaler Bericht

Die oder der ISIK erstellt im Auftrag des SDI gestützt auf die jährlichen Protokolle aus den Steuerungsmeetings in den Direktionen und der Staatskanzlei einen Bericht zur Informationssicherheit in der kantonalen Verwaltung. Dieser Bericht wird dem Regierungsrat durch das SDI zur Kenntnisnahme vorgelegt. Zur Erstellung der kantonalen Berichte wird eine verwaltungsweit einheitliche Vorlage verwendet. Die Vorlage wird von der oder dem ISIK in Absprache mit dem SDI, den Direktionen und der Staatskanzlei festgelegt.

7. Rollen und Verantwortlichkeiten

Die Rollen und Verantwortlichkeiten berücksichtigen eine klare Trennung zwischen Governance- und Management-Strukturen (COBIT 2019) und stärken das Risikobewusstsein sowie die Entscheidungskompetenz der Linienorganisation bzw. der Risikoverantwortlichen.

Im Folgenden sind die Organe aufgeführt, denen spezifische Verantwortlichkeiten im Bereich der kantonalen Informationssicherheit zugewiesen sind.



7.1 Governance-Strukturen

Der Regierungsrat steuert und misst in Zusammenarbeit mit dem SDI die Umsetzung bzw. Einhaltung der kantonalen Anforderungen an die Informationssicherheit.

7.1.1 Regierungsrat

Der Regierungsrat trägt als oberste, leitende und vollziehende Behörde des Kantons die Gesamtverantwortung für die Informationssicherheit in der kantonalen Verwaltung.

- **Steuerung:** Der Regierungsrat erlässt auf Antrag der Finanzdirektion und nach Vorberatung durch das SDI die AISR sowie die kantonale Informationssicherheitsstrategie. Er entscheidet über Ausnahmen vom Geltungsbereich der AISR und über Anpassungen der kantonalen Informationssicherheitsstrategie.
- **Kontrolle:** Der Regierungsrat lässt sich regelmässig durch die Berichterstattung des SDI (einschliesslich kantonales Steuerungsmeeting) über die Belange der Informationssicherheit informieren. Dazu gehören insbesondere die Kenntnis über den aktuellen Umsetzungsstand der Informationssicherheitsstrategien, die Ergebnisse der Risikoanalysen und der Prüfungsaktivitäten sowie über vorhandene Optimierungspotenziale.

7.1.2 Gremium Steuerung Digitale Verwaltung und IKT

Das SDI beaufsichtigt im Auftrag des Regierungsrates die Tätigkeiten zur Informationssicherheit und stellt direktionsübergreifend sicher, dass die Informationen und damit verbundenen Werte des Kantons Zürich entsprechend den Vorgaben des Regierungsrates angemessen geschützt sind.

- **Steuerung:** Das SDI berät den Regierungsrat hinsichtlich Anpassungen der kantonalen Informationssicherheitsstrategie sowie der AISR und erlässt die BISR. Es stellt sicher, dass die Informationssicherheit im Rahmen der IKT-Strategie der Direktionen und der Staatskanzlei sowie bei wichtigen Projekten des IKT-Projektportfolios angemessen berücksichtigt wird. Ferner steuert es die Umsetzung der kantonalen Informationssicherheitsstrategie und beauftragt bei Bedarf die oder den ISIK mit deren Überarbeitung.
- **Kontrolle:** Das SDI stellt die Durchführung der Prüftätigkeiten sicher und gibt die Metriken sowie den jährlichen Plan für die kantonalen Prüftätigkeiten frei. Es prüft die Berichte der zuständigen Stellen hinsichtlich des aktuellen Stands der Informationssicherheitsstrategie, potenzieller Risiken sowie des Optimierungspotenzials und setzt den Regierungsrat in regelmässigen Abständen darüber in Kenntnis.

Das SDI ist die Eskalationsstelle, falls in den vorberatenden Gremien und Fachstellen in Bezug auf die Informationssicherheit keine Einigung erzielt werden kann.

7.2 Managementstrukturen

Die Direktionen und die Staatskanzlei verantworten die Umsetzung der Informationssicherheit innerhalb ihres Verantwortungsbereichs nach den kantonalen Informationssicherheitsvorgaben des Regierungsrates bzw. des SDI.

7.2.1 Direktionsvorstehende

Die Direktionsvorstehenden tragen die Verantwortung für die Informationssicherheit in ihrem Verantwortungsbereich und handeln entlang den Zielen und Grundsätzen dieser AISR. Sie sorgen für eine nachhaltige Umsetzung der Informationssicherheit und unterstützen proaktiv.

Dahingehend haben die Direktionsvorstehenden folgende Aufgaben:

- Sie erlassen die AISR-DIR/SK und die Informationssicherheitsstrategie der Direktion oder Staatskanzlei.
- Sie integrieren die Informationssicherheit in ihre Verwaltungsprozesse.
- Sie weisen die informationssicherheitsrelevanten Aufgaben, Verantwortlichkeiten und Kompetenzen zu und stellen sicher, dass diese verstanden und wahrgenommen werden.
- Sie beauftragen die Verwaltungseinheiten mit der Umsetzung der Vorgaben zur Informationssicherheit, insbesondere der Informationssicherheitsstrategie.
- Sie stellen im Rahmen der vorherrschenden Prozesse angemessene Mittel für die Umsetzung der Informationssicherheitsmassnahmen bereit.
- Sie fördern eine angemessene Sicherheitskultur durch Verpflichtungserklärungen zu Schulungs- und Sensibilisierungsmassnahmen.
- Sie stellen sicher, dass ihr Risikomanagementsystem Informationssicherheitsrisiken in angemessener Weise berücksichtigt.
- Sie gewährleisten, dass die Angemessenheit und die Wirksamkeit des ISMS sowie der festgelegten Anforderungen regelmässig überprüft und die daraus folgenden Massnahmen umgesetzt werden.
- Sie stellen sicher, dass die gesetzlichen Anforderungen und die kantonalen Vorgaben zur Informationssicherheit eingehalten und erkannte Mängel zeitnah behoben werden.
- Sie sorgen dafür, dass Optimierungspotenzial fortlaufend erkannt, bewertet, vorgetragen, beschlossen und umgesetzt wird.

7.2.2 Risikoverantwortliche

Die Verwaltungseinheiten bestimmen in ihrem Verantwortungsbereich Risikoverantwortliche, die im Rahmen der ihnen übertragenen Handlungsbefugnis sicherstellen, dass Informationssicherheitsrisiken angemessen identifiziert, bewertet und behandelt werden.

7.2.3 Individuum

Mitarbeitende sowie externe Partner sind für die Einhaltung der Informationssicherheitsanforderungen und -massnahmen gemäss den Vorgaben der Direktionen bzw. der Staatskanzlei verantwortlich und nehmen an den geforderten Sensibilisierungs- und Schulungsmassnahmen teil. Wahrgenommene Informationssicherheitsereignisse haben sie zeitnah zu melden.

7.3 Supportstrukturen

Die direktionsübergreifenden Support-Strukturen unterstützen die Governance- und Managementstrukturen bei der Wahrnehmung ihrer Verantwortlichkeiten.

7.3.1 Kerngruppe Cyber

Die KGC besteht aus der oder dem ISIK, der Chefin oder dem Chef des AFI, der Chefin oder dem Chef der Informatik der Kapo sowie Vertreterinnen und Vertretern der KFO, der Staatsanwaltschaft und einer kantonalen kritischen Infrastruktur.

Die KGC nimmt unter der Leitung des ISIK folgende Aufgaben wahr:

- Sie berät das SDI in Bezug auf Informationssicherheitsvorfälle und Sensibilisierungsmassnahmen kantonsnaher Organisationen.
- Sie unterstützt Fach- und Krisenstäbe (z.B. CSIRT) bei der Durchführung von Übungen und wertet die Übungsergebnisse im Hinblick auf die Informationssicherheit aus.
- Sie zieht Lehren aus der Bewältigung von Informationssicherheitsvorfällen in der eigenen Organisation oder der Umwelt, entwickelt darauf aufbauende Optimierungsmassnahmen und beantragt dem SDI bzw. dem Regierungsrat deren Umsetzung.
- Sie stellt sicher, dass die kantonsnahen Organisationen und die Gemeinden in regelmässigen Abständen informiert und hinsichtlich der sie betreffenden kantonalen Informationssicherheitsanforderungen sensibilisiert werden.
- Sie unterstützt das SDI und den Regierungsrat bei Differenzen in der kantonalen Informationssicherheitsorganisation.

7.3.2 Fachgruppe Informationssicherheit

Die FAGIS besteht aus zwölf Mitgliedern: der oder dem ISIK, einer Vertreterin oder einem Vertreter der DSB, allen acht ISID und jeweils einer Verbindungsperson zur Kapo sowie zur IKT-Grundversorgung im AFI.

Die FAGIS nimmt unter der Leitung der oder des ISIK folgende Aufgaben wahr:

- Sie berät das SDI bei der Erfüllung seiner strategischen Informationssicherheitsaufgaben.
- Sie behandelt die Anliegen der Direktionen und der Staatskanzlei in Bezug auf Fragen zur Informationssicherheit.
- Sie beurteilt die Entwicklung kantonal relevanter Informationssicherheitsrisiken und stellt die daraus abgeleiteten Erkenntnisse dem SDI zur Verfügung.
- Sie sorgt für eine fortlaufende Optimierung der BISR bezüglich Verständlichkeit, Angemessenheit und Umsetzbarkeit.

- Sie stellt dem SDI den Antrag zum Erlass und zur Anpassung der BISR.
- Sie setzt bei Bedarf Expertinnen und Experten oder Fachgruppen ein, um operative Informationssicherheitsthemen im Rahmen der FAGIS zu behandeln.

7.3.3 Kantonales Zentrum für Informationssicherheit

Das CISC ist das Kompetenzzentrum des Kantons für Informationssicherheit und nimmt unter der Leitung der oder des ISIK folgende Aufgaben wahr:

- Es koordiniert die Umsetzung der kantonalen Informationssicherheitsstrategie.
- Es stellt die im Rahmen der kantonalen Informationssicherheitsstrategie beim CISC angesiedelten Informationssicherheitsservices den Direktionen bzw. der Staatskanzlei zur Verfügung.
- Es prüft die Eignung der bestehenden und den Bedarf an neuen kantonalen ISSE für die Direktionen und die Staatskanzlei.
- Es prüft die Erfassung, Relevanz, Qualität und Entwicklung der kantonal relevanten Informationssicherheitsrisiken sowie die Angemessenheit und Wirksamkeit ihrer Behandlung aus einer aggregierten, kantonalen Perspektive.
- Es unterstützt bei der Erstellung der Prüfpläne und führt die kantonale Qualitätssicherung innerhalb der Direktionen bzw. der Staatskanzlei durch.
- Es erstellt jährlich einen konsolidierten Bericht zuhanden des Regierungsrates bzw. des SDI mit den gewonnenen Erkenntnissen und den daraus abgeleiteten Empfehlungen zu den durchgeführten Prüftätigkeiten.
- Es berät im Auftrag der oder des ISIK Fachgruppen und Gremien sowie die Direktionen und die Staatskanzlei zu Aspekten der Informationssicherheit.

7.3.4 Informationssicherheitsbeauftragte/r des Kantons Zürich

Die oder der ISIK wird vom AFI angestellt und leitet die KGC, die FAGIS sowie das CISC. Sie oder er ist die zentrale Ansprechperson für interne und externe Anfragen zur Informationssicherheit in der kantonalen Verwaltung und vertritt bei Bedarf die Anliegen der Informationssicherheit in den Krisen- und Fachstäben des Kantons (z.B. CSIRT).

In dieser Funktion nimmt die oder der ISIK folgende Aufgaben wahr:

- Sie oder er berät den Regierungsrat bzw. das SDI in Fragen der Informationssicherheit.
- Sie oder er stellt im Auftrag des Regierungsrates bzw. des SDI die Umsetzung und Weiterentwicklung der kantonalen Informationssicherheitsstrategie sicher.
- Sie oder er sorgt für eine zweckmässige Abstimmung der direktionsübergreifenden Zusammenarbeit im Bereich der Informationssicherheit und stellt erkannte Optimierungspotenziale in den entsprechenden Fachgruppen und Gremien zur Diskussion.
- Sie oder er gewährleistet die erforderliche Sichtbarkeit der kantonalen Informationssicherheitsaktivitäten, der kantonalen Informationssicherheitsrisiken sowie der berechtigten Interessen der Direktionen und der Staatskanzlei.
- Sie oder er prüft in regelmässigen Abständen die Angemessenheit des kantonalen Regelwerks (AISR, BISR, ISST, ISSE) und leitet gegebenenfalls notwendige Optimierungsmassnahmen ein.
- Sie oder er erarbeitet im Auftrag des SDI die kantonalen Metriken zur Messung und Beurteilung der direktionsübergreifenden Wirksamkeit der Informationssicherheit.

- Sie oder er stellt im Auftrag des SDI die Planung und objektive Durchführung der Qualitätssicherungen sicher und kann ausserordentliche Prüftätigkeiten zur Ermittlung spezifischer Risiken beim SDI beantragen.
- Sie oder er informiert das SDI zuhanden des Regierungsrates regelmässig über den Stand der Informationssicherheit in der kantonalen Verwaltung.

7.3.5 Informationssicherheitsbeauftragte/r in der Direktion

Jede Direktion und die Staatskanzlei bestimmt eine oder einen ISID, die oder der mit den individuellen Bedürfnissen der Direktion bzw. der Staatskanzlei in Bezug auf die Informationssicherheit vertraut ist und diese im Rahmen ihrer bzw. seiner Mitgliedschaft in der FAGIS vertritt.

Als Mitglieder der FAGIS nehmen die ISID folgende Aufgaben wahr:

- Sie vertreten die individuellen Bedürfnisse der jeweiligen Direktionen und der Staatskanzlei im Rahmen der FAGIS.
- Sie gewährleisten die notwendige Sichtbarkeit der kantonalen Informationssicherheitsaktivitäten innerhalb der Direktionen und Staatskanzlei und stellen die direktionsübergreifende Abstimmung und Zusammenarbeit sicher.
- Sie unterstützen bei der Abwicklung von berechtigten Anliegen der Direktionen und der Staatskanzlei in Bezug auf Fragen zur Informationssicherheit.
- Sie erstatten quartalsweise Bericht über die kantonal relevanten Informationssicherheitsrisiken aus den Direktionen und der Staatskanzlei und stellen die Berichte dem CISC in dem vom SDI geforderten Umfang und Format zur Verfügung.
- Sie prüfen die Verständlichkeit, Angemessenheit und Umsetzbarkeit der BISR und kantonalen Standards sowie den Bedarf neuer und die Angemessenheit bestehender kantonaler Informationssicherheitsservices und stellen erkannte Optimierungspotenziale der oder dem ISIK zur Verfügung.
- Sie prüfen Anträge zuhanden des SDI für den Erlass und die Anpassung von BISR.
- Sie stellen im Auftrag der Direktionen und der Staatskanzlei sicher, dass die erhobenen Metriken im geforderten Format der oder dem ISIK bereitgestellt werden.
- Sie führen das direktionsinterne Steuerungsmeeting zur Informationssicherheit durch und gewährleisten, dass die Protokolle an die Teilnehmenden sowie an die oder den ISIK verteilt werden.
- Sie melden der oder dem ISIK wesentliche Vorkommnisse im Bereich der Informationssicherheit innerhalb der jeweiligen Direktion oder der Staatskanzlei.

Direktionsinterne Aufgaben
Die direktionsinternen Aufgaben, Kompetenzen und Verantwortlichkeiten der ISID werden durch die Direktionsvorstehenden festgelegt und in der AISR-DIR/SK der jeweiligen Direktion bzw. der Staatskanzlei verankert.

8. Schnittstellen zu weiteren Fachthemen

Aufgrund des multidisziplinären Charakters der Informationssicherheit bestehen Schnittstellen zu unterschiedlichen kantonalen Fachstellen. Im Folgenden werden wesentliche Schnittmengen sowie hierfür vorgesehene Auslegeregelungen beschrieben:

- **Datenschutz**
  Die Umsetzung eines Datenschutz-Managementsystems (DSMS) erfolgt im Verantwortungsbereich der Direktionen oder der Staatskanzlei (§ 60 Abs. 1 lit. e VOG RR). Der «Leitfaden Datenschutz-Managementsystem (DSMS)» der oder des DSB kann die Verwaltungseinheiten bei der Erfüllung der datenschutzrechtlichen Anforderungen des IDG in den Projekten und Verwaltungsprozessen unterstützen.

- **Risikomanagement**
  Die Direktionen und die Staatskanzlei gewährleisten, dass ihr jeweiliges Risikomanagementsystem Informationssicherheitsrisiken in angemessener Weise berücksichtigt. Bei der Erarbeitung und dem Erlass von Anforderungen an Informationssicherheitsrisiken müssen die oder der ISIK und das SDI sicherstellen, dass dies unter Berücksichtigung des Integralen Risikomanagements (vgl. § 14 VOG RR, RRB Nr. 1001/2022, IntRM) der Sicherheitsdirektion (Kapo) erfolgt.

- **Krisenmanagement**
  Die Direktionen und die Staatskanzlei sind verantwortlich für den Aufbau und Betrieb des Krisenmanagements. Bei eskalierenden Informationssicherheitsvorfällen muss die verantwortliche Stelle für das Management dieser Vorfälle sicherstellen, dass die bestehenden Krisenmanagementstrukturen sowohl bei ihr selbst als auch in den weiteren betroffenen Direktionen und der Staatskanzlei eingebunden werden. Dabei werden die geltenden Regelungen des Bevölkerungsschutzgesetzes (BSG, LS 520) und der Verordnung über den Einsatz der kantonalen Führungsorgane (KFOV, LS 172.5) berücksichtigt. Diese Regelungen gelten sowohl für eine ausserordentliche Lage gemäss § 2 BSG als auch für den Einsatz der KFO gemäss § 2 KFOV in anderen Situationen.

- **Kontinuitätsmanagement**
  Der Aufbau und Betrieb eines Kontinuitätsmanagements erfolgt im Verantwortungsbereich der Direktionen oder der Staatskanzlei unter Berücksichtigung des Definitionsrahmen des Integralen Risikomanagements. Das IT-Kontinuitätsmanagement bei der für die IKT-Systeme verantwortlichen Stelle muss sicherstellen, dass die betrieblichen Anforderungen der betroffenen Verwaltungseinheiten bei der technischen Umsetzung berücksichtigt werden. Die Leiterin oder der Leiter IT-Kontinuitätsmanagement AFI erarbeitet Hilfsmittel, welche die Informationssicherheitsanforderungen (Wiederherstellung, Aufrechterhaltung) des kantonalen Regelwerks angemessen berücksichtigen, und unterstützt bei Bedarf beratend. Die Direktionen und die Staatskanzlei können diese als Basis verwenden oder Verfahren und Massnahmen eigenständig erarbeiten und umsetzen.

- **Informationsverwaltung**
  Wesentliche Aspekte der Informationssicherheit können nur mit einer sinnvoll organisierten und korrekt umgesetzten Informationsverwaltung erreicht werden, nicht zuletzt die Vollständigkeit und Verfügbarkeit von Informationen. Das Staatsarchiv stellt Hilfsmittel zum Thema zur Verfügung und unterstützt die Verwaltungseinheiten bei der Umsetzung.

- **Personalsicherheit**
  Personenbezogene Informationssicherheitsanforderungen sind in Übereinstimmung mit den Vorgaben des Personalgesetzes (PG) und seinen Verordnungen (PVO und VVO) auszugestalten. Vor dem Antrag durch die FAGIS bzw. dem Erlass durch das SDI ist das Personalamt zur Stellungnahme einzuladen. Bei Widersprüchen zum Personalgesetz oder seinen Verordnungen gehen diese vor.

- **IKT-Infrastrukturen**
  Beim Aufbau und Betrieb von IKT-Infrastrukturen sind die technischen und organisatorischen Anforderungen der Informationssicherheit durch die verantwortlichen Organisationseinheiten angemessen zu berücksichtigen und wirksam umzusetzen.
  - **Amt für Informatik**
    Im Rahmen der IKT-Grundversorgung unterstützt eine dedizierte Informationssicherheitsbeauftragte oder ein dezidierter Informationssicherheitsbeauftragter im AFI die Umsetzung der IKT-Sicherheit. Die Ausgestaltung der IKT-Sicherheit der einheitlichen Schutzstufen wird in den Servicebeschreibungen festgelegt.
  - **Kantonspolizei**
    Aufgrund der eigenständig aufgebauten IKT-Infrastruktur betreibt die Kapo ein eigenes ISMS. Der Betrieb dieses ISMS wird durch die Sicherheitsdirektion beauftragt, durch die Kommandantin oder den Kommandanten der Kapo verantwortet und durch eine dedizierte Informationssicherheitsbeauftragte oder einen dezidierten Informationssicherheitsbeauftragten unterstützt.
- **Data Governance**
  Die kantonale Data Governance definiert unter anderem Prinzipien und Richtlinien, welche die Grundlagen der kantonalen Datenbewirtschaftung regeln. Da die Data Governance einen effizienten und effektiven Austausch und die Informationssicherheit einen angemessenen und wirksamen Schutz der Informationen gewährleistet, ist eine enge Abstimmung zwischen den beiden Disziplinen notwendig. Dies betrifft insbesondere die Identifikation und Behandlung von Risiken im Zusammenhang mit Informationen. Die oder der ISIK bzw. das CISC begleitet daher die Ausgestaltung der Data Governance aus Sicht der Informationssicherheit und trägt aktiv zu harmonisierten Anforderungen bei. Sollte es dennoch zu Widersprüchen kommen, gehen die besonderen Anforderungen den allgemeinen vor.
- **Beschaffung und Einkauf**
  Informationssicherheitsrisiken in der Lieferkette haben in den letzten Jahren stark zugenommen. Im Rahmen des kantonalen Beschaffungswesens müssen neben dem Gesetz über den Beitritt zur Interkantonalen Vereinbarung über das öffentliche Beschaffungswesen (BeiG IVöB), der totalrevidierten Submissionsverordnung (SVO) sowie der Beschaffungspolitik des Regierungsrates auch Anforderungen an die Informationssicherheit berücksichtigt werden.
- **Physische Gebäudesicherheit**
  Die Gebäude der kantonalen Verwaltung und ihre technischen Einrichtungen, einschliesslich der Verkabelung, sind vor Gefahren und Umwelteinflüssen, vor unbefugtem Zutritt und vor Störungen zu schützen und ordnungsgemäss instand zu halten. Dabei beschränken sich die Anforderungen des kantonalen Regelwerks auf die Aspekte der physischen Informationssicherheit und widerspiegeln nicht das volle Spektrum an geltenden Regelungen. Bei Widersprüchen zu physischen, gebäude- oder rechenzentrenspezifischen Regelungen gehen diese vor. Die Sicherstellung der physischen und umgebungsbezogenen Sicherheit innerhalb der Verwaltung liegt in der Zuständigkeit der Immobiliennutzerin und der Betreiberorganisation. Bauliche Massnahmen werden je nach Projektgrösse durch das Immobilienamt oder das Hochbauamt umgesetzt.

Um mögliche Diskrepanzen zu minimieren und möglichst harmonisierte Informationssicherheitsanforderungen in den einzelnen Fachthemen zu gewährleisten, erfolgt die Erarbeitung der themenspezifischen Aspekte der AISR und insbesondere der BISR in enger Zusammenarbeit mit den genannten Fachstellen.

Anhang: Zuweisung der ISO/IEC 27001 Anhang A Massnahmen zu den BISR

Gemäss Kapitel 7.1.2 ist das SDI zuständig für den Erlass aller BISR.

Im Zeitpunkt des Erlasses der vorliegenden AISR sind die 93 Informationssicherheitsmassnahmen des Anhangs A der ISO/IEC-27001:2022-Norm bzw. die zugehörigen ISO/IEC-27002:2022-Umsetzungshinweise:

- 37 organisatorische Massnahmen (5.01–5.37)
- 8 personenbezogene Massnahmen (6.01–6.08)
- 14 physische Massnahmen (7.01–7.14)
- 34 technologische Massnahmen (8.01–8.34)

wie folgt den BISR zugewiesen:

BISR-2: Richtlinie für die Verwaltung von organisationseigenen Werten

- 5.09: Inventar der Informationen und anderen damit verbundenen Werten
- 5.10: Zulässiger Gebrauch von Informationen und anderen damit verbundenen Werten
- 5.11: Rückgabe von Werten

BISR-3: Richtlinie für die Informationsklassifikation und -kennzeichnung

- 5.12: Klassifizierung von Information
- 5.13: Kennzeichnung von Information

BISR-4: Richtlinie für Identitäts- und Zugriffskontrolle

- 5.15: Zugangssteuerung
- 5.16: Identitätsmanagement
- 5.18: Zugangsrechte
- 8.02: Privilegierte Zugangsrechte
- 8.03: Informationszugangsbeschränkung

BISR-5: Richtlinie für Personalsicherheit

- 6.01: Informationssicherheitsrichtlinien
- 6.02: Beschäftigungs- und Vertragsbedingungen
- 6.04: Sanktionierung von Pflichtverletzungen
- 6.05: Verantwortlichkeiten bei Beendigung oder Änderung der Beschäftigung

BISR-6: Richtlinie für Schulungsmassnahmen in Informationssicherheit

- 6.03: Informationssicherheitsbewusstsein, -ausbildung und -schulung

BISR-7: Richtlinie für mobile Endgeräte

- 8.01: Endpunktgeräte des Benutzers

BISR-8: Richtlinie für die Handhabung von Speichermedien

- 7.10: Speichermedien
- 8.10: Löschung von Informationen

BISR-9: Richtlinie für Telearbeit

- 6.07: Telearbeit
- 7.09: Sicherheit von Werten ausserhalb der Räumlichkeiten

BISR-10: Richtlinie für Passwörter

- 5.17: Informationen zur Authentifizierung
- 8.05: Sichere Authentifizierung

BISR-11: Richtlinie für kryptographische Massnahmen

- 8.24: Verwendung von Kryptographie

BISR-12: Richtlinie für die Verwaltung von Geräten und Betriebsmitteln

- 7.08: Platzierung und Schutz von Geräten und Betriebsmitteln
- 7.13: Instandhaltung von Geräten und Betriebsmitteln
- 7.14: Sichere Entsorgung oder Wiederverwendung von Geräten und Betriebsmitteln

BISR-13: Richtlinie für Datensicherung

- 8.13: Sicherung von Information

BISR-14: Richtlinie für Protokollierung und Überwachung

- 8.15: Protokollierung
- 8.16: Überwachung von Aktivitäten
- 8.17: Uhrensynchronisation

BISR-15: Richtlinie für die Verwaltung von Bedrohungen und Schwachstellen

- 5.07: Bedrohungsintelligenz
- 8.08: Handhabung von technischen Schwachstellen

BISR-17: Richtlinie für die Verwaltung der Netzwerksicherheit

- 8.20: Netzwerksicherheit
- 8.21: Sicherheit von Netzwerkdiensten
- 8.22: Trennung von Netzwerken
- 8.23: Webfilterung

BISR-18: Richtlinie für die Handhabung von Informationen

- 5.14: Informationsübertragung
- 5.33: Schutz von Aufzeichnungen
- 5.34: Datenschutz und Schutz personenbezogener Daten
- 8.11: Datenmaskierung
- 8.12: Verhinderung von Datenlecks

BISR-19: Richtlinie für die Sicherheit von Informationssystemen

- 5.37: Dokumentierte Betriebsabläufe
- 7.07: Aufgeräumte Arbeitsumgebung und Bildschirmsperren
- 8.06: Kapazitätssteuerung
- 8.07: Schutz gegen Schadsoftware
- 8.09: Konfigurationsmanagement
- 8.18: Gebrauch von Hilfsprogrammen mit privilegierten Rechten
- 8.19: Installation von Software auf Systemen im Betrieb
- 8.32: Änderungssteuerung

BISR-20: Richtlinie für die Integration und die Entwicklung von Informationssystemen

- 8.04: Zugriff auf den Quellcode
- 8.25: Lebenszyklus einer sicheren Entwicklung
- 8.26: Anforderungen an die Anwendungssicherheit
- 8.27: Sichere Systemarchitektur und technische Grundsätze
- 8.28: Sicheres Coding
- 8.29: Sicherheitsprüfung in Entwicklung und Abnahme
- 8.30: Ausgegliederte Entwicklung
- 8.31: Trennung von Entwicklungs-, Prüf- und Produktionsumgebungen

BISR-21: Richtlinie für die Sicherheit von Testdaten

- 8.33: Testdaten

BISR-22: Richtlinie für Beziehungen zu Lieferanten

- 5.19: Informationssicherheit in Lieferantenbeziehungen
- 5.20: Behandlung von Informationssicherheit in Lieferantenvereinbarungen
- 5.21: Umgang mit der Informationssicherheit in der IKT-Lieferkette

- 5.22: Überwachung, Überprüfung und Änderungsmanagement von Lieferantendienstleistungen
- 6.06: Vertraulichkeits- oder Geheimhaltungsvereinbarungen

BISR-23: Richtlinie für die Sicherheit von physischen Infrastrukturen

- 7.01: Physische Sicherheitsperimeter
- 7.02: Physischer Zutritt
- 7.03: Sichern von Büros, Räumen und Einrichtungen
- 7.04: Physische Sicherheitsüberwachung
- 7.05: Schutz vor physischen und umweltbedingten Bedrohungen
- 7.06: Arbeiten in Sicherheitsbereichen
- 7.11: Versorgungseinrichtungen
- 7.12: Sicherheit der Verkabelung

BISR-24: Richtlinie für den Umgang mit Informationssicherheitsvorfällen

- 5.24: Planung und Vorbereitung der Handhabung von Informationssicherheitsvorfällen
- 5.25: Beurteilung und Entscheidung über Informationssicherheitsereignisse
- 5.26: Reaktion auf Informationssicherheitsvorfälle
- 5.27: Erkenntnisse aus Informationssicherheitsvorfällen
- 5.28: Sammeln von Beweismaterial
- 6.08: Meldung von Informationssicherheitsereignissen

BISR-25: Richtlinie Informationssicherheit bei Störungen und IKT-Kontinuität

- 5.29: Informationssicherheit bei Störungen
- 5.30: IKT-Bereitschaft für Business Continuity
- 8.14: Redundanz von informationsverarbeitenden Einrichtungen

BISR-26: Richtlinie für die Umsetzung der Informationssicherheit

- 5.01: Informationssicherheitsrichtlinien
- 5.02: Informationssicherheitsrollen und -verantwortlichkeiten
- 5.03: Aufgabentrennung
- 5.04: Verantwortlichkeiten der Leitung
- 5.05: Kontakt mit Behörden
- 5.06: Kontakt mit speziellen Interessensgruppen
- 5.08: Informationssicherheit im Projektmanagement
- 5.31: Rechtliche, gesetzliche, regulatorische und vertragliche Anforderungen
- 5.32: Geistige Eigentumsrechte

BISR-28: Richtlinie für die Beurteilung der Wirksamkeit der Informationssicherheit

- 5.35: Unabhängige Überprüfung der Informationssicherheit
- 5.36: Einhaltung von Richtlinien, Vorschriften und Normen für die Informationssicherheit
- 8.34: Schutz der Informationssysteme während der Überwachungsprüfung

BISR-29: Richtlinie für die Nutzung von Cloud-Diensten

- 5.23: Informationssicherheit für die Nutzung von Cloud-Diensten

Ergänzende Anmerkung:

- BISR-16 orientiert sich an den ISO/IEC-27001:2022-Klauseln 6.1 (Risikobewertung und -behandlung), 8.1 (Betrieb), 9.1 (Überwachung und Bewertung), 10.2 (Korrekturmassnahmen), der ISO/IEC 27005 (Informationssicherheitsrisiken) und der ISO/IEC 31000 (generelle Risiken).
- BISR-27 orientiert sich an den ISO/IEC-27001:2022-Klauseln 6.1 (Risikobewertung und -behandlung), 8.1 (Betrieb) 9.1 (Überwachung und Bewertung) und 10 (Verbesserung).